Tampere University

Amira Ferraboli

# CYBER RISK MANAGEMENT: APPROACHES AND TRENDS IN FINLAND

Faculty of Management and Business
Master's thesis
November 2021

# ABSTRACT

Amira Ferraboli: Cyber Risk Management: Approaches and Trends in Finland
Master's Thesis
Tampere University
Degree Programme in Security and Safety Management
November 2021

---

Cyber risks reflect uncertainty within the objectives and assets associated with information and technology systems. The increasing importance of the cyber domain is all spheres of society has determined that cyber risks ought to be managed to protect systems and their information from undue access, use, modification, disclosure and destruction. Cyber risk management is a package of practices, tools, techniques and processes employed to identify, analyse, evaluate, respond and monitor cyber risks.

The objectives of this study are two. First, to understand and describe how risk and risk management are understood and approached by private companies operating in the cyber risk field in Finland. Second, to understand the current cyber risk management market in Finland and identify its trends. This study is a qualitative research seeking to describe and interpret cyber risk management practices in Finland. The primary data for this study was collected through semi-structured exploratory interviews conducted with five professionals working for different private companies operating in the cyber risk field in Finland. The collected data was thematically and inductively analysed to establish categories and patterns. The results of this analysis were utilized to build understandings, approaches and conclusions.

The results and conclusions of this study indicate that the interviewed professionals working in the cyber risk field in Finland understand risk as the negative effect and impact of uncertainty on systems and assets. These professionals view risk management as a combination of policies, tools, methods and processes developed to address cyber risks. They mostly follow international standards and frameworks to carry out their activities and develop their cyber risk management processes. The interviewed professionals approach cyber risk management in different ways in terms of proactivity, customization and comprehensiveness of their services. The results and conclusions of this study further indicate that most of the interviewed professionals believe that the Finnish cyber risk management market is still very technical and underdeveloped. They also see a gap between international best practices and local practices in terms of cyber risk management. Finally, the results and conclusions show that professionals operating in the cyber risk field in Finland see the increasing use of diverse analytical techniques, the increasing importance of international standards and frameworks, and the approximation between governmental and corporate players as trends in their field.

Keywords: cyber risk, cyber risk management, risk management, risk management process, cyber security, information security.

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

# TABLE OF CONTENTS

# 1 INTRODUCTION

This research dedicates to studying the management of risks that exist in the cyberspace and in information systems, as well as the tools, frameworks and processes that are employed in doing so. The importance of cyber risk management has been increasing throughout the years across several fields as businesses expand their online presence and their reliance on information systems. However, not many studies have been developed to follow this growth, especially considering studies that look at the phenomenon from a social-economic perspective and not from a technical one. The importance of cyber risk management combined with the lack of studies in the field is what motivated this research. Also, a previous work experience with risk management and an interest in understanding more about the non-technical cyber world were catalysers for this research.

In the below paragraphs, a brief history of the cyberspace and of information systems will be presented, and data will be provided to highlight the growing importance of the topic. The subsequent subsections of this introduction will explain in detail the objective of this study and its research questions, will discuss the concepts of risk and risk management, will define other important concepts utilized in this study, will investigate previous studies connecting risk management and the cyberspace, will explain the research methods utilized in this research and will describe the organization of its sections.

The first rudimentary computer is said to have been developed in the beginning of the 19$^{th}$ century as a calculating machine fed by steam. The notion of modern computers started flourishing in mid-1930's, when Alan Turing developed his universal machine, capable of computing solutions to all computable problems (De Mol, 2019). In the following years, advancements were made one after another, until the first personal computers were released into the market between the 70's and 80's. Approximately in this same period, the U.S. Defence Department's Advanced Research Projects Agency Network ("ARPANET"), the predecessor of the internet we know nowadays, was born and started to evolve. In 1989, the *world wide web* ("www") was created to revolutionize the history of communication and data sharing (Roser, Ritchie, and Ortiz-Ospina, 2015). Initially, computers and the internet were scientific tools, and were not designed to become mass products/services. Still, their massification potential eventually became blatant. The biggest challenge for inventions is usually turning them into marketable innovations that will spread and be broadly adopted by average users. Computers and the internet did not fail this stage. In mid-1990's, they were both widely available to and used by the public.

Latest data made available by the specialized market and consumer data company Statista, indicates that as of January 2021, 59.50% of the world's population was using the internet. This was, by then, equivalent to 4.66 billion people. The same source further indicates that on the same date, 4.32 billion people were using social media platforms worldwide. (*Worldwide digital population as of January 2021*, 2021) When we look closer to computer and internet usage in individual countries, the figures are even more impressive. According to the Organisation for Economic Co-operation and Development ("OECD"), in 2020, 97.30% of all households in the United Kingdom, for example, had internet access. In Finland, in 2020, this percentage was 96%, and in the U.S., in 2019,[1] it was 79.90%. (*Information and communication technology (ICT) - Internet access - OECD Data*, 2021) When it comes to the percentage of households with access to computers from home, the OECD indicates that, in 2017, it was 91.70% in the United Kingdom. In Finland, in 2017, this percentage was 93.50%. (*Access to computers from home - OECD Data,* 2021)

However, individuals and households are not the sole owners of computer and users of internet. Millions of companies own computers with internet access and rely on them to conduct several daily tasks, to develop their core businesses and, ultimately, generate revenue. Data made available by the OECD shows that, in 2019, 95.45% of all businesses in the United Kingdom with at least 10 employees had a broadband connection, and 83.30% had a website or a home page. In Finland, in 2020, these percentage were, respectively, 100% and 95.92%. The OECD further indicates that the percentage of employees using a computer with internet access was 60.87% in the United Kingdom, in 2019, and 80.37% in Finland, in 2020.[2] (*ICT Access and Usage by Businesses*, 2021) As depicted in these figures, the successful development and commercialization of computers, as well as the ever-increasing growth of the internet, unlocked a new dimension of our lives: the digital dimension.

E-mail, instant messaging, real-time video communications, online research and the endless flow of information, project/task management tools, specialized software for product development, online learning platforms, online banking, e-commerce, e-books, smart devices, social media networks, artificial intelligence, cloud computing, cryptocurrencies. The digital dimension has unprecedently facilitated and increased productivity, as well as provided opportunities for most businesses and individuals. Opportunities, however, are usually accompanied by threats and vice-versa, and that was not different with the digital dimension.[3] While accessing the internet provides one with a seemingly

[1] Not all indicators are available for all year in all selected countries. The figures presented in this research are always the latest available ones from the selected database for each indicator and its respective country.
[2] No information on the percentage of persons employed using a computer with internet access in the U.S. was available from OECD's statistics pages.
[3] Definitions for *threats* and *opportunity* are provided in section 1.2.1 of this research.

endless range of resources, it also enables other parties to exploit existing vulnerabilities. Before societies had access to computers and the internet, the risks[4] to which individuals and entities were exposed to were primarily health and safety, financial, legal, political, regulatory, economic, reputational, strategic, operational, competition, compliance and technology risks. Nevertheless, no cyber risks existed. Cyber briefly refers to a collection of automated information systems accessible over networks (Bayuk et al, 2012, p.1). Cyber risks, thus, designate the risks that arise from a presence in these networks and information systems.[5]

In the 90's, after the internet became widely available to the public, the rapid spread of viruses, as well as the occurrence of first cyber-attacks[6] gave a hint of the threats that the digital dimension could expose companies and individuals to. Furthermore, the fear that digital means and tools could become a strong ally of terrorism started concerning policy makers. In late 90's and early 2000's, wireless internet was developed and popularized, escalating concerns even more. If in the beginning of the digital era, cyber threats to companies and individuals came mostly from amateur insiders and acquainted persons, nowadays cybercrime[7] has become as professional and profitable as other types of crime.[8] Online scams to steal money, identity and Internet Protocol[9] theft, cyber espionage, denial of service ("DoS")[10] attacks, data breach, phishing,[11] spear phishing,[12] malware,[13] for example, each day become more sophisticated and harmful. (Leeuw and Bergstra, 2007)

By 2020, 1.13 billion malwares had already been identified worldwide, and until July 2021, this number was 1.25 billion. In 2020, 137.7 million new malwares were discovered worldwide, and in 2021, this number already reached 111.8 million by July (AV-TEST Institute, 2021). Moreover, investigations conducted in 2019, found that out of a sample of malwares, 93.60% behaved in a

[4] A definition for *risk* is provided in section 1.2.1 of this research.
[5] Definitions for *cyber* and *cyber risk* are provided and discussed in-depth in section 2.1.1 of this research.
[6] A definition for *cyber-attack* is provided in section 1.4 of this research.
[7] A definition for *cybercrime* is provided in section 1.4 of this research.
[8] Apart from cybercriminals, foreign intelligence entities have also been depicted, at times, as a threat to a peaceful digital environment. In this research, we will not focus on the activities conducted by foreign intelligence entities addressing other countries, or on the strategies and policies developed by countries to defend themselves. Instead, we will concentrate on the threats posed by cybercriminals to private companies and on the mechanisms they utilize to address them.
[9] Internet Protocol refers to the register of a system's address information when it is transferring data across network boundaries (NIST, n.d.-j).
[10] A denial of service is the prevention of authorized access to resources or the delaying of legitimate operations (NIST, n.d.-i).
[11] Phishing refers to a technique for attempting to acquire sensitive data through a fraudulent solicitation in email or on a website, in which the perpetrator disguises itself as a legitimate business or reputable person (NIST, n.d.-m).
[12] Spear phishing refers to a highly personalized modality of phishing directed at specific targets. Differently from conventional phishing attacks that tend to be massive and generic, spear phishing attacks use information about companies and their employees to produce persuasive and realistic messages (National Cyber Security Center, 2021).
[13] A malware is a malicious software, firmware or hardware that is intentionally included or inserted in a system with the objective of causing harm to a computer's normal functioning (NIST, n.d.-k).

polymorphic way, meaning that a vast majority of malwares are able to mutate and develop new versions of themselves in order to escape being detected (Webroot, 2020).

In terms of the harmfulness of cybercrimes, it is usually measured monetarily, and includes the costs to remediate incidents, as well as the costs to recover credibility and reputation. The global average cost of a single data breach, in 2020, was US$ 3.86 million. In 2021, this amount increased to US$ 4.24 million. (IBM, 2021) By 2025, global cybercrime damages are expected to cost annually a total of US$ 10.5 trillion to companies and entities (Cybersecurity Ventures, 2021).

Specifically regarding Finland, in 2019, when inquired about the major cyber threats for their businesses, almost two thirds of the interviewed companies operating in Finland mentioned phishing and malware attacks (*Major cyber security threats of companies in Finland 2019,* 2021). Also in 2019, 91% of interviewed companies stated that they believed that the risk of becoming a victim of cybercrime was increasing (*Perceptions about the development of cybercrime risks in Finland 2019,* 2021). Another survey, conducted in 2020, found that 87% of companies operating in Finland believed that information and cyber risks were significant (*Perception of information and cyber security risks in companies in Finland 2014–2020*, 2021). Finally, information made available by Statista shows that, in 2020, 12,038 information security violations and threats were reported to the Finnish National Cyber Security Center, meaning that there were about 33 reported incidents per day.[14] Among the total number, 4,912 were attempts of or successful scams, 3,771 were attempts of or successful phishing, 980 were attempts of or successful malware invasions, and 805 were data breaches. (*Number of information security violations and threats reported in Finland 2020*, 2021) It is key to highlight that these are only the identified and reported violations. Every year millions of violations at global level are either not detected or not reported to authorities.

The relevance of cyber threats as well as their potential consequences and damages were briefly stressed by the figures presented above. The next step is to consider what to do about these threats. Societies have always attempted to manage all kinds of risks around them. The attempt of making good decisions in the face of uncertainty and risks is probably as ancient as mankind, and evolution seems to have chosen the individuals who have been able to make better use of their reasoning to reduce the uncertainty of resources and protection, even if back then this was eventually attributed to luck or divine power (Kloman, 2009). Naturally, the type, quality, timeliness, suitability and success of these management attempts have varied over time and case. Escape routes were planned for the occasion of natural and engineering disasters; insurances were created for a possible loss of property

[14] In Finnish, *kyberturvallisuuskeskus*. Available at: https://www.kyberturvallisuuskeskus.fi/en/homepage.

or money; legal, political, economic and regulatory advisors were hired to assist governments and companies in making decisions, dealing with stakeholders, and in planning recovery plans for potential economic crisis or political instabilities; compliance officers were hired to make sure policies and norms were enforced and caused no reputational damages to entities and individuals; strategic and operational planning, as well as market analysis were developed.[15]

Similarly, societies understood that the cyber risks, introduced by the digital era, also had to be managed. Managing cyber risks roughly means being able to deal with them and their potential consequences.[16] When dealing with the potential positive consequences of risks, companies, entities and individuals should be ready to identify, increase and take advantage of opportunities in the digital dimension that could improve their performance, capacity, flexibility, or desirable attributes; that could enhance their presence in the digital dimension or that could create value for their businesses (MITRE, 2015b). Whether these positive consequences of risks apply to cyber risks as well is a question that future studies will have to answer.

When dealing with the potential negative consequences of risks, it is important to highlight that they cannot be completely eliminated, they can just be reduced and managed. No matter how hard one would attempt to achieve a zero per cent likelihood of an incident, this figure is unlikely to be achieved as threats also evolve, becoming more complex and evading previously established counter measures. As stated by Bernstein (2012), we can never be certain of a thing, because there will always be ignorance to some extent. In this sense, more important than pondering "if" a risk will materialize or not, is to consider "when" and "how" it could happen, and which consequences it would have. Time and experience have shown that as essential as preventing incidents, is knowing the complete scope of threats, and their characteristics, and being ready to effectively respond to them. (Rothrock and Clarke, 2018)

Information security and cyber security[17] were born as the sciences dedicated to managing risks to information systems and addressing incidents in the cyberspace.[18] Their objective is to protect companies, societies and individuals from cyber-attacks and damages, and to give them control over networked information systems. Together with cyber security and information security were created the cyber security and information security professionals, who received the tasks of managing and

[15] It is important to highlight that these risk management initiatives are described in a very simplistic way with the sole purpose of illustrating the argument. In reality, they are way more complex and sophisticated than the pairs of words used to describe them.
[16] A definition for *cyber risk management* is provided and discussed in-depth in section 2.1.1 of this research.
[17] Definitions for *cyber security* and *information security* are provided in sections 2.1.2 and 2.1.3 of this research.
[18] A definition for *cyberspace* is provided in section 1.4 of this research.

securing information systems, identifying for potential vulnerabilities and threats, addressing their potential consequences and recovering from potential incidents. The success of cyber security and information security controls and cyber security and information security professionals is, thus, measured based on their ability to create a resilient and reliable cyberspace. (Bayuk et al, 2012, p.1)

Cyber security and information security became essential in several spheres of societies. Countries, unions of countries, regional and global organisations started developing their cyber security and information security strategies, policies and standards to guide cyber practices in the governmental and semi-public spheres. At the same time, companies and professionals also started developing their own cyber policies, processes and standards in the private sphere. Furthermore, scholars, researchers and institutions dedicated their time to observe and develop a formal understanding on the theme, and to introduce it into the business and public administration literature and academic discussion. In this context, it is important to add that actions in all these spheres are not expected to be isolated, but concomitant, complementary and guiding to one another.

Initiatives to promote cyber awareness and to make the developed strategies, policies and standards known and assimilated by people became key. A study conducted in 2019 showed that most of the impediments to an effective cyber security implementation in companies operating in Finland were due to negligent users (37%), insufficient knowledge about the cyber domain (33%) and inability to keep staff informed about cyber threats (32%) (*Impediments to effective cyber security implementation in companies in Finland* 2019, 2021).

Considering what has been exposed above, the conclusion is that creating and using strong, comprehensive, reliable and resilient cyber risk management frameworks, standards and processes has proven to be the best way to address cyber risks. It is also the suitable path to make the most out of cyber resources, to protect societies, systems and their information, to gain credibility and trust from employees and stakeholders, and to increase a business revenue and competitive advantage.

## 1.1 Aim of the research and research questions

This research has two objectives. First, to *understand and describe how risk and risk management are understood and approached by private companies operating in the cyber risk field in Finland*. This study is particularly interested in mapping the definitions, methodologies, norms, models and proceedings followed/utilized by companies in Finland when managing the cyber risks that their clients are/may be exposed to. Second, to *understand the current cyber risk management market in Finland and identify its trends.* In this sense, this study wants to understand what kind of methodologies, processes, frameworks and standards are becoming relevant; what kind of

modifications and improvements are being made to cyber risk management approaches; or what kind of innovations are rising. By defining these two objectives, this study wants to describe the current state of cyber risk management practices in Finland, and then, to identify towards where these practices are going.

The research questions of this study are:

1. How do companies operating in the cyber risk field in Finland understand and approach cyber risks and cyber risk management?

2. How companies operating in the cyber risk field in Finland see the current Finnish market?

3. What are the trends that companies operating in the cyber risk field in Finland observe for cyber risk management?

As implied by the objectives and the research questions presented above, this study has some scope limitations. The first one refers to the type of risks that it is dedicated to. As previously stated, there is a wide range of risks that actors need to manage including but not limited to financial, reputational, judicial, political, strategic, and health & safety risks. This study focuses on cyber risks. This choice was made based on the growing relevance of the theme, as previously depicted and on a personal interest for the topic.

The second limitation refers to the group of actors selected as the target of this study: *private companies operating in the cyber risk field in Finland.* For the purposes of this study these companies are defined as private companies that commercialize services or products with the objective of assisting their clients in managing cyber risks. These companies are either Finnish companies operating in the Finnish territory or multinational companies with branches operating in the Finnish territory. They may offer cyber security services, exclusively, or may have a wider catalogue of services, in which cyber security services are included. Moreover, they may be large, small, experienced, or young companies. It is important to highlight that this study is not focused and does not include analyses about governmental entities, hybrid companies, international organisations, non-profit organisations and individuals. This study is also not focused on companies that conduct cyber risk management activities in-house to serve internal clients. Rather, it is limited to companies that serve external clients and whose core businesses are the provision of cyber risk management services or the development of cyber risk management products. This second limitation was moulded based on the availability of resources. It was also motivated by the lack of studies conducted with these delimitations in Finland.

Finally, this study does not have the aim of providing a comprehensive and unified understanding about cyber risk management concepts and practices from all companies operating in the cyber risk field in Finland. It simply aims at mapping the practices and concepts utilized by some companies, and in finding similarities or distinctions among them, as well as between them and the selected theoretical framework. This study also does not aim at providing a forecast about the future of cyber risk management in Finland. It just aims at collecting companies' perceptions on the trends of cyber risk management practices. The ultimate objective of this research is to provide the cyber risk management corporate community and the scientific community with sample information on how cyber risk management theory is meeting cyber risk management practices in Finland, and on the paths that the cyber risk management market is deciding to take in the country.

## 1.2 Background of the research

This research is inserted in the scientific field of risk management and, consequently, relies heavily on the concepts of *risk* and *risk management*. Thus, it is important and useful to present a summary of selected literature and standardization on risk and risk management. We note that the literature on these topics is broad, and that the objective of the following sub-sections is not to present an extensive review and discussion about them. Therefore, only selected literature will be presented and discussed. We note that the relevance, credibility and suitability of sources were considered during the selection.

### 1.2.1 Risk

For decades, authors and institutions have been debating and writing about the conceptualization of risk and its developments. For Rosa (2003), a *risk* is a situation or event that poses humans or something of human value at stake, and whose outcome is uncertain. *Risk* has also been conceptualized as uncertainty about the consequences of an activity and its severity with respect to something that is valued by humans (Aven and Renn, 2009). According to the International Organization for Standardization ("ISO") (2009), a *risk* is the positive or negative effect of uncertainty on objectives. Renn (2009) adds that the positive or the negative characterization depends on the values that organisations associate with the effects. Uncertainty, in turn, is the lack of knowledge and understanding of variables affecting the objectives (ISO, 2009), or the lack of knowledge about whether an event will take place, and if so, what will be its consequences (Aven et al., 2011). It is important to mention that when the level of uncertainty is low or high, it does not necessarily mean that there is a low or high risk, respectively (Aven and Renn, 2009).

In most instances, societies, consulting companies and individuals use the term *risk* to refer exclusively to the negative effects of uncertainty on objectives. These risks that have purely unfavourable outcomes were described by Aven et al. (2011) as pure risks, while risks that allow for both favourable and unfavourable outcomes were categorized as speculative risks. When referring solely to the negative or solely to the positive effects of uncertainty, the terms *threat* and *opportunity* have also been used in the literature, respectively. *Threat* is a circumstance or event with a harmful potential (NIST, n.d.-n). *Opportunity* is a condition or event that may result in a beneficial outcome (NIST, n.d.-l) or a situation where, on balance of probabilities, the net expectation is a favourable outcome (Shortreed, 2009). In this research we employ the term *risk* to designate both negative and positive effects of uncertainty on objectives. The terms *threat* and *opportunity* are, thus, employed to designate only one or another effect.

Scholars and institutions have tried to find ways to express risks, and in general, it has been argued that risks are defined in relation to potential events and their consequences, which would affect an established objective. The metrics of risks, or measurement of risks, have been deemed as essential to create a material and informed discussion about risks, and to facilitate decision making processes by providing a quantitative measure for risk evaluation (Johansen and Rausand, 2014). It is, thus, possible and key to estimate and measure risks. The likelihood that events will occur and that their consequences will unfold is usually how risks are expressed. In this context, likelihood refers to the chance that something will happen based on a measurement methodology defined by the *risk owner*, which is the individual or entity that has authority and responsibility to manage a risk. (ISO, 2009; Renn, 2009)

### 1.2.2 Risk Management

Risk management or enterprise risk management ("ERM") has also been a topic of interest of scholars and institutions in the recent years. Most of the work produced in the field and the standards developed have focused on defining risk management, understanding its origins, differentiating the approaches to risk management, establishing a risk management framework, including a risk management process, and exploring risk management techniques for specific fields.

*Risk management* has been described as a logical approach to uncertainty and a modern alternative to faith and luck, which one day were the only guidance individuals had while dealing with their uncertainties (Kloman, 2009). The core of risk management was also described by Bernstein (2012) as maximizing areas that are somewhat controlled and minimize the areas that are completely out of control, whose causes and effects are unknown. The ISO (2018) defined in its standard 31000:2018

- Risk Management – Guidelines ("ISO 31000"),[19] that risk management as a way to build societies and to conduct businesses in a more productive and prudent way, and as a way to create and protect value. Still according to the ISO (2018), risk management is a package of coordinated activities to direct and control organisations' exposition to risks, and to set strategies, make informed decisions and achieve objectives. It includes both the internal and external contexts to which organisations are exposed to.

It is relevant to notice that organisations tend to focus on managing the threats to their objectives. Nevertheless, the approaches to risk management have been broadened in the recent years, and the number of organisations that are attempting to manage potential opportunities through risk management processes has been increasing (ISO, 2009). Thus, in this research, we employ the term risk management to designate the activities developed by organisations to direct and control their exposition to both threats and opportunities.

In order to develop risk management activities, risk management principles, framework and processes are necessary. The *principles of risk management* establish the features of an effective and efficient risk management. According to them, a risk management should be integrated, structured, comprehensive, customized, inclusive and dynamic, and should consider the best available information, as well as human and cultural factors. A *risk management framework* is a combination of elements that allow organisations to integrate, design, implement, evaluate, monitor and improve their risk management into activities and core functions. These elements include policies, plans and processes. A *risk management policy* sets organisations' purposes related to managing risks. A *risk management plan* defines the resources, approaches, practices, relationships, responsibilities, sequence and timing of activities applied/developed while managing risks. A *risk management process* ("RMP") is the use of risk management policies, plans and practices to communicate and consult shareholders about managing risks, to establish a context with parameters and criteria for managing risks, and to assess, treat, monitor, review, record and report risks. (ISO, 2009; ISO, 2018)

Studies published in the last decade argue that a RMP can be *proactive* and/or *reactive*. Some companies and leaders are not able to anticipate threats before they become a problem and are not able to recognize opportunities that could have been seized way earlier or that were not taken and ceased to exist. A reactive approach to risk management means taking action towards risks when stimulated by their presence. A proactive risk management means thinking in advance about risks and making decisions in their regard before they emerge. ("Proactive vs. Reactive", 2019) The

[19] We highlight that the copyrights of the standards described and cited in this study were duly respected. The access to these standards was legal and the proper acknowledgement to their sources were made whenever they were mentioned.

proactive approach also involves identifying, analysing and evaluating risks, but more than that, it involves using previous experience to prevent negative consequences of risks and to gain confidence to pursue opportunities. In this sense, acquiring consistent knowledge and experience in managing risks and sharing them with team members is key for developing a successful RMP that is not only reactive, but also proactive. (Kerzner, 2014, pp. 318 – 319) A proactive or a reactive approach isolated are not enough to deal with the complexity of risks. A combination of both, however, unites the best of worlds and generates a stronger and more comprehensive RMP.

RMPs are understood and conducted differently by organisations, especially if we consider their specific market niches. Still, the risk management cyclic nature and division into phases seem to be common features of most processes. Gustav Hamilton was the first one to develop the concept of risk management cycle, in mid-1970's, and to divide it into phases, including assessment, control and communication (Kloman, 2009). More recently, in 2009, the ISO has proposed a standard for risk management, by compiling and incorporating the best practices from the leading risk management standards, such as the Committee of Sponsoring Organizations of the Treadway Commission's Enterprise Risk Management — Integrated Framework ("COSO"), the Project Management Institute ("PMI") Practice Standard for Project Risk Management, and the Australian New Zealand Risk Management Standard ("AS/NZS 4360:2004") (Shortreed, 2009). The ISO standard also treated the RMP as a cycle and divided it into phases: risk assessment, treatment, monitoring, reviewing, communicating, reporting and registering. (ISO, 2018) The ISO standard has, since then, been used as a guide for several entities in their RMPs (Renn, 2009). In 2018, the ISO published an edited version of its risk management standard, which substituted the original one published in 2009.

Before taking the first step in managing risks, the ISO proposes that organisations should conduct a pre-assessment and define a scope, a context and a set of criteria in order to customize the RMP and enable the development of adequate risk assessment and treatment. The scope involves tools, resources, responsibilities, relationships and expected outcomes, for example. The context involves understanding the organisation's objectives and activities, defining the organisation's risk environment, and assessing the organisational factors that may be risk sources. The criteria consider the amount and type of risk that an organisation is willing to take relative to its objectives, the significance of these risks and ways to define and measure consequences and likelihood of events. The scope, context and criteria should be constantly reviewed and amended throughout the whole RMP. (ISO, 2009; ISO, 2018; Shortreed, 2009)

The first phase of the RMP is the *risk assessment.* It refers to finding and studying risks and their sources, assessing the organisation's exposure or vulnerability to risks, and making an estimation

about risks, considering the likelihood of events and the potential severity of consequences. According to Renn (2005), the core of risk assessment relies on the systematic use of analytical methods and tools. The risk assessment phase can be divided into the subphases of risk identification, risk analysis and risk evaluation. (ISO, 2009; ISO, 2018)

The first subphase, *risk identification*, refers to finding and describing risks, their sources, causes, events and potential consequences, based on historical data, expert's input, theoretical review or a combination of techniques. Risks should be identified even if their sources are not controlled by the organisation. (ISO, 2009; ISO, 2018)

The second subphase, *risk analysis or risk characterization*, refers to understanding the nature of the identified risk, judging its severity and determining its level. It involves a meticulous study about uncertainties, risk sources, events, consequences, likelihood, scenarios and controls. The analysis can be qualitative, quantitative or a mix of both. A risk matrix, which is a tool for classifying risk by defining ranges for the severity of its consequences and their respective likelihood, can be used in the process. The level of a risk is, thus, calculated and expressed in terms of the combination of the severity of its consequences and their likelihood. These two variables are independently classified either as very low (1), low (2), medium (3), high (4) or very high (5). (ISO, 2009; ISO, 2018; Renn, 2009) Traditionally, the risk matrix is used to analyse threats.

MITRE (2015a), a not-for-profit organisation, adds that apart from risk matrixes, several other risk management techniques can be useful while assessing the likelihood of events and outcomes. The Monte Carlo probabilistic simulations are one of them. Monte Carlo is a term utilized to refer to a process of modelling and simulating a system affected by randomness. Some scenarios are generated and statistics are used to understand the value of assets and information, and to guide decision making processes. (Brandimarte, 2014, p. 3)

The third subphase, *risk evaluation*, refers to comparing the identified risks with the criteria defined for risks, in order to decide if they are wanted, acceptable or tolerable. In this context, *acceptable* refers to a situation where the risks are so low that additional efforts for treating the risk are not needed. *Tolerable*, in turn, refers to a situation or activity that is worth pursuing, but that demands initiatives to reduce the risks within the necessary limits. The results of a risk evaluation will depend on the *risk perception* of organisations, which will vary according to the established context for the RMP. They will also depend on an organisation's judgement and subsequential decision on pursuing, taking or avoiding risks *(risk attitude)*, on the quantity and the kind of risks that an organisation would be ready to pursue and take *(risk appetite)*, and on an organisation's willingness to take and withstand risks *(risk tolerance)*. If a risk is deemed tolerable, actions should be designed and implemented to

make it acceptable in the future. As a result of a risk evaluation, organisations will consider treatment options, maintain the *status quo* and/or reconsider objectives, for example. (ISO, 2009; ISO, 2018; Renn, 2009)

MITRE (2015a) suggests in their *Systems Engineering Guide for Risk Management* that between risk assessment and risk treatment, another phase should take place: *risk prioritization*. Though the focus of the document lies in engineering projects, this step could be replicated in different RMPs. In the risk prioritization phase, the assessed risks should be processed to generate a ranking of criticality, from the most to the least critical risk. This way, organisations could prioritize which risks deserve immediate treatment and bigger allocation of resources, and which risks can be treated with less urgency and less resources.

After the risk assessment is done, the *risk treatment* starts. The main objective of this phase is to enhance the likelihood of positive consequences and reduce the likelihood of negative consequences to acceptable or tolerable levels (Shortreed, 2009). Options are selected and implemented to address and modify an assessed risk to create value. These options are themselves assessed, evaluated and chosen by the organisation and stakeholders, based on the risk analysis and evaluation, and on each option's expected efficiency, effectiveness, minimalization of side effects, sustainability, fairness, political and legal implementability, and ethical adequacy. The options include the following *risk controls*: avoiding a risk by interrupting or not engaging in an activity that generates or could generate this risk and/or removing the risk source *(risk avoidance)*, decreasing the likelihood or changing the consequences of risks *(risk reduction* or *risk limitation)*, increasing a risk to seize an opportunity *(risk increase* or *risk exploitation)*, accepting a risk and its potential benefit or burden *(risk acceptance, risk retention or risk assumption)*, observing a risk to detect changes in its nature and potential consequences (*risk watching*), and sharing a risk with other parties through contracts or insurance *(risk transfer or risk sharing)*. (ISO, 2009; ISO, 2018; Renn, 2009; MITRE; 2015b; McShane, 2018)

When considering threats, for risks with very low (1), low (2) or medium (3) severity of consequences and likelihood, risk retention or risk watching could be, hypothetically, the most adequate treatment options. For risks with very high (5) or high (4) severity of consequences and likelihood, risk avoidance, risk transfer or risk reduction could suit better as treatment options. When considering opportunities, for risks with very low (1), low (2) or medium (3) intensity of consequences and likelihood, risk watching or risk increase could be adequate treatment options. For risks with very high (5) or high (4) intensity of consequences and likelihood, risk retention would, hypothetically, be the most adequate treatment.

Once a treatment is chosen, a risk treatment plan should be developed. This plan should include, for example, an explanation about the proposed treatments and why they are adequate, a statement about the expected benefits arising from the treatments, a description of the people responsible for implementing the treatments and the necessary resources, and a chronogram of the treatments' phases. The implementation of the selected risk treatment options, or at least, the supervision of this implementation, if it is conducted by a third party, is a responsibility of the organisation conducting the RMP. (ISO, 2009; ISO, 2018; Renn, 2009)

It is relevant to notice that when dealing exclusively with threats, the risk treatment has frequently received the following alternative names in the work of scholars or in the daily practices of organisations: *risk mitigation*, *risk elimination* or *risk reduction*. (ISO, 2009; ISO, 2018)

Throughout the whole risk management cycle, it is recommended that *risk monitoring* and *risk reviewing* are conducted in a continual basis. The status of risks is checked and observed in order to detect changes in old risks or to detect new risks, which could have been unintendedly created by an implemented risk treatment option. Also, a revaluation of risk controls taken in the past is conducted to determine if their effects are suitable and effective in relation to stablished objectives. *Risk reporting* and *risk registering* are generally perceived as important steps and are also conducted along the whole risk management cycle. As a result, risks, their assessment, selected treatment, monitoring and reviewing are communicated to stakeholders and across the organisation, and are officially recorded to keep the RMP decisions traceable, and to assure their availability as future reference. (ISO, 2009; ISO, 2018; Shortreed, 2009)

The ISO also proposed that the RMP should include activities of communication and consulting throughout all its phases. This means that organisations should inform stakeholders about the RMP, should help them understand the risks and the available treatment options and should seek for their feedback while taking risk management decisions. (ISO, 2009; ISO, 2018) According to Renn (2009), the benefits of this dialogue with stakeholders depends on the quality of the communication processes. These, as argued by the author, should be designed so that stakeholders are engaged and encouraged to contribute to the process, and to improve the quality of the final products of risk management. Renn also defends the importance of the communication between risk professionals, so that they can exchange information and improve overall management.

As previously stated, the RMP is generally understood as a continuous cycle, and as soon as the last phase is over, the first one restarts once again. The phases of the RMP usually follow a logical sequence, as the one presented is this section, but they may be eventually conducted in a different order depending on a variety of factors and circumstances affecting the organisation. (Renn, 2009)

Occasionally, an independent *risk management audit* may be conducted to investigate whether an organisation has been applying a risk management framework and process effectively, and has been properly addressing and managing risks. (ISO, 2009) In this sense, it is relevant to notice that organisations can always count on the help of experts to assist them in the development of risk management activities.

## 1.3 Risk management in the cyber dimension: previous studies

Already in the late 1970s, Madnick (1978) published an article stating that an effective computer security could only be achieved when combined with management policies and procedures. In the 1980's and 1990's a risk-based approach to information systems and computers was addressed by academics, but in a very fragmented way (McShane, Eling and Trung, 2021). Later, in the beginning of the 21st century, several studies involving the cyber and risk management domains started appearing. Blakley, McDermott and Geer (2001) argued that most information security programmes neglected important aspects of risk management processes, and that information security should, thus, be transformed into information risk management. Siegel (2002) and Gordon (2003) proposed cyber risk management frameworks, which, for the first time, discussed an action towards cyber risk apart from the traditional and technical response of risk mitigation. They proposed risk transfer, an insurance approach, as a possible response to cyber risk. Collier, Linkov and Lambert (2013) stated that cyber security should not only be composed of technical issues, but also of social and economic analyses. Falco et al (2019) argue that advancements in the cyber risk science can only be made with the combination of efforts from computer science, behavioural science, economics, law, management and political science.

Siponen and Oinas-Kukkonen (2007) reviewed information security studies developed in the 2000's and found that most of them presented no interdisciplinarity with the risk management field. McShane, Eling and Trung (2021) state that even after several attempts to bring the cyber domain closer to management and economic views, the technical ones remain stronger. The result is that cyber studies usually lack this essential social interdisciplinarity.

Apart from the themes and studies mentioned above, since the 1980's several studies were conducted about a specific phase of cyber risk management. Cyber risk identification studies focused, for example, on describing worm attack, on finding ways to identify new types of cyber risks more effectively, on investigating the degree of awareness and qualification that companies had to identify cyber risks, or on developing a consistent way to catalogue cyber risks. Cyber risk analysis studies investigated, for example, ways to measure the likelihood and the impacts of cyber risks and

cyberattacks; or described the relationship between decrease of consumer spending or shareholders' trust after a cyber incident; or investigated characteristics of organisations that make them more or less susceptible to cyberattacks. Cyber risk treatment studies investigated possible ways to avoid, mitigate, or transfer risk, as well as the correlation between firm's cash holdings and risk retention. (McShane, Eling and Trung, 2021)

Specifically regarding this study, no research was found to link cyber phenomena, risk management and the Finnish private sector.

## 1.4 Central concepts and definitions

In this subsection of the introductory chapter, the central concepts of the research will be listed and defined. It is important to note that most of these concepts have several different definitions among literature and standards. The objective of this section is not to present an extensive analysis about all definitions and interpretations of the selected concepts. Its sole aim is to make the reader familiarized with the central concepts of this research and their meaning in its context. Thus, only a few definitions and interpretations will be presented. The selection of the definitions and interpretation was made in accordance with the credibility of their sources and with their compatibility with this research. We highlight that some concepts and definitions relating to risk and risk management were already explained in section 1.2 or will be explained in section 2.1 of this research. Thus, they will not be repeated in this section.

*Cyber*

As previously mentioned, *cyber* refers to a collection of automated electronic systems accessible over networks (Bayuk et al, 2012, p.1). It is usually used as a prefix that is aggregated to other words to associated them with information and communication networks (NIST, n.d.-a).

*Cyberspace*

The term refers to the interdependent network of information technology infrastructure, which includes telecommunication networks, computer systems with their processors and controllers, and the internet (NIST, n.d.-g).

Cyberspace also refers to the fifth physical domain in which mankind can operate, apart from land, sea, aerospace and outer space. It is the domain which has as a distinctive characteristic the use of electronics to create, use, share, store, and modify information via interdependent and interconnected networks accessible through information-communication technologies. (Kuehl, 2009, pp. 25, 28)

*Cyber threat*

The term designates circumstances or events with the potential to adversely impact entities' operations, assets and professionals via an unauthorized access to an information system. A cyber threat is also the potential cause of a cyber incident. (NIST, n.d.-h)

*Cyber incident*

The term refers to the result of the unduly use of an information system and/or network, which causes actual or potential damage to this system and/or network or to the information they contain (NIST, n.d.-c).

*Cyber-attack*

The term designates an attack that targets entities' and individuals' use of the cyberspace to steal confidential information or to disrupt, disable, destroy or maliciously control a computer environment or infrastructure, as well as their data or information (NIST, n.d.-b).

*Cybercrime*

The term refers to all crime that happens in networked information systems or through them. They can be divided into cyber-dependent crimes, which are directed at networked information systems, such as disruption of systems, damage to data and, computer invasion; and cyber-enabled crimes, which utilize networked information systems for committing a crime, but are not directed at them, such as online money laundering and drug trafficking. (Police of Finland, 2021)

*Cyber resiliency*

The term refers to the ability to anticipate, withstand, recover from and adapt to adverse conditions and stresses on systems, which are powered by cyber resources (NIST, n.d.-d).

*Information systems*

The term designates a combination of technology-intensive resources (supercomputers, personal computers, cell phones, telecommunication systems, and production control systems, for example) utilized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. It also designates all other variables that affect these resources, such as people, processes, facilities, and the cyberspace. (NIST, 2011)

*Stakeholder*

The term refers to an individual or an organisation that can affect or be affected, or that perceive themselves as affected by a decision or activity taken or conducted by a third party. This individual or organisation is, thus, a *stakeholder* of the third party. (ISO, 2009)

*Trend*

The term is defined as the (1) movement in one direction of the values of a variable over a period of time or (2) the term used to describe a research outcome that, if it were stronger, would be statically significant – but it is not (Vogt and Johnson, 2015). The Merriam-Webster dictionary (n.d.) states that a *trend* is (1a) a prevailing tendency or inclination; (1b) a general movement; (1c) a current style or preference; (1d) a line of development; (2) the general movement of a statistically detectable change and (3) a line of general direction or movement.

*Vulnerability*

The term refers to a weakness in an information system, in the system security implementation, procedures or internal controls that could be exploited by a threat source (NIST, 2011).

## 1.5 Research methods

The success of a study is greatly dependent on the appropriate choice of the methodological tools to be employed. In order to make a decision in this regard, the researcher needs to consider which is the methodological tool and the specific method that meet the objectives of the study and that is able to provide adequate answer to the research questions. (Liu, 2017, p. 1511) To meet the objectives of this study and to answer the research questions listed in section 1.1, a qualitative research methodology was selected. Moreover, semi-structured interviews were chosen as the specific method to develop this qualitative study.

Qualitative research is a way of describing, understanding and interpreting a complex phenomenon in a holistic way by digging deep into participants' experience and knowledge about them (Eriksson and Kovalainen, 2008, p. 5). It is also a way of investigating the meanings that individuals and groups assign to social and human problems (Creswell, 2007, p. 36). The qualitative research was deemed as the most adequate methodology for this study, since the research questions defined in this study are quite complex and are impacted by several aspects and variables at the same time. Besides that, the objectives of this study are directly connected to the experiences and meanings created by a group (private companies operating in the cyber risk field in Finland*)* in relation to a social problem, which, in this case, is the incorporation of risk management activities into their businesses.

In qualitative research, the study of the defined social problem usually relies on primary data that is collected among the targeted individuals and groups or on secondary data that has been collected by someone else (Creswell, 2007, p. 37). Since no secondary data was available to answer the research questions of this study, primary data collection was necessary.

Interviews are a widely used tool in qualitative research and they were defined as a suitable method for the data collection of this study. Specifically, guided and semi-structured interviews were conducted. This type of interview allows the researcher to list the main topics they want to discuss with the participant, and to prepare open questions in advance, but also allows the researcher and the interviewee to ask and answer with a great degree of flexibility and informality. It provides participants with the possibility of elaborating more in-depth and comprehensive answers, of justifying their answers, and of raising interesting aspects not addressed by the pre-prepared questions. (Eriksson and Kovalainen, 2008, p. 82)

Due to health restrictions posed by the Covid-19 pandemics, the interviews for this study were conducted synchronously via video call or asynchronously via e-mail, depending on the availability and on the requirements of the participants.

More details about the methodology and the results for this study are provided in sections 3 and 4. The interview questionnaire utilized to guide the semi-structured interviews is reproduced in the Appendix 1 of this study.

## 1.6 Organisation of the research

This research is organized and presented in five parts that follow a logical sequence. Section 1 explains the topic of this research and its relevance, as well as the purpose of the study, its research questions and delimitations. It also provides a summary of the background literature for this research, and definitions about its central concepts. Section 2 is the theoretical part of the research. It presents and discusses different cyber risk management processes, standards and frameworks, and places this study into the cyber risk management research map. It also discusses cyber risk management definitions, products, services, and trends. Section 3 explains the methodology of the research's empirical part. Details about the design, reliability and validity of the research are provided to the reader. Moreover, the collection, handling and analysis design of data are discussed. A critical view of the limitations of the data collection is also included. Section 4 describes the data and presents the results derived from them. Section 5 provides interpretation about the results, discussing how they answers the research questions. Section 5 also highlights and discusses the limitations of the research results and opines on further investigation to be made in connection with the topic and the research questions.

# 2 CYBER RISK MANAGEMENT

The introduction of this study explained and exemplified the breadth of the cyber dimension, as well as the threats and opportunities enabled by and/or directed to it. The introduction also advocated towards the relevance and importance of cyber activities in all social spheres, especially professional and business relationships. The general concepts of risk and risk management were, then, introduced and briefly discussed. A preliminary analysis of previous studies conducted combining risk management and cyber phenomena was presented. In this section, risk management and cyber will be deeply melded and jointly studied. This section's main objective is to review and analyse relevant definitions, processes, standards and frameworks to risk and risk management from the cyber perspective, as a way to create basis, support, guidance and justification for this research and its research questions.

The first subsection will present the definitions and understandings of risk and risk management from the cyber perspective. The second subsection will dedicate to review and analyse cyber risk management processes, standards and frameworks developed and/or recommended by reputed authors and institutions, and recognized by the international scientific community as best practices. The third subsection will present and explain what the main cyber risk management services and products are, and will describe some of their remarkable characteristics. The fourth subsection will review literature, standards and strategies to list and debate cyber risk management trends or risk management trends and their applicability in cyber risk management field. Finally, the fifth subsection will place the current study into the cyber risk management research map.

## 2.1 Definitions and terminologies

In sections 1.2.1 and 1.2.2 of this study two terms that are the core of this research, *risk* and *risk management*, were introduced, defined and discussed. In this section we want to revisit these definitions and discussions to bring a different and specific point of view. This subsection aims at exploring the cyber definitions for *risk* and *risk management* and the meanings that these two broad concepts have for authors and institutions dedicated to the study of cyber phenomena.

### 2.1.1 Cyber risk and cyber risk management

A risk associated with the cyber environment is denominated *cyber risk*. The term cyber risk reflects an uncertainty on or within objectives linked to *information and technology systems*. These objectives can be, for example, keeping a cyberspace protected, reliable and resilient, and making sure its information is confidential, integral and available. (NIST, n.d.-e) Refsdal, Solhaug, and Stølen (2015)

divide cyber risks into malicious exclusively, such as malwares, DoS and phishing attacks; non-malicious exclusively, such as human error leading to data breaches or technological failures; and both malicious and non-malicious, such as unauthorized access to information systems, which could be either accidental or the result of hacker activity.

Cyber risk is typically employed to designate the negative effects of uncertainty on objectives, including financial loss, operational disruption or adverse impacts arising from unauthorized access, use, disclosure, disruption, modification, or destruction of a system or its information (NIST, n.d.-e). The definitions of risk presented in section 1.2.1 stated that risks can have a positive or a negative effect. Definitions of cyber risk typically only include the negative effects of uncertainty on objectives linked to information and technology systems. Nevertheless, future research could investigate if cyber risks can also cause positive effects such as saving money and resources while conducting cyber activities, changing cyber policies and updating technologies. (McShane, Eling and Trung, 2021)

Risk management specifically dedicated to cyber risks is denominated *cyber risk management*. Cyber risk management is a set of coordinated actions taken to identify, assess, and respond to cyber risks (Petrenko, 2019, p. 145). It is also a mean to approach and achieve cyber resilience and cyber security (Petrenko, 2019, p. 142). Cyber resilience, in this sense, means being able to absorb, withstand and quickly adapt to shocks and adverse conditions that could compromise information and technology systems and their respective information. It also means being able to minimize consequences and reduce potential negative outcomes (Petrenko, 2019, p. 2).

In the context of cyber risks, it is also essential to present definitions of and a brief discussion about other key concepts employed in the cyber domain, which frequently appear in the literature associated with the present study: *cyber security risk*, *information security risk, cyber security management and information security risk management*.

### 2.1.2 Cyber security risk and cyber security management

Cyber security is described as an ability to control the access to *systems* that are interconnected through networks, as well as the *information* contained in these systems (Bayuk et al, 2012, p.1). It is also the process of protecting information and the cyberspace by preventing, detecting, and responding to cyber-attacks (NIST, n.d.-f). Finally, cyber security is also described as the desired end state in which the cyber environment can be trusted and its functioning is secured (Finnish Ministry of Defence, 2019).

Cyber security aims at preventing cyber incidents that could compromise systems and their respective information, at detecting and responding to cyber threats and incidents effectively in case they

materialize, and at successfully recovering from them. In order to successfully achieve its objectives, a cyber security strategy needs to have the right means and mechanisms in place. (Bayuk et al, 2012, p.2-3)

The means usually refer to people, processes and technology, which should be concomitantly and not independently used. People need to be informed, trained and qualified to deal with cyber risks and cyber-attacks. This applies not only to cyber security or IT professionals, but to all individuals, professionals and stakeholders of companies and institutions. Also, cyber security processes and routines need to be developed and followed by them. Plus, up to date and suitable technologies need to be employed in the daily activities of companies and entities, and in dealing with cyber threats and incidents. (Bayuk et al, 2012, p.2-3)

The mechanisms through which cyber security objectives are achieved are usually referred to as confidentiality, integrity and availability, also known as the CIA triad. The concept of the CIA triad was originally developed in the field of information security, and it refers to all kinds of information, including digital data and information addressed and managed by cyber security activities. Confidentiality refers to keeping the information of a system protected and only accessible to the authorized individuals. Integrity means maintaining the information of a system authentic and intact. Availability refers to the ability of providing information of a system or making a system operational in a timely manner. (Bayuk et al, 2012, p.2-3)

In conclusion, cyber security designates a method to use people, processes and technologies to prevent, detect, respond to and recover from cyber threats and incidents that pose dangers to the confidentiality, integrity and availability of data and information in the cyberspace (Bayuk et al, 2012, p.3). *Cyber security risks*, thus, are those that reflect uncertainties towards cyber security.

The term *cyber security management* has been, at times, interchangeably employed with cyber risk management to designate a management process that is focused on cyber matters. The cycle of cyber security management, however, involves identifying not only risks and vulnerabilities, but also cyber incidents. It also involves remediating and recovering from them, as well as monitoring their progression and regression. Based on the effectiveness of cyber security risk response actions and on the evolution of threats and incidents, amendments can be done to the original strategies and the processes will restart. (Bayuk et al, 2012, p.12).

The American National Institute of Standards and Technology ("NIST") developed a Cybersecurity Framework, published in 2018, in which they explore five functions or phases of an effective cybersecurity approach. The first phase is identification, and it refers to understanding the business

context and conducting risk assessment. The second phase is protection, and it refers to creating and implementing the proper safeguards to information systems. The third phase is detection, and it refers to developing and implementing tools to identify cyber security incidents. The fourth phase is response, and it refers to developing and implementing responses to a detected cyber security incident. The last phase is recovery, and it refers to developing and implementing actions to maintain plans for resilience and business continuity, and to restore capabilities or assets affected by the incident. (NIST, 2018, pp. 7-8)

A proactive approach to cyber security management involves the three most common means of a cyber security strategy: people, processes and technology. People, clients and stakeholders need to be educated on the matter and their levels of education should advance over time. In the medium or long run, this initiative should be transformed into cyber security processes and into a single cyber security culture. From the technology perspective, vulnerabilities of systems need always to be scanned for threats, as well as uncommon features and traffic, so that a panoramic view of threats is created employing a risk-oriented approach (Petrenko, 2019, p. 31).

Though always treated exclusively as threats by authors and institutions, there is a possibility that cyber security risks could also be seen as opportunities to improve, protect and empower systems and businesses. More research on the theme would be needed to confirm this hypothesis.

### 2.1.3 Information security risk and information security risk management

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability (NIST, 2011). It is also the level of confidentiality, integrity and availability of information with respect to an asset, a data source, systems, and processes (Bayuk, 2007).

As previously seen in section 1.4, information systems are a combination of technology-intensive resources, and all other variables that affect these resources, which are utilized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. They are constantly exposed to threats that have the potential to compromise the confidentiality, integrity and the availability of information and adversely affect an organisation's businesses. *Information security risks*, thus, are risks to an organisation's operations, assets and individuals due to an unduly penetration to information systems. (NIST, 2011; NIST, 2012) These risks usually deal with the notions of threat, vulnerability and impact. (Talabis, Martin, and Wheeler, 2013).

*Information security risk management* refers to a set of coordinated activities to direct and control an organisation regarding information security risk. In this context, *information security management*

*system* (“ISMS”) are the policies, procedures, guidelines and resources managed by an organisation with the objective of protecting information assets. (ISO/IEC, 2018a; Calder and Watkins, 2019) The NIST states that an effective information security risk management demands organisations to operate in interconnected environments utilizing advanced and legacy information systems. The same entity also highlights that managing information security risks is a complex, multifaceted and non-exact science, because it involves compiling and combining the best judgements of professionals from all levels of the organisation. (NIST, 2011)

Though always treated exclusively as threats by authors and institutions, once again, there is a possibility that information security risks could also be opportunities to improve, protect and empower systems and businesses. More research on the theme would be needed to confirm this hypothesis.

### 2.1.4 Brief terminology comparison and discussion

Analysing the six definitions provided above, it is possible to infer that they are all intersecting each other and dealing with a common concept, *information systems*, and a common problem, the necessity to protect (and optimize) these systems and their respective information, as well as to manage the risks to them.

The most notable differences in the definitions presented in sections 2.1.1, 2.1.2 and 2.1.3 seems to be that cyber risk and cyber risk management tend to deal with both *information systems* and *technology systems* located in the cyberspace, while information security and information security risk management focuses on *information* or *information systems* located or not in the cyberspace. Also, cyber security and cyber security management tend to deal not only with risks, threats and vulnerabilities, but also incident management and recovery plans.

As stated by McShane, Eling and Trung (2021), since the 1970s, cyber research has employed several different names to designate its object of study, among them computer security, information security, cyber security, information security management and cyber security management. According to the same authors, the wide array of terminologies in the field motivated the publication of several papers trying to reduce the semantic variety that caused confusion to many.

For von Solms and Van Niekerk (2013) and Refsdal, Solhaug, and Stølen (2015) there is a difference between information security and cyber security. While information security applies exclusively to information assets, stored or not in the cyberspace, cyber security applies to information and noninformation assets (individuals or objects), as well as infrastructures that are accessible and manipulable through the cyberspace. We note that our understanding is that cyber risks can affect

information assets in information systems or noninformation assets linked to technology systems, accessible through the cyberspace.

In this study, we opted to utilize the term cyber risk management to explicitly convey the idea that cyber risks are being managed by a risk management process. According to McShane, Eling and Trung (2021), cyber risk management is the newest name adopted in cyber studies, and it is employed to bring together both technical and management dimensions, which are equally needed when tackling cyber risks.

## 2.2 Processes, standards and frameworks

In section 1.2.2 the *principles of risk management*, as well as the concepts of *risk management framework* and *risk management policy* were introduced and briefly explained. Also, the concept of *risk management process* was presented, and its phases were thoroughly described and discussed. Several standards and guidelines prepared by different institutions and authors, with special credit to the ISO 31000, were combined to provide a rich and comprehensive view on the steps, characteristics and variables of an effective and efficient RMP that reflects international best practices.

The analysis in section 1.2.2 was a generalist one and did not focus on any specific industry or field. Rather, it described and discussed risk management procedures and techniques that are widely used and adapted by a variety of businesses, including cyber businesses.

The objective of this subsection is to understand what kind of risk management processes, standards, and frameworks are being followed or used as inspiration in the cyber world. This section wants to investigate to which extent generalist risk management processes, standards and methodologies are adapted, followed or utilized as inspiration in the cyber industry, and which specificities need to be considered. This section also wants to understand and briefly describe which are the specific processes, standards and frameworks that influence and/or are employed by cyber risk professionals in their daily tasks or in the development of their own risk management processes and frameworks. For this purpose, this section will review selected existing literature that deals with cyber risk management to find out the processes, standards and frameworks that they have developed or that they cite, analyse and recommend. We highlight that not all processes, standards and frameworks will be mentioned and thoroughly described due to restrictions in length and in the objectives of this study.

It is important to state that the copyrights of all mentioned standards were duly respected during the conduction of this study. The access to the standards was legal and the proper acknowledgement to their sources were made whenever they were mentioned.

### 2.2.1 Background

Cyber risk management processes, standards and frameworks are developed and constantly improved with the objective of providing trustworthy and quality guidance to managers and technical experts throughout their cyber risk management ventures. Standards and frameworks recommend or make specific cyber risk management processes and methodologies biding to organisations. They also suggest or enforce the most adequate steps, tools and methods to deal with cyber risks.

Most standards and frameworks are relatively new in the cyber scene. They mostly belong to or were adapted from two sources: generalist risk management standards, such as the AS/NZS 4360:2004 and the ISO 31000, both previously mentioned and/or described in section 1.2.2; and cyber security, information security and business continuity frameworks and standards, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework ("OCTAVE"), the Information Systems Audit and Control Association's ("ISACA") Risk IT Framework, NIST Special Publication 800-39 – Managing Information Security Risk ("NIST SP 800-39"), the NIST Special Publication 800-30 – Guide for Conducting Risk Assessments ("NIST SP 800-30"), the Canadian government's Guide to Security Risk Management for Information Technology Systems ("MG-2"), the British Standards Institutions BS 7799-3:2006 – Information security management systems- Guidelines for information security risk management ("BS 7799-3:2006"), the Risk Managements Insight's FAIR Framework, the ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements ("ISO/IEC 27001"), the ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls ("ISO/IEC 27002"), the ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management ("ISO/IEC 27005"), the ISO 22300:2021 – Security and resilience – Vocabulary ("ISO 22300"), among others. (Petrenko, 2019, p. 142; Talabis, Martin, and Wheeler, 2013).

At this point, this study would like to briefly comment about some of the ISO/IEC standards from the 2700 family mentioned above, which are all dedicated to information security. The ISO/IEC 27001 is one of the most widely adopted risk-based security standards worldwide, whose objective is to establish the ground for the development of an effective ISMS. The ISO/IEC 27001 specifies a series of auditable requirements that, if followed, allow an organisation to be certified. It determines that organisations must choose and utilize a risk assessment methodology to identify assets and asset owners, vulnerabilities, threats and risks, as well as to analyse and evaluate these risks. It also determines that organisations should apply information security controls. In order to achieve these requirements, the ISO/IEC 27001 suggests that organisations should follow the guidance provided

by the ISO/IEC 27005 and by the ISO/IEC 27002. These documents are codes of practices that drive organisations towards best practices without setting any requirements themselves. (Talabis, Martin, and Wheeler, 2013; Calder and Watkins, 2019)

In the upcoming sections, phases, features and components of the cyber and information security risk management processes described by the OCTAVE framework, the NIST SP 800-39, the NIST SP 800-30, and the ISO/IEC 27005 will be jointly presented and discussed. Selected cyber risk literature will also be presented whenever they dialogue with the content of standards and frameworks, agreeing, disagreeing or bringing a different point of view. Instead of creating subsections for each of these standards and frameworks, this study has decided to mix their contents by creating thematic subsections for the phases and the components that they describe. We selected the information security standards and frameworks described in the following subsections among the major ones. We also considered which of them were the best fits for this study's objectives and delimitations. Standards, processes and frameworks referring to cyber security management were not included in this section because they deal not only with risks and threats, but also cyber incidents, cyber incident management, recovery plans and business continuity strategies. As previously stated, this study is specifically interested in the risk and risk management understandings and approaches of cyber businesses. Nevertheless, a brief description of cyber security processes and frameworks can be found in section 2.1.2.

The *OCTAVE* framework, published in a technical report in June 1999, was created by the Software Engineering Institute at the Carnegie Mellon University to allow organisations to manage information security risks. (Alberts et al, 1999, vii) It is a highly regarded framework among the scientific community despite its complexity. There are three different versions of the OCTAVE, the original one designed for large organisations, one designed for small organisation, and one newer optimized version, which focuses on risk assessment and demands less resources ("OCTAVE Allegro"). In this study we describe parts of the original OCTAVE framework and parts of the OCTAVE Allegro. (Talabis, Martin, and Wheeler, 2013)

The *NIST SP 800-39*, published in March 2011, is one of the standards guiding information security risk management processes (NIST, 2011). The *NIST SP 800-30* was published in September 2012 as a complementation to NIST SP 800-39. It dedicates specifically to describe how to prepare, conduct and maintain an information security risk assessment, one of the phases of the information security risk management (NIST, 2012).

The ISO/IEC 27005:2018 was published by the ISO and the International Electrotechnical Commission ("IEC") in 2018. It provides guidance for conducting information security risk

management and serves as support for the general concepts presented by ISO/IEC 27001:2013. The main objective of the document is to assist organisations in the implementation of information security based on a risk management approach. (ISO/IEC, 2018b)

As noticeable, the abovementioned standards and frameworks dedicate specifically to the management of information security risks. According to what was discussed in section 2.1, cyber risks and information security risks deal roughly with the same concepts, which allows managers to look at these standards for guidance.

We highlight that in the following subsections we will mostly address cyber risks and information security risks simply as "risks".

### 2.2.2 Introduction to cyber risk management phases

The NIST SP 800-39 states that an organisation and its professionals should be able to holistically address risks that are both strategic and tactical ones. In order to do so, they should implement a cyclic information security risk management process ("ISRMP"), which would develop a better understanding of information security risks affecting the organisation's assets, operations and individuals (NIST, 2011). This ISRMP should be comprised of four different components/phases: *risk framing*, *risk assessment*, *risk response* and *risk monitoring*.

Alberts et al (1999, p. 2) also states that organisations should be able to make decisions based on identified risks to the confidentiality, integrity and availability of information assets. In order to do so, they should follow the OCTAVE framework to manage information security risks. This framework would be comprised of three phases: *building of enterprise-wide security requirements*, *identification of infrastructure vulnerability*, and *determination of security risk management strategy and plans*. OCTAVE Allegro proposes eight steps for assessing a risk: *establishment of risk measurement criteria*, *development of an information asset profile*, *identification of information asset containers*, *identification of areas of concern*, *identification of threat scenarios*, *identification of risks*, *analysis of risks* and *selection of mitigation approach*. (Talabis, Martin, and Wheeler, 2013)

The ISO/IEC (2018b) divides the ISRMP into the following phases: *context establishment*, *risk assessment*, subdivided into *risk identification*, *risk analysis* and *risk evaluation*, *risk treatment*, *risk acceptance, risk communication*, and *risk monitoring and review.* We note that this division of phases is very similar to the one proposed by the ISO 31000, discussed in section 1.2.2, which focuses on general risk management.

Refsdal, Solhaug, and Stølen (2015) state that the main objectives of a cyber risk management process are to reduce the risk of incidents by proposing adequate responses to identified threats, and to comply with risk management laws and regulations. The authors propose a cyber risk management process, which is very similar to the general risk management process proposed in the ISO 31000 and to the ISRMP proposed by the ISO/IEC 27005. This process contains the following phases: *context establishment*, *risk identification*, *risk analysis*, *risk evaluation*, *risk treatment* and *risk monitoring*.

Refsdal, Solhaug, and Stølen (2015) state, that cyber risk management processes are not fundamentally different from general risk management processes, but that they do differ in specific points. Differently from the environment of general risk management processes, where the sources of risks are somehow known and reduced in scale, the cyberspace, the main environment addressed by cyber risks management processes, is susceptible to infinite and widespread risk sources due to its global and borderless nature. Looking for and analysing all these risk sources, thus, is a complex task. They argue that one way to navigate this immense amount of risk sources affecting the vulnerabilities of systems and infrastructures is to divide the *risk identification* into *identification of malicious cyber risk* and *identification of non-malicious cyber-risk*. This because the nature of risks, their sources, the vulnerabilities they explore, their consequences and the ways to identify them greatly depend on whether they are intentional and planned or unintentional and accidental.

### 2.2.3 Risk framing: establishing the context and building enterprise-wide security requirements

*Risk framing*, as defined by the NIST SP 800-39, refers to establishing a context for risks by describing the environment in which risk-based decisions will be debated and taken. The main product of this phase is a *risk management strategy* that will define how risks will be addressed and strategically managed, and which methodologies will be used in doing so. This strategy will also inform the three other phases of the ISRMP. A risk frame is delineated by identifying risk assumptions (hypotheses about the threats, their possible consequences and their respective likelihood and severity), risk constraints (financial, legal or technological constraints, e.g.), risk tolerance (the type, level and quantity of risks that an organisation would be ready to take), priorities and trade-offs (the relative importance of risks and the compensations among them).

This phase should be mainly implemented by the first tier of a multitiered risk management approach, composed of senior leaders and executives, whose focus lies on the organisational perspective of risk management. The first tier creates context and governance structures for the ISRM activities conducted by the organisation and develops strategies to invest into information security risk

management resources. Nevertheless, risk framing should constantly receive feedback from and be complemented by the second and third tiers' understanding of the organisation's risk frame and by the information and knowledge generated in the other phases of the ISRMP. The second tier is basically composed by business owners and the third tier is comprised of program managers, information systems' owners and controllers. More details about these tiers will be presented along this section. (NIST, 2011)

The first phase of the ISRMP proposed by the ISO/IEC is equivalent to NIST's risk framing as it deals with *context establishment*. In this phase, organisations will plan how they will conduct the ISRMP, will define the scope of the process, its boundaries and its targeted and supporting assets, will define the responsibilities of internal and external parts, will check for legislative and regulatory requirements, and will define the basic criteria to analyse and evaluate risks, as well as to measure their impact. Some criteria will also be defined in relation to the organisation's risk appetite, risk tolerance, risk attitude and risk acceptance. During the context establishment organisations will also examine whether they have the necessary resources for conducting a risk management process. (Lachapelle and Halili, 2015) In this sense, this phase is important because it allows managers to wisely plan the allocation of available resources on the relevant assets and matters. (Refsdal, Solhaug, and Stølen, 2015)

Equivalent phases to the risk framing and context establishment phases described above, are established by the OCTAVE framework, *build enterprise-wide security requirements*, and by the OCTAVE Allegro framework: *establishment of risk measurement criteria*, *development of an information asset profile* and *identification of information asset containers*.

Build enterprise-wide security requirements refers to identifying the perceptions and assumptions of three different tiers (senior managers, operational managers and staff-level personnel) about the organisation's assets, the threats to them, indicators of risk, the organisation's current security strategy (organisational and technical practices, as well as trainings and policies) and laws and regulations to be followed. It also refers to integrating the individual perspectives collected from the three tiers to elaborate an organisational view of assets, risk indicators (organisational issues, such as the lack of documented policies for information assets protection), and of the available and required security strategies. (Alberts et al, 1999, p. 9) The outputs of this phase include prioritized lists of enterprise assets with attributed values, the profiles of threats to the organisation, an overview of the current security strategies, risk indicators, security requirements and a security requirement. (Alberts et al, 1999, p. 15; 21; 26)

Establishment of risk measurement criteria is quite straightforward and refers to defining a way to measure risk in each area of the organisation that could be potentially impacted. Development of an information asset profile and identification of information asset containers refer to listing important assets of the organisation and identifying which assets contain relevant information. (Talabis, Martin, and Wheeler, 2013)

The main difference between establishing the context in a cyber risk management process and in a general risk management process refers to the need to map how information systems build their interactions in the cyberspace, so that the origin of cyber threats is detected and the information and noninformation assets that they affect are tracked. (Refsdal, Solhaug, and Stølen, 2015)

### 2.2.4 Risk assessment: identifying, analysing and evaluating

*Risk assessment* as defined by the NIST SP 800-39 is the stage in which risks are identified, analysed and determined within the context of the defined risk frame. For the ISO/IEC, risk assessment is the stage in which the value of information assets is determined, the existing threats, vulnerabilities and their potential consequences are identified, and the current risk controls and their effects are investigated. (Lachapelle and Halili, 2015) For Talabis, Martin, and Wheeler (2013), a risk assessment is, to a large extent, a synonym of getting to know yourself as an organisation and investigating your own features that make you less or more susceptible to risks.

A risk assessment should be planned in advance, to consider the scope of the assessment, the associated assumptions and constraints and the sources of information that will be utilized as input. During the risk assessment, internal or external vulnerabilities are researched, threats sources are identified and examined, and threat events are identified and investigated. This because risks tend to materialize due to a combination of threat events, each taking advantage of one or more vulnerabilities (NIST, 2012).

Most of vulnerabilities are found by the second and third tiers, and they refer to process, architecture-related or information systems' issues. Threat sources are also usually identified by these tiers, and they may have as their origin: adversaries (individuals or groups that decide to exploit an organisation's dependence on cyber resources), accidents (errors committed by professional while performing their daily tasks), failures in structures (malfunction of equipment or software) and environmental disasters. In this context, the culture and established practices of an organisation will greatly influence the number of threat sources and vulnerabilities identified and the willingness of employees from these tiers to communicate them. (NIST, 2011)

The risk assessment proposed by the ISO/IEC is formally divided into three sub-phases. The first one is *risk identification,* and it refers to identifying relevant assets, threats (accidental or deliberate, from human origin or not), the cyber controls in place, the potential vulnerabilities that could be exploited (defaulting processes, physical environment, malconfigurations in systems, among others), and the potential consequences of risks (loss of credibility, reputation, revenue, operating conditions, among others). (Lachapelle and Halili, 2015)

Refsdal, Solhaug, and Stølen (2015) propose a double identification phase, one for malicious cyber risks and one for non-malicious cyber risks. Regarding malicious risks, the authors state that the first step is to identify their sources, then the threats that these sources pose, and then, vulnerabilities that they will try to explore in information systems and infrastructures. The most effective ways to conduct this phase is through technical tests, brainstorm sessions, workshops and interviews with professionals who are likely to be aware of the targets and the weaknesses of organisations, their systems and infrastructures. Regarding non-malicious risks, Refsdal, Solhaug, and Stølen (2015) state that the sources for unintended accidents are numerous and, thus, following the same sequence of steps as in the identification of malicious risks becomes impractical and wasteful. The recommendation, then, is to implement the steps in reverse order, starting by mapping which are the information and non-information assets that could be harmed, then which vulnerabilities could lead to this damage, and which threats would be channelled by them. The last step in this case would be identifying the origin of mapped threats.

The second phase of the OCTAVE framework, *identification of infrastructure vulnerabilities*, is similar to parts of the risk assessment phase proposed by the standards and authors discussed above. It refers to utilizing the inputs from the first OCTAVE framework phase to map high-priority information assets to information infrastructure and to perform infrastructure vulnerability evaluations. (Alberts et al, 1999, p. 35) In order to do so, the following activities are recommended: identification of the information structure configuration, consolidation of assets with infrastructures, examination of the access paths that lead to important assets, examination of data flows, identification of assets that support important assets, determination of high-priority components of infrastructures, selection of intrusion scenarios, establishment of the scope of the infrastructure examination, and conduction of infrastructure examination. The outputs of this phase include a map of the physical configuration of the information infrastructure, a compilation of information about assets (their location in infrastructure, access paths, data flows and supporting assets), a list of high-priority infrastructure components, a compilation of intrusion scenarios, a list of existing and missing policies

and practices, and a compilation of potential vulnerabilities and verified vulnerabilities. (Alberts et al, 1999, p. 36-47)

The OCTAVE Allegro framework proposes three identification steps: *identification of areas of concern*, *identification of threat scenarios*, *identification of risks*. In these phases vulnerabilities are investigated and a catalogue of threats is built. Also, threats are combined with their potential impacts to generate risks. (Talabis, Martin, and Wheeler, 2013)

After threats and vulnerabilities are identified, organisations need to analyse and determine them in terms of likelihood, consequences and impact (NIST, 2011). The NIST includes risk identification and risk determination into the same package of risk assessment. The ISO/IEC designates two separate phases for analysing and determining risks: *risk analysis* and *risk evaluation*.

Risk analysis is about estimating the potential consequences and the likelihood of incidents to determine the level of risks for all relevant scenarios that were assessed. The level of risk is, thus, a combination between various factors such as the impact of their consequences and/or their likelihood and/or the value of assets and/or the easiness of vulnerability exploitation. It can be expressed in several different scales, depending on the number of factors utilized, and on the criteria established by the company. In this sense, Refsdal, Solhaug, and Stølen (2015) state that the popularity of approaches utilising more than two factors to determine the level of risks has been growing.

Risk evaluation refers to comparing the identified risks and their respective levels with the evaluation and acceptance criteria defined in the context establishment phase. The main output of this phase is a list of assessed risks prioritized in accordance with the defined risk evaluation criteria. (Lachapelle and Halili, 2015; Refsdal, Solhaug, and Stølen, 2015)

The likelihood and the impact of identified risks on organisations are measured in accordance with the selected assessment approach: a qualitative one, a quantitative one or a mix of both. For that, a set of measures and analytical techniques ought to be defined by each organisation depending on their risk policy, on the level of uncertainty of risks and on the selected analytical approach: threat-oriented, asset/impact-oriented, or vulnerability-oriented. A threat-oriented approach focuses on identifying threat sources and threats events and on the study of threat scenarios. An asset/impact-oriented approach focuses on identifying impacts and consequences, and then, the threat sources and events that could lead to them. A vulnerability-oriented approach focuses on identifying exploitable weaknesses in an organisation's information systems and environments, and then, the threat sources and events that could take advantage of them. (NIST, 2012)

The third phase of the OCTAVE framework, named *determination of security risk management strategy and plans,* is divided into two processes. The first of them also deals with conducting a multi-dimensional risk analysis utilizing the inputs from the previous phases. The main objective of this analysis is to determine and prioritize the risks to the organisation based on their impact and likelihood. The activities in this phase involve determining points of vulnerability in potential intrusion scenarios, examining assets exposed by the validated intrusion scenarios and the threats over these assets, build a statement/understanding of the actual risk, and select priority risks to the organisation. (Alberts et al, 1999, p. 49) As also stated by Petrenko, when risks are successfully assessed, it is possible to establish trade-offs and prioritize the risks according to their predicted potential impact. Moreover, it is possible to provide accurate and good quality input to the subsequent phase. (Petrenko, 2019, p. 145 - 146)

By the end of this multi-dimensional risk analysis proposed by the OCTAVE framework, a list of validated intrusion scenarios, a compilation of exposed assets and the possible impacts on them, an estimation of threat likelihoods, and a list of risks and prioritized risks are generated as outputs (Alberts et al, 1999, p. 55). The second process of the third phase of the OCTAVE framework will be described in section 2.2.5.

The sixth step of the OCTAVE Allegro framework also refers to *analysing risks*. Talabis, Martin, and Wheeler (2013) state that in comparison with other frameworks, this analysis, however, is much more focused on the impact of risks than on their likelihood.

Risk determination usually utilizes as analytical input actual threat or vulnerability information, such as historical data related to risks and their predicted impact; expert assessments counting on previous knowledge about the mapped cyber threats, vulnerabilities and risks; and analytical techniques and methods to weight potential impacts and severity, such as but not limited to probability and consequences matrixes, structured what-if technique (“SWIFT”); root cause assessment (“RCA”); damage potential, reproducibility, exploitability, affected users and discoverability method (“DREAD”); spoofing identity, tampering with data, repudiation information disclosure, denial of service and elevation of privilege classification (“STRIDE”); MERIT; business impact analysis (“BIA”); failure mode and effect analysis (“FMEA”); layers of protection analysis (“LOPA”); event and attack tree analysis; bow-tie analysis; human reliability assessment (“HRA”); sneak analysis; Delphi technique; checklists-based method; brainstorming technique; preliminary hazard analysis (“PHA”); Bayes network-based analysis; Monte Carlo simulations; or even semi structured or structured interviews. (Petrenko, 2019, p. 145 – 147; van der Linden, 2007) We note that this study does not aim at explaining these techniques and methods or the specificities about the types of data

that they utilize. It only aims at mapping the techniques that are recommended and/or used in the analysis of cyber risks.

The reliability of a risk analysis and determination depends on the accuracy and integrity of the data collected and utilized. Also, the interpretation of a risk analysis and determination will greatly depend on certain parameters established by the organisation. The time horizon of identified threats, for example, may determine that they should not be a point of concern within the next years. (NIST, 2011) Whenever risks are found to go in the same direction to harm the same assets, it is also possible to aggregate them and conduct a joint evaluation. This because the individual effects of these risks may not be significant, but when they are combined, they may cause bigger impact. (Refsdal, Solhaug, and Stølen, 2015)

Refsdal, Solhaug, and Stølen (2015) identify three main differences between the analysis of cyber risks and the general analysis of risks. The first one is that the analysis of malicious cyber risks should be conducted separately from the analysis of non-malicious cyber risks. Exception is made to the risks that are both malicious and non-malicious, which are analysed together. The second one is that it may be hard to make estimations about the likelihood of malicious threats due to their diversity and complexity. Advanced persistent threats, for example, may be more challenging to analyse because of the degree of uncertainty that they offer and their ever-changing nature, making it difficult to utilize historical data to reach any conclusions (NIST, 2012). The second one is that the nature of the cyberspace makes it easier to employ technologies to monitor and test variables that can assist in the development and sharing of analyses.

### 2.2.5 Risk response: treating a risk

*Risk response* as defined by the NIST SP 800-39 refers to developing courses of action in relation to an assessed risk, taking into consideration the defined risk frame. It also involves studying and determining the most appropriate course of action based on the organisation's risk tolerance and implementing the selected one. (NIST, 2011) When responding to the identified and analysed risks, organisations usually have the option of taking passive actions or active actions. The passive actions refer mostly to *risk acceptance*, when the observed risk is within the organisation's tolerance and no countermeasure or engagement is needed, or *risk avoidance*, when the observed risk exceeds the organisation's risk tolerance and, thus, there is the need to transform one or more features of the organisation's cyber activities. Among the active actions are *risk sharing*, when part of the risk and its liability is shared with a third party, *risk transference*, when the entire responsibility over the risk is transferred to a third party, or *risk limitation* also known as *risk reduction* and *risk mitigation*, when

measures are taken to address and decrease the probability that the identified risk will materialize, and to soften their potential adverse consequences. (NIST, 2011; Petrenko, 2019, p. 147-148)

The practice of sharing cyber risks has created the cyber-insurance field and its products. Though it is still a growing and not very well-structured market, several organisations can already count on cyber-insurance to reduce their exposition to a cyber risk. (Refsdal, Solhaug, and Stølen, 2015)

The ISO/IEC has an equivalent phase to risk response entitled *risk treatment*. Some of the treatment options proposed overlap the ones suggested by the NIST and by Petrenko: *risk retention*, equivalent to risk acceptance, *risk avoidance*, *risk sharing* and *risk modification*, equivalent to risk mitigation. The main output of this phase is a risk treatment plan. (Lachapelle and Halili, 2015)

As previously stated, the third phase of the OCTAVE framework is divided into two processes, one described in section 2.2.4. The other process, entitled *protection strategy development*, refers to developing and implementing a strategy to reduce information security risks. It includes activities such as identifying possible mitigation approaches, developing a protection strategy, and implementing the selected protection strategy. The protection strategy should include the selected mitigation approaches and an estimation of the impact of these approaches in the exposed assets that are at risk. (Alberts et al, 1999, p. 68-74) We highlight that, as noticed from the description above, the OCTAVE framework refers to all possible risk responses as mitigation approaches.

The OCTAVE Allegro framework also proposes a *selection of mitigation approach* phase. In this phase the assessed risks will be categorized into the following mitigation approaches according to their risk score: *mitigate*, *mitigate or defer*, *defer or accept*, and *accept*. For risks that fall into the first and last approaches, organisations have no response alternative. For risks that fall into the second or third approaches, organisations can decide which approach to follow among the two available ones. (Talabis, Martin, and Wheeler, 2013)

Depending on the risk response chosen, residual risks may remain, demanding a reassessment. In some of these situations, a recurring cycle between risk assessment and risk response is born (NIST, 2011). To address residual risks, the ISO/IEC suggests an extra phase for the ISRMP: *risk acceptance*. During this stage, organisations assess whether they are willing to take the residual risks or not. (Lachapelle and Halili, 2015)

For Refsdal, Solhaug, and Stølen (2015) there are two main differences between the risk treatment of a general risk management process and the one of a cyber risk management process. The first one refers to the technical complexity of information systems, which end up requiring equally technical risk responses. The authors, state, however, that these technical responses may be eventually

combined with socio-technical ones. The second difference refers to the distinction between malicious and non-malicious cyber risks, which tend to require unequal treatment actions. Malicious cyber risks, for example, are hard to go extinct and thus, may require responses other than risk elimination.

### 2.2.6 Risk communication and consultation

*Risk communication and consultation* is a phase of the ISRMP proposed exclusively by the ISO/IEC. The justification for the establishment of this step separately lies on the extreme importance of informing the organisation's collaborators and stakeholders about the factors of each of the phases of the ISRMP and its results and receiving feedback from them. This way, risk awareness is improved and the efficiency of the process tends to increase. (Lachapelle and Halili, 2015)

The ISRMP established by the NIST does not address communication matters in an independent phase, nevertheless, the NIST also highlights the importance of communication during the whole process. The ISRMP cycle is dynamic and flexible, allowing phases to dialogue between themselves and complement each other. Thus, it is key to maintain good communication flows between the process' phases and to document all the phases and tasks conducted. (NIST, 2011) The phases of the ISRMP are not sequential in nature because organisations have flexibility to perform them differently, but the consistency of the process lies on utilizing the output of one phase as input to conduct another one, but not necessarily in a predetermined order. For this reason, once again, communication is key. (NIST, 2011)

### 2.2.7 Risk monitoring

*Risk monitoring* refers to strategically following up the assessed risks and the responses given to them. This phase is also conducted with the objective of maintaining and even increasing risk awareness inside an organisation. Risk monitoring involves verifying if the planned responses were duly implemented and if information security requirements defined by the organisation's mission and strategy, and by local and international legislation, policies guidelines and standards, are met. It also involves assessing whether the chosen course of action is being effective in relation to the assessed risks and if there were any changes to the organisation's information systems and environments that might impact the originally selected responses. If issues are found with compliance and effectiveness of responses, risk monitoring results may determine that the organisation revisit the risk response phase of their ISRMP. If changes in the information systems and environments are detected, then the organisation may need to conduct new risk assessments. (NIST, 2011; NIST 2012)

The ISO/IEC also argues towards the importance of risk monitoring. It is in this phase that new relevant assets to be included in the scope of the ISRMP are discovered and that new or modified threats and vulnerabilities are detected. It is also the phase in which organisations review their assessment outcomes, their analyses, and responses to check if their decisions remain applicable to the current circumstances. In case changes in the estimated impacts are identified, for example, new reassessments and new responses are needed. (Lachapelle and Halili, 2015)

The second process of the third phase of the OCTAVE framework, entitled *protection strategy development*, includes in its activities the creation of a comprehensive plan to effectively manage risks in a continuous base. This activity includes monitoring the effectiveness of the selected mitigation approaches, monitoring indicators to identify new risks or changes to previously spotted risks, and developing a chronogram for the periodic application of the OCTAVE framework. (Alberts et al, 1999, p. 59-60)

Risk monitoring can be conducted in an automated or in a manual way depending on the organisation's culture, resources and techniques. The first method seems to be faster, more efficient and less prone to errors. (NIST, 2011) In fact, the dynamism of cyber risks may demand that the monitoring phase is conducted in a similar fast pace. As a result, managers may not have much choice than to utilize automated monitoring tools. This is the biggest difference in relation to general risk monitoring phases. (Refsdal, Solhaug, and Stølen, 2015)

### 2.2.8 Other considerations

When presenting the risk framing, it was mentioned that the NIST SP 800-39 proposes a multitiered approach to information security risk management. As previously discussed, the first tier deals with risk management activities from an organisational perspective, directly affecting the activities conducted by the second and the third tiers, which deal with risk management activities from a mission/business process perspective and an information systems perspective, respectively. In this sense, the second tier is responsible for information security risk management activities, such as defining the types of information needed to successfully execute the mission/business processes and the sensitivity of this information; incorporating information security requirements into mission/business processes; and establishing an information security architecture that is efficient and that follows the strategic goals of the organisation. The third tier, in turn, is guided by the risk activities of the first and second tiers. It is responsible for activities such as categorizing the organisation's information systems; allocating security controls to information systems and environments; and managing the selection, implementation and assessment of these security controls.

The initiatives taken by the second and third tiers usually belong to the assessment, response or monitoring phases. (NIST, 2011)

## 2.3 Services and products

The objective of this subsection is to make the reader familiarized with some of the main cyber risk management services and products offered by organisations that operate in the field. This section wants to provide palpable examples of what these marketable solutions are. For this purpose, selected cyber risk management products and services will be presented. This section will also discuss two different categorizations of cyber risk management services and products: a phased approach and a technical sophistication approach. We note that this is not intended to be a comprehensive analysis of all cyber risk management products and services that exist, and on the ways to categorize them, but only an illustrative sample.

One of the services that organisations operating in the cyber risk management field offer clients is to *assist* them in *developing and implementing their risk management programs, objectives, policies and processes*. These organisations have extensive exposure to risk management practices and may provide useful guidance and tips to clients based on their experience and expertise.

Another service that organisations that operate in the cyber risk management field offer clients is to *assist* them *in interpreting and complying with international standards and frameworks*. Several clients understand what they have to do in term of cyber risk management when they read these international documents, but they do not know how they can do it. Thus, hiring consulting services from experts may clarify their path, reduce their worries and increase their market reputation.

A third line of service that cyber risk management organisations offer clients relates to *collecting and analysing data* so that relevant information is found. Clients' systems and platforms usually produce large volumes of data at high speed. This data could be utilized to provide insights to the clients' cyber risk management practices, for example, to spot new threats and detect changes in previously mapped vulnerabilities. However, the sea of data created in increasingly faster paces makes it harder for professionals to process and analyse it in a timely manner. Providers of cyber risk management services can assist clients in finding accurate and high-quality data that fit the client's context and that would truly generate value to them. They can also assist clients in processing and analysing the retrieved data quickly enough to avoid unwanted consequences, and in selecting the right kind of method to conduct the analyses. (Hodson, 2019).

To conclude this list, organisations that operate in the cyber risk management field also develop and commercialize *specialized software* that are dedicated to managing cyber risks. These software help clients visualise, organise, integrate and communicate the steps and actions that are being conducted in each phase of their cyber risk management process.

### 2.3.1 Phased approach

It is possible to categorize cyber risk management services and products utilizing distinct approaches. A phased approach is one of the options. In this approach, cyber risk management solutions are divided according to the phase of the cyber risk management process that they dedicate to. Several providers of cyber risk services have segmented solutions to assist clients in selected phases.

*Cyber risk assessment services and tools*, for example, help clients in determining risks by identifying and analysing threat sources, vulnerabilities, assets, likelihood and impact. Providers of cyber risk services, will, for example, explain about and look for signs of cyber-terrorists, black hat hackers, hacktivists or insiders as sources of threats. They will also attempt to locate the attack point of each of these potential sources and to understand the threat that they represent. The specialists will further scan information systems and infrastructures to spot vulnerabilities, such as inadequate attack detection and response system, unprotected local network and weak encryption and integrity check. (Refsdal, Solhaug, and Stølen, 2015) Providers of cyber risks management services may also assist clients in selecting the appropriate scales, as well as analytical tools and techniques to analyse identified risks.

In this context, *threat modelling* services are also provided to assist clients in identifying, analysing and documenting the vulnerabilities of an application or system, the threats to them, and the mitigation options for the identified threats and vulnerabilities. Threat modelling takes the attacker point of view and describes what are their goals with the attack, and which methods they could use to be successful. It also analyses what are the entry points of these applications and systems and the assets that they possess, so that the attacker could successfully affect them. The output of a threat modelling service is a threat model, which details a system's or platform's threat profile, as well as the analysis of vulnerabilities and mitigations in relation to the profile. The model is expected to be reviewed regularly to account for threat and vulnerability changes. (van der Linden, 2007)

While cyber risk assessment and threat modelling have similarities, their nature and analytical point of view are distinct. Moreover, cyber risk assessments are highly dependent on the inputs from the context establishment phase, such as a list of assets to protect, the company's risk criteria and risk

appetite, and the definition of roles and responsibilities. Both of them are important in cyber risk management activities and should be complementarily conducted.

Other phases of cyber risk management processes may receive special attention from clients and generate a demand for specific services and products. To develop an efficient risk monitoring, for example, clients may request cyber risk management providers to develop and implement automated monitoring systems.

It is important to highlight, however, that cyber risk assessment has received a lot more attention than the other phases of the process. During the conduction of this study's literature review, a large number of books and articles dedicate exclusively to cyber risk assessment and risk assessment were found.

### 2.3.2 Technical sophistication approach

Another way to categorize cyber risk management services and products is through a technical sophistication approach.

There are roughly two types of solutions in terms of technical sophistication that providers of cyber risk management services can offer. First, those that address risks caused by traditional sources of threats, such as groups of hackers with limited capabilities, intentional internal offenders and unintended offenders. Second, those that address risks caused by advanced persistent threats, which are posed by adversaries with great expertise and a large quantity of resources. These adversaries persist in the attacks for an extended period of time and are able to adapt and resist to the organisations' protection and mitigation initiatives. (NIST, 2011) This category is usually represented by cyber-terrorist groups and highly skilled and resourceful groups of hackers.

All services mentioned in the previous subsections could receive the due adaption to address either traditional sources of threat or advanced persistent threats. Both types of solutions require constant investments over the years, to account for technological, methodological and legal changes. Nevertheless, the investments in solutions that aim at addressing cyber risks caused by advanced persistent threats tend to extend for even more years and to demand more financial resources because the degree of uncertainty is higher. (NIST, 2011; Refsdal, Solhaug, and Stølen, 2015)

## 2.4 Trends

The main objective of this subsection is to review existing literature, standards, frameworks and official governmental documents to list and discuss cyber risk management trends or risk management trends and their applicability in cyber risk management field. This revision will be made

both in terms of global trends and trends identified in Finland. Trend, in this context, refers to a general movement or a line of development toward a specific direction.

We note that the trends presented in this subsection have a very diverse nature and deal with different features of risk management. They were chosen based on their fitting to this study and on feedback received from interviewees. Not all existing trends were selected and reproduced here. The order that the trends are presented does not implicate that one deserves more attention than another, or that one is stronger than another.

### 2.4.1 Managing cyber opportunities

As previously stated, according to the ISO (2009; 2018), a risk is the positive (opportunity) or negative (threat) effect of uncertainty on objectives. Historically, organisations have focused on managing the threats to their businesses and activities. In the recent years, however, the approaches to risk management have been widened, and several organisations started employing risk management processes to identify, analyse and pursue potential opportunities to increase their values. Risk treatment actions involving *risk increasing* or *risk exploitation* started being discussed in the literature and adopted by organisations, showing that risks can also be positive. (ISO, 2009; McShane, 2018)

The NIST SP 800-39, the NIST SP 800-30 and the OCTAVE framework do not address the positive aspects of cyber risks, the opportunities, but focuses exclusively on negative aspects of cyber risks, the threats. The ISO/IEC 27005 admits that risk treatment can involve taking or increasing a risk to seize an opportunity, but does not include risk increasing or risk exploitation in the possible treatment actions for risks identified when conducting an ISRMP (ISO/IEC, 2018b).

There is the possibility that cyber opportunities could be explored and managed through cyber risk management processes, similarly to what has been happening in the risk management field. More studies are needed to tell if cyber risks only have negative effects or if they could also be seen as opportunities that could be managed with the employment of risk management tools, including processes, standards and frameworks. (McShane, Eling and Trung, 2021)

### 2.4.2 Plurality of analytical techniques

As previously mentioned, diverse analytical techniques and methods to analyse vulnerabilities and threats and to weight potential impacts are being employed in the cyber risk management field. Many of these techniques are not new per se, but their application into the cyber risk management field seems to be recent. The results that some of them have been delivering are being increasingly

appreciated by professionals and leading to an expansion in their use. Analytical techniques employed in the field include, for example, SWIFT, STRIDE, attack tree analysis, Delphi technique, checklists, brainstorming technique, semi structured interviews and Monte Carlo simulations. (Petrenko, 2019, p. 145 – 147; van der Linden, 2007)

It is important to highlight that standards usually do not recommend the use of one technique or method over another. Thus, organisations are able to try them and discover which ones fit their objectives, necessities and data best.

We highlight that this study will not explain all these analytical techniques in detail because it would go beyond its scope and objectives. Still, throughout the sections of this study, one or another technique are briefly described.

### 2.4.3 Increasing importance of international standards and frameworks

Providers of cyber risk management services may utilize preestablished processes and frameworks, like the ones we presented in section 2.2, or may create their own methodologies. Less work is needed when an organisation decides to utilize standards and frameworks, since the creative effort has already been done. Moreover, well-known standards, like the ISO/IEC 27001 or ISO/IEC 27005, are synonyms of best practices and are easier to argue in favour of. They are still not binding, however, globalization has requested organisations each day more to follow guidelines that can be monitored and accepted by others.

The disadvantage is that standards and frameworks were not specifically designed for one or another company, thus, they may not perfectly fit the organisation's needs and context. (Talabis, Martin, and Wheeler, 2013) When an organisation decides to build its own cyber risk management methodology, on the other hand, caution is needed in order not to miss or misinterpret important aspects connected to the theme. Talabis, Martin, and Wheeler (2013) also argue that convincing stakeholders about the quality and credibility of the methodology may be harder. If these challenges are overcome, then, chances are a personalized and easier to implement methodology will be ready to be used. The same authors opine that the best option to deal with this dilemma would be to pick a standard that is recognized, but that allows for some flexibility and adaptation.

### 2.4.4 Approximation of governmental and business spheres in Finland

Finland's Cyber Security Strategy, launched in 2019, established national objectives for the development of the Finnish cyber environment. Among the objectives is the need for better coordination of cyber management initiatives and practices, and cooperation in planning, and

preparedness to deal with risks, and in monitoring them. (Finnish Ministry of Defence, 2019). Cyber criminals tend to keep gaining sophistication and access to better resources, and thus, they are likely to aim for more advanced goals throughout time (Petrenko, 2019, p. 29). Cooperation between public sector organisations, representatives of the cyber industry, and of cyber research institutes is expected to be deepened so that cyber risk management actors can work together in developing and harmonising cyber programmes and guidelines. (Finnish Ministry of Defence, 2019)

## 2.5 Placing this study into the cyber risk management research map

Until now, the cyber risk management research has basically been divided into two big areas: analyses of a specific step of the cyber risk management process or an overall analysis of the whole cyber risk management phenomenon (McShane, Eling and Trung, 2021). This study is located in the last big area, as it is dedicated to analysing all the phases of the cyber risk management process, as well as other features of the cyber risk field.

Among the studies dedicated to analysing the whole cyber risk management phenomenon, some have focused on describing and explaining risk management standards and/or frameworks and technical standards and/or frameworks utilized in the cyber domain, others have dedicated to investigating terminology differences between the concepts and definitions utilized in the cyber risk management processes, and others have engaged in understanding how social and economic sciences can help cyber risk management.

This study has very specific objectives: to investigate how risk and risk management is understood and approached by companies operating in the cyber risk field in Finland, and to understand how these companies see the current cyber risk field in Finland and its trends. In order to reach its objective, this study mixes some of the features and objectives of previous studies conducted in the field. It describes and compares risk management standards and/or frameworks, as well as technical standards and/or frameworks. It argues in favour of and brings a social/ business view to the cyber risk domain. Finally, it tangentially presents discussions about different terminologies utilized in the cyber dimension, which may confuse the reader.

# 3 METHODOLOGY

The objective of this section is to explain the methodology of this study and to clarify and justify choices made when designing the research, and when collecting, handling and analysing data. This section also aims at presenting methodological limitations of this study.

The objectives of this research are to understand and describe how risk and risk management are understood and approached by private companies operating in the cyber risk field in Finland, and to understand the current state of the Finnish cyber risk management market and identify its trends. Literature review showed that there is no research in English about how companies operating in the cyber risk sector in Finland understand and approach risk management, neither with a qualitative nor a quantitative methodology. Still, a few studies about risk management approaches utilized in other fields of business were identified, most of them utilizing qualitative methodologies. As stated in section 1.5, in order to meet the established objectives and to answer the research questions defined in section 1.1, this study also opted to employ a qualitative research methodology to describe, understand and interpret the experiences and perceptions of the target companies and their respective employees.

## 3.1 Research design

This qualitative research was designed following the standards for scientific research. First, a problem was identified and literature was reviewed to find concepts, previous understandings and investigations connected to the problem. Then, research questions were developed to guide the quest for a deeper understanding on the problem. Subsequently, data was collected and analysed, categories and patterns were established, and results were presented giving voice to the participants, but also showing the researcher's judgement and independent thinking. (Creswell, 2007, pp. 36-37; 41; 51)

Semi-structure interviews were selected as the single method research design of this study and were its sole source of data. For the purposes of this study, a single method was deemed appropriate to provide a rich enough database for analysis. (Cassell, 2015, p. 4) When it comes to the type of interview selected, this study employed exploratory interviews. Semi-structured exploratory interviews allow the researcher to gather information about a selected a topic and provide interviewees with a greater space for dialogue, in-depth reflection, and discussion of pertinent issues that naturally emerge from the conversation. (Eriksson and Kovalainen, 2008, p. 82; Cassell, 2015, pp. 12-13) The interview questions were independently prepared and were informed by the literature presented in the introduction and in the theoretical framework of this study. They resulted in a mix

of open-ended and broad questions, to stimulate participants to freely talk about their experience, and closed questions, to gather specific information from participants (Cassell, 2015, pp. 16; 29). It is important to note that when answering to closed questions, participants were always invited to justify and comment on their answers.

Below we describe in detail how each of the three research questions were studied.

*How do companies operating in the cyber risk field in Finland understand and approach cyber risks and cyber risk management?*

This is the main question of this study. To understand and answer it, the first step was to conduct a literature review, including books, articles, frameworks and standards, on risk and risk management and then, on cyber risk and cyber risk management. The objective of this step was to investigate and present what are the understandings of risk and cyber risks in selected literature, and what are the international best practices in terms of risk management and in terms of cyber risk management. This phase set the stage, created parameters and informed the local field investigation that was conducted in Finland. The second step was to collect data from participants in Finland through interviews. The data gathered from these participants is the product of their own experience and perceptions. The third step was to code, describe and analyse the collected data. The fourth step in studying this question was to compare the results interpreted from participants in Finland with the parameters created while reviewing the literature. This stage was important to capture the conformities, specificities and peculiarities of companies operating in the cyber risk field in Finland, and to build their understandings of and approaches to cyber risk and cyber risk management. Finally, conclusions were drawn to answer this research question.

*How companies operating in the cyber risk field in Finland see the current Finnish market?*

To address this research question, the first step was to understand and describe the current state of cyber risk management in the academic field worldwide. Articles were the main sources of information in this step. They were reviewed to map research developments, achievements and gaps globally. The second step was to collect data from interviewees in Finland. The interviewees as sources of information relied on their experience and perception to answer the question about the current state of the cyber risk field. The third step was to code, describe and analyse the collected data. The fourth step involved cross checking the results derived from participants answers in Finland against the information reviewed in the literature. Common aspects on the current state of cyber risk management globally and locally were expected to be found, as well as singularities of the Finnish perspective. At last, conclusions were prepared to answer this research question.

*What are the trends that companies operating in the cyber risk field in Finland observe for cyber risk management?*

To address this third research question, the first step was to identify global and Finnish trends for cyber risk management in the literature. Books, articles, standards and governmental strategies were the main sources of information during this step. The second step was to collect data from interviewees in Finland. These participants utilized their experience and perceptions to answer the questions regarding trends for cyber risk management. The trends previously identified in the literature were also discussed with them. The third step was to code, describe and analyse the collected data. The fourth step involved gathering information in the literature about trends pointed by the interviewees. Thus, material collected from the literature and from interviewees complemented and fed each other. The last step was to draw conclusions to answer this research question.

## 3.2 Data collection

In a qualitative study, data is collected through non-probability sampling and sample sizes tend to be smaller (Cassell, 2015, p. 33). The qualitative researcher usually tries to find the most interesting participants as sources of data, as a way to maximize the chances of acquiring relevant information that will sufficiently answer the research questions and achieve the research's objectives. (Liu, 2017, pp. 1511-1512; Saunders and Townsend, 2018, p. 482) However, their success in acquiring valuable data greatly depends on their ability to gain and maintain access to organisations and people. Potential participants usually receive several requests for information sharing and it may be that they will deny or ignore most of them due to lack of time, interest and trust. (Saunders and Townsend, 2018, p. 482; Eriksson and Kovalainen, 2008, p. 106)

There is no right or wrong number of participants in qualitative research samples (Saunders and Townsend, 2018, p. 490). An adequate choice of interviewees and the quality of the information obtained from them have a greater weight on the success of the research than the sample size (Eriksson and Kovalainen, 2008, p. 290). Considering this, the targeted number of interviews for this study was defined between three and five employees of private companies operating in the cyber risk field in Finland.

During the conduction of this study, some issues in gaining access to participants were faced. Around 43 professionals from 36 different companies operating in Finland were contacted, but less than 8% replied to the contact and accepted to take part in the interview. As a way to overcome this issue, a convenience sampling method was also utilized. This means that to reach the desired sample size, recommended participants were contacted and interviewed (Cassell, 2015, p. 34). Even when access

to participants was gained, maintaining the relationship proved to be challenging. In this sense, some actions were taken, notably: explanations about confidentiality concerns, flexibilization of the interview format, and commitment to send the finished thesis afterwards to raise interest.

Potential participants were initially contacted by e-mail between May 2021 and August 2021. A preamble introducing the study and its objectives, as well as the pre-prepared interview questions were shared with potential interviewees, and they were invited to participate in the study as sources of information. Anonymity and confidentiality of sensitive information were guaranteed, and a voluntary participation, with freedom to withdraw were offered. When potential participants provided their informed consent to take part, the interview format and the date and time were defined. In total, five interviews were conducted in English, between June and August 2021, with five professionals working for five different companies operating in the cyber field in Finland. From now on, we will refer to these interviewees as Interviewee 1, from Company A; Interviewee 2, from Company B; Interviewee 3, from Company C; Interviewee 4, from Company D; and Interviewee 5, from Company E. Interviewee 1 replied to the interview questionnaire on June 16, Interviewee 2 replied on August 13, Interviewee 3 replied on August 13, Interviewee 4 replied on August 17, and Interviewee 5 replied on August 26.

Qualitative interviews are usually conducted face to face, however, due to health restrictions posed by the Covid-19 pandemics, the semi-structured interviews of this study were conducted synchronously via video call or asynchronously via e-mail, whenever this method was deemed more convenient by the involved parties and allowed more interviewees to participate in the study (Eriksson and Kovalainen, 2008, p. 78). The follow-ups to the interviews were conducted by e-mail.

Synchronous video call interviews are similar to face-to-face interviews and allow the researcher and the participant to have a greater interaction and to follow-up questions simultaneously (Eriksson and Kovalainen, 2008, pp. 104-106). For these interviews, permission to record was requested from interviewees and the content of the conversation was later transcribed into a Word document. Notes were also made in real time during the interviews and were transferred to the transcription. The duration of video call interviews was between 45 minutes and 1 hour.

Asynchronous e-mail interviews limit the contact between the researcher and the participant, reduce the spontaneity of interviews, threaten the focus of participants, and pose risks to the identity verification of the participant, as it become impossible to assure if they were really the ones who answered the proposed questions. On the other hand, e-mail interviews are useful tools to access participants that are difficult to reach due to availability constraints and, thus, would appreciate writing answers with flexibility of time and date. Moreover, e-mail interviews allow participants to

better elaborate their responses, as they can think and write with no time restriction, and can edit their answers as many times as they want (Eriksson and Kovalainen, 2008, pp. 104-106; Cassell, 2015, p. 25-28) For these interviews, a deadline for answering was agreed with participants and their answers were returned in written format. In some cases, follow-ups were conducted. The material was, then, compiled and stored in Word documents.

## 3.3 Handling of data and analysis

The raw data containing confidential information, such as names of interviewees and their positions, the name of the organisation they work for, and any other information that could compromise the anonymity of participants was safely stored to prevent unduly access from third parties. Later, this confidential information was erased from the transcribed and compiled material.

The collected, transcribed and compiled data from participants was reviewed and organized into thematic packages of data. This was mostly done in an inductive way, going through data several times to establish patterns, common themes and categories inside the risk management universe. Later, the information resulting from this thematic analysis was used to build interpretations about the understanding, the approaches and the trends associated with risk management in the cyber risk field in Finland. (Creswell, 2007, pp. 38-39; Cassell, 2015, pp. 77; 80)

## 3.4 Reliability and validity of the research

Reliability and validity are utilized as the basic concepts for the evaluation of quantitative and qualitative research in most fields of science. Reliability refers to the extent to which a methodological choice generates the same results for the same research being conducted several times. Validity, in turn, refers to the extent to which the results derived from the research accurately describe and explain the studied phenomenon. There is no agreement, however, about whether the results derived from interviews can be evaluated with the classic criteria of reliability and validity. (Eriksson and Kovalainen, 2008, p. 290-292) This because qualitative research is, by nature, an interpretative investigation about the gathered data. Ideally, results should adhere to data and should disregard the researcher's own perception and knowledge acquired while consulting books and articles. However, there is no way to completely suppress personal touches in qualitative research, because the results are partly based on the participants' input and partly dependent on the researcher's interpretation. (Creswell, 2007, pp. 38-39; 43) This is, thus, one methodological limitation of this study in terms of validity and reliability.

As previously stated in section 1.1, this study does not aim at providing a comprehensive and unified understanding about risk management understandings and practices of all companies operating in the cyber risk field in Finland. This is another methodological limitation of this study.

It is important to highlight, however, that this study was developed with professional integrity and following research ethics principles, such as benefit to all involved parties; respect to the rights of participants; maintenance of the anonymity and confidentiality of sensitive data; and honest report of data (Carpenter, 2018, pp. 39-40). Moreover, this study followed a rigorous and established scientific methodology (Eriksson and Kovalainen, 2008, pp. 70-74; Creswell, 2007, p. 44). Rigor is a set of standards that the scientific community employs to assess the trustworthiness, quality and the value of a research. In order to rigorously develop this study, research questions were defined, methodological commitments were chosen and justified, and a formal and controlled way of collecting, analysing, interpreting and reporting data was ensured. (Liu, 2017, p. 1512) Finally, it is relevant to mention that the strengths and limitations of this study were presented with transparency and critical self-reflectiveness (Eriksson and Kovalainen, 2008, p. 290; Carpenter, 2018, pp. 39).

# 4 DATA ANALYSIS AND RESULTS

The objective of this section is to describe the data collected during the interviews, discuss their meaning and interpret their results. As described by Durdella (2019), the data analysis part of this study moved from diffused sources of primary and intact data to groups of reorganized data. The first step was to summarize and simplify data, the second step was to categorize and code them into patterns, and then to describe and interpret their meanings, applied to the objectives and context of this research.

When it comes to interpretation, Durdella (2019) argues that the researcher does not (and should not) make a completely subjective analysis, simply utilizing their own knowledge about the theme to interpret the interview data and codes. At the same time, the researcher also does not (and should not) reproduce the opinions and perceptions gathered from the field work (the interviews) nor from the literature reviewed. Rather, the researcher should retain their personal lenses, which shape the world and the studied phenomena from the researcher's unique perspective and combine them with the insights and interpretations that come from academics and arise from interviewees. A blended interpretation is, thus, recommended in the data analysis process. This study made great efforts to achieve this optimal balance between interpretation approaches.

## 4.1 Description of data

The data utilized in this section was gathered from five interviews conducted with five employees of five different companies that provide cyber risk management services and products to clients in Finland: Interviewee 1, from Company A; Interviewee 2, from Company B; Interviewee 3, from Company C; Interviewee 4, from Company D; and Interviewee 5, from Company E.

This study attempted to utilize all collected material, but gave priority to the segments and parts that were the most relevant to the objectives of this study. As previously stated, this study employed a thematic data analysis approach, meaning that after being collected, summarized, anonymized and compiled, data was rearranged, reorganized and coded according to the topic they referred to. This way, similar pieces of information were put together to build a common understanding about the phenomena they all refer to in their micro realities. This section follows the same thematic approach and presents data, results, discussions and interpretations in thematic blocks that correspond to the ones utilized while rearranging, reorganizing and coding data. Naturally, the rearranging and coding phase was more complex than just a simple division into boxes. After this first box division, keywords, notable sentences, opinions and technical pieces were highlighted, coloured and brought

together. Still, it is worth mentioning that the first big division and categorization of data served as inspiration for the division of this section. The following four subsections are also symmetric to the first four subsections presented in section 2 of this study. The main objective of this symmetry was to allow the reader to clearly recognize the different sources of information consulted in this study dialoguing about the same phenomena, complementing each other's views, agreeing or disagreeing about specific aspects, and placing stress into different or similar elements.

The first thematic block and first subsection of this section deals with definitions and understandings of risk and risk management from the perspective of interviewees. The second subsection describes and briefly explains the main cyber risk management services and products that are offered by interviewees. The third block discusses the processes, standards and frameworks utilized by interviewees. The fourth subsection presents insights about the current cyber risk management scene in Finland, and the cyber risk management trends mentioned and explained by interviewees.

We highlight that during the interviews the terms risk and risk management were utilized, but participants were asked to provide their answers from a cyber point of view, which is their specialties.

We further highlight that great efforts were made in an attempt to present reliable and valid results in this section. The integrity of data was maintained during the collection and analysis. Despite the interpretivist nature of this study, its results adhere to the data collected as much as possible. As previously stated, the results of this study do not aim to fit the practices and understanding of all companies operating in the cyber risk field in Finland. Still, during the data collection phase we sought to interview as many participants as possible, all representing different companies, so that results could reflect and summarize their practices and understandings as accurately and comprehensively as possible. (Eriksson and Kovalainen, 2008, p. 290-292; Creswell, 2007, pp. 38-39; 43)

## 4.2 Definitions and understandings

The first question of the interview questionnaire aimed at investigating what the interviewees' understanding of risk and risk management is. This study is interested in analysing and comparing academic and standardized general risk management understandings and definitions, presented in section 1.2, with academic and standardized cyber specific understandings and definitions, presented in section 2.1, and with cyber specific understanding in the Finnish market. This last block of understanding is the result of years of experience and environmental influence shaping professional's view on phenomena.

### 4.2.1 Cyber risk

Some respondents characterized *risk* as a combination of likelihood, referring to threats or vulnerabilities, and impact towards relevant assets. Others stated that risk is the possibility that some unwanted outcome would unfold.

While answering the first proposed question, interviewees utilized the terms *cybersecurity risk*, *security risk*, *information security risk* and *cyber risk* to designate the type of risk they were dealing with in a daily basis.

### 4.2.2 Cyber risk management

Some interviewees described *risk management* as a continuous effort towards identifying, evaluating, prioritizing and treating risks related to relevant assets. They added that risk management sets the foundation for information security and cyber risk management. Other interviewees described it as a helpful method to organize the use of cyber resources and to guide cyber operations, and as an essential tool that organisations utilize as input for decision making.

Most interviewees also considered risk management to be the best mean to address security related issues that could impact an organization, its business performance and its ability to achieve its goals, mostly because it provides the right mechanisms to properly prioritize and informatively treat them. Some risks, some interviewees stated, should be accepted, while others should be mitigated so that the organization can operate successfully. Only through a risk management process professionals can visualize which risks should receive a specific treatment.

Respondents mentioned that the understandings that professionals have about risk management tends to be based on security certifications, standards and academic books. Nevertheless, this understanding becomes way more complex when they start to deal with risk management in real life, because there are a lot of conditions, variables and specificities to be considered when actually implementing risk management practices.

Finally, respondents mentioned that the best companies are the ones that have a solid understanding of risks and that have an adequate, active and ever-updating risk management programme.

## 4.3 Services and products

The interview questionnaire proposed two questions to investigate what are the services and products that organizations operating in the cyber risk field in Finland offer clients, and what are their main characteristics. This study is interested in analysing and comparing cyber risk management services

and products described by the reviewed literature, presented in section 2.3, with the ones provided by the interviewees. This study is also interested in understanding which characteristics of general risk management services and products, presented in section 1.2 and referring, for example, to reactive or proactive approaches, are also applied to the services and products provided by the interviewees.

### 4.3.1 Main types

Some respondents stated that variations of *threat modelling* services are their core businesses. They added that these variations usually employ the following techniques: STRIDE, checklists, attack tree analysis and Monte Carlo simulations. For these respondents, their key tasks are to identify, understand and document the threats and vulnerabilities that their clients could be exposed to.

Some respondents stated that they mainly offer *cyber risk assessment* services that compose the clients' risk management processes. These services would include information security risk identification and analysis and cyber business continuity risk assessment.

Some respondents stated that they assist clients in *interpreting, implementing and following cyber frameworks and standards*, such as the ISO/IEC 27001, and the Security Development Lifecycle ("SDL") methodology. They added that they also assist clients in *defining and developing their risk management policies, practices and processes*.

It is relevant to highlight that most respondents stated that they provide at least two of the services listed above. It is also relevant to note that most respondents stated that workshops are the most effective way to develop/deliver their services with/to clients.

### 4.3.2 Characteristics: customization and level of proactivity

When asked about the customization of services and products for each client, respondents stated that threat modelling services tend to follow the same approach for all clients. They added that they have been developing these well-established and well-functioning approaches throughout years of experience, repetition and improvements. Although they have a template to follow, these respondents stated that they usually have to tailor parts of their solutions to fit their clients' context and needs.

Regarding cyber risk assessment services, some respondents stated that they also have a template that they utilize with the due context adaptations. Other respondents stated, however, that their scope is completely tailored to the necessities and assumptions of their clients. Still, they shared that they were planning to develop a generic risk assessment template based on a guideline from the Finnish National

Cyber Security Centre.[20] They highlighted that this guideline is based on NIST standards and on the ISO/IEC 27001. Even if they succeed in this task, they added, clients' specificities would still play a big role on how they develop their solutions.

For services focused on the assistance for standards and methodologies adoption, as well as on the development of risk management policies, practices and processes, interviewees also stated that some degree of tailoring is combined with general templates.

When asked about the level of proactivity of their service and products, some respondents stated that most of their services and products are included in the proactive approach to risk management, as they mostly try to visualize and address risks before they lead to incidents. Some of these respondents stated, however, that they have also been involved in developing, implementing and testing reactive risk management measures to mitigate risks that were not identified, that were not adequately treated or that were modified, and which materialized into incidents. They added that this is a requirement from the ISO/IEC 27001. These measures include incident management initiatives, disaster recovery plans and business continuity practices.

Other respondents stated that the organisations to which they are linked to provide both proactive and reactive services and products. Some of these respondents added, however, that they have mostly been dealing with reactive cases. They opined that great efforts are being made to stress the importance of proactive solutions, which should be seen as investments to the organisation's future. According to these respondents, proactive initiatives tend to be less complex and cheaper than the reactive ones.

## 4.4 Processes, standards and frameworks

The interview questionnaire proposed six questions to investigate how cyber risk management processes proposed by organizations operating in the cyber risk field in Finland look like, and what are their phases and relevant features. These questions were also built to investigate which are the standards, frameworks and own methodologies that guide these organisations. This study is interested in analysing and comparing cyber risk management processes described by the reviewed literature, presented in sections 1.2 and 2.2, with the ones described by the interviewees. This study is also interested in understanding if and how interviewees make use of internationally recognized risk

[20] Available at: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter.

management and cyber risk management standards and frameworks, some also presented in sections 1.2 and 2.2, and/or if interviewees have develop their own cyber risk management methodologies.

### 4.4.1 International best practices and own methodologies

When asked about the international best practices standards and framework that they follow to develop their cyber risk management products and services, most respondents stated that they mainly look for guidance from the ISO/IEC 27001, which set requirements for information security management systems, and from the ISO/IEC 27005, which provides details on how to meet these requirements and to conduct an information security risk management.

Some respondents also mentioned that they follow and look for guidance from the ISO 31000, which provides guidance for general risk management, from the ISO 22301:2019 – Security and resilience – Business continuity management systems - Requirements ("ISO 22301"), which set requirements for business continuity management systems, from the PMI's Practice Standard for Project Risk Management, and from MITRE's Guide for Risk Management. Some respondents added that for governmental clients they also follow the instructions for information security management elaborated by the Finnish Government Information Security Management Board ("VAHTI").[21] Fewer respondents also stated that they have developed their own methodologies to conduct cyber risk assessments, based on the ISO/IEC 27001 and on several NIST guidelines, or that they do not follow one specific standard or framework, but combine parts of all standard and frameworks previously mentioned.

Most respondents stated that though they follow international frameworks and standards that are international best practices, these documents leave some space for professionals to develop or choose the tools that they want to employ in the risk management practices. In this sense, some respondents mentioned that they conduct workshop and make use of Microsoft Office Excel template sheets to list relevant assets, risk treatment plans, security targets and to monitor the ongoing treatments. They also mentioned that, on upper-level requirements, risks and controls are also managed and monitored via a project management software, which is able to connect risks to the respective treatments and controls. Respondents also stated that throughout their years of experience and interaction with clients, they have also been improving their tools and techniques of risk management.

[21] Available at: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_5_2009.pdf.

### 4.4.2 Cyber risk management process phases

Most respondents stated that risk management needs to take place at multiple levels inside an organisation covering products, processes, projects and functions. They added that there should be some variations depending on the level that you are dealing with, but that the main basic steps of risk management processes are the same.

First, it is necessary to understand the context of the organisation, their processes and infrastructure, the data they utilize and the implications of that, the assets that they want to protect and the roles and responsibilities of each person involved to create a scope of work. Also, to optimize the use of resources and to deal with bigger than average systems, it is important to prioritize the most relevant assets. This is the *context establishment* phase. Some respondents stated that this phase is usually a responsibility that they share with the client.

Second, relevant threats, their probability and impact need to be identified, analysed and evaluated. For threat identification and analysis, respondents stated that they employ a variety of methods depending on the situation and context, including data flow diagram, to describe systems, and checklists, threat trends, attack trees, STRIDE, Monte Carlo simulations, interviews, and a 1-5 scale risk matrix to determine the likelihood (rare, unlikely, possible, likely, almost certain) and the severity of risks (insignificant, minor, moderate, major, catastrophic). A risk portfolio is the final product of this *risk assessment* phase. Some respondents considered that this is the most critical phase of cyber risk management and that most mistakes arise from an improper and incomplete assessment of risks. They added that an effective way to avoid mistakes in this phase is to have experts with different backgrounds and perspectives working together and addressing all aspects and not only the technical ones.

Third, suitable controls should be selected and a risk treatment plan should be created. Respondents added that risk treatment plans are created for all risks that are not within the acceptable level. Some respondents also stated that the client always has the last word when it comes to choosing how to handle a risk, and thus, their job is to provide solid information to simplify and support the client's decision. Treatments include mitigation, avoidance, sharing, and transference. This is the *risk treatment* phase. Respondents stressed that, in some case, threats and vulnerabilities are so severe that they demand immediate action. In these situations, there is no time for elaborated analysis and treatment considerations.

At last, organisations should make sure to monitor and review the risk scenarios and repeat the first, second and third steps regularly. According to respondents, businesses evolve, as well as

infrastructures, technologies and risks, consequently. The main objective of this phase, thus, is to follow the evolution of selected risk treatments, to gather information about new vulnerabilities and threats, and to identify and adapt to changes in the environments and risk levels. This is the *risk monitoring* phase.

Respondents added that they document all the phases of the process and create handbooks for each client with evidence of compliance, because it is a requirement of audits, and of the ISO/IEC 27001 and the ISO 22301. They also stated that reports with the main findings and conclusion are shared and discussed with clients and that recommendation are made based on them.

## 4.5 Current State and Trends

The interview questionnaire proposed three questions to investigate how interviewees see the Finnish cyber risk management market and what are the trends that organizations operating in the cyber risk field in Finland see in the Finnish cyber risk management field. This study is interested in analysing and comparing cyber risk management trends described in section 2.4, with the ones pointed and described by the interviewees. It is important to highlight that this study does not have a specific section dedicated to describing the current state of cyber risk management in the world according to the reviewed literature, because this description was made throughout several different sections.

When asked to describe the current state of the Finnish cyber risk management market, most respondents mentioned that the cyber risk management field is still not very well established and very well advertised in Finland, with only about a dozen of companies operating in it. Fewer respondents, however, considered that the cyber risk management market is already well established in Finland and that several organisations provide specialized services in this sense.

Most respondents stated that global companies operating in Finland tend to have more rigid and standardized ways of approaching cyber risk management, which are compatible with international best practices. Nevertheless, they opined that most local companies are far behind in terms of developing and implementing the expected cyber risk management policies, processes, practices and controls. Fewer respondents, however, argued that the Finnish market is quite homogeneous in terms of cyber risk management practices and that most organisations already follow international best practices.

Most respondents stated that there is a great demand for cyber risk management and information security risk management services in Finland, but that most organizational efforts and service requests are focused solely on risk assessment. While it is an important step, risk assessment alone has limited

value. These respondents stated that many organisations do not have a systematic and comprehensive approach to cyber risk management that includes plans of action and monitoring. For them, the continuous practice of monitoring threats, vulnerabilities and risks is not on the sufficient and desired levels. The Covid-19 pandemics and the shift towards remote work has evidenced, like never before, how poor cyber risk management can impact the stability and the security of working tools, respondents said. In this, sense respondents concluded that the market for proper cyber risk management in Finland is huge, and that it could be prosperous and vibrant if organisation's traditional mindset against risk-based thinking was changed in the next years.

In addition, respondents stated that the old belief that cyber risk management is a responsibility of IT departments, and that technology can solve all kind of issues that may appear, limit the prosperity of the field in Finland. Respondents also stated that cyber risk management controls are also needed for processes and people, and not only for technologies.

### 4.5.1 Focus on cyber threats

When inquired about the possibility that managing cyber opportunities would be a trend in Finland, respondents stated that several standards, including the ISO 31000 and the ISO/IEC 27001, already discuss the management of opportunities and require organisations to reflect about it and implement practices in this sense.

Some respondents stated that addressing threats and opportunities would, definitely, be the most correct way to introduce risk management into an organisation, as several improvements could be made to achieve better financial results. All respondents confirmed, however, that most professionals tend to focus on cyber threats and their negative impact to businesses, rather than on the positive impact that opportunities could have. They added that international standards and cyber risk management literature like to include and reflect about both threats and opportunities, but that this is not a reality in the Finnish market yet. All respondents agree that managing cyber opportunities is, thus, not a trend in Finland.

### 4.5.2 Plurality of analytical techniques

Some respondents believe that the plurality of analytical techniques, utilized in cyber risk assessment, in threat modelling and in other risk management practices, is becoming a trend in Finland. For these respondents, the use of Monte Carlo simulation to identify and analyse risks, instead of employing the traditional risk matrices, for example, have proved to be more efficient in some cyber risk management processes. They also positively stressed the increasing use of managed detection and

response (“MDR”) and endpoint detection and response (“EDR”) solutions to assess, treat and monitor cyber threats.

Only few companies are currently using the Monte Carlo simulation, according to respondents, and in the next two years, they expect to see much more companies offering services that include non-traditional analytical techniques. Finally, respondents argued that the employment of non-traditional analytical techniques has been raising the interest of clients and has been pushing the cyber risk management market forward.

### 4.5.3 Increasing importance of international standards and frameworks

Respondents stated that different standards proposed by the ISO/IEC are becoming increasingly important in different sectors, demanding that cyber risk management practices are treated in a much more formal way in the future, even in small companies.

In this sense, some respondents stated that the ISO/IEC 27001 still has the status of a recommended international best practice standard, but that there are ongoing discussions that indicate that it might become mandatory in some specific fields. In case this hypothesis would materialize, respondents opined, there would be a huge gap between what is required and expected from organisations and what they, actually, put into practice in terms of cyber risk management and information security risk management practices, controls, processes, and policies. This situation would increase the demand for comprehensive cyber risk management services.

### 4.5.4 Approximation of governmental and business spheres

Some respondents stated that governmental and business interactions, feedback and joint efforts in terms of cyber risk management have been on the rise in Finland. These respondents highlighted that several governmental initiatives to understand cyber risks, information security risks and cybersecurity risks, and to provide guidelines on how to manage them have taken place in the last year and have counted on the help of business experts and institutional researchers. They added that private companies have also been increasingly relying on governmental documents and guidelines to develop their own cyber risk management methodologies.

# 5 DISCUSSION AND CONCLUSIONS

In this section we will present our discussions and conclusions to answer this study's research questions. For this purpose, we will makes use of the results described in section 4 and of the conceptual literature described in sections 1 and 2. This section will also present the limitations of this conclusions and the recommendations for further research.

As previously stated, this research had very specific objectives. First, *to understand and describe how risk and risk management are understood and approached by private companies operating in the cyber risk field in Finland*. Second, *to understand the current cyber risk management market in Finland and identify its trends.* Three research questions were prepared in association with these objectives. We will list these questions below and will elaborate answers for them having as base the results of this study.

*How do companies operating in the cyber risk field in Finland understand and approach cyber risks and cyber risk management?*

The thematic analysis of the data collected from the interviews, presented in section 4, and the literature review, presented in sections 1 and 2, show that the understanding of *cyber risk* among companies operating in the cyber risk field in Finland divides into two branches. Both of these branches roughly associate the term risk with uncertainty, consequence and impact, just like the definitions and discussions presented in the literature review of this study. One branch addresses risk in terms of its origins, employing the concepts of threat and vulnerability, which are key in the cyber risk domain and were largely explored during this study. It also addresses risk in terms of its likelihood and in terms of its impact towards something relevant and valuable, the assets. This understanding is pretty much aligned with the international literature, standards and frameworks. The second branch does not directly address the origins of risk or the targets of risk. Rather it focuses on risk in terms of possibility of events, a rough equivalent to likelihood in this context, and in terms of its consequences.

Regarding the nature of the outcomes, the understanding of cyber risk among the interviewees is also similar to the one depicted in the reviewed literature, frameworks and standards. For companies operating in the cyber risk field in Finland, a risk is overwhelmingly the negative effect of uncertainty into outcomes. Though the positive effects of uncertainty, the opportunities, are discussed by general risk management literature and standards, they are also not integrated into the cyber risk management literature and standards.

To conclude the discussion about the understanding and approach to risk, this study would like to highlight that companies operating in the cyber risk field in Finland utilize multiple terms to refer to the risks they face in the cyberspace, including cybersecurity risk, information security risk and cyber risk. This reiterates the terminology variety (and confusion) in the field, explained in previous sections of this study.

In terms of the understanding and approach to cyber risk management, companies operating in the cyber risk field in Finland believe that cyber risk management is a combination of tools, methods, policies and processes to guide their cyber operations and to address cyber risks associated with relevant assets. This understanding is in line with the understanding presented in the literature review of this study. For them, the importance of establishing risk management practices and following risk management standards and frameworks is undoubted, still, they do see a gap between the theoretical and the practical facets of risk management in terms of complexity and variability.

Most companies develop cyber risk management processes that dialogue with general risk management processes and cyber risk management processes established by international standards and frameworks. ISO and ISO/IEC standards for information security are the ones that they mostly look for guidance from. These processes rough include the following phases: context establishment, risk assessment, risk treatment and risk monitoring.

The companies operating in the cyber risk field in Finland offer services that can be classified in terms of proactivity, customization and comprehensiveness. When it comes to proactivity, companies offer packages of services that are divided into two categories. First, those that are mostly proactive with a touch of reactive practices. Second, those that are both proactive and reactive, but focus on reactive practices. In terms of customization, while most companies operating in the cyber risk field in Finland have general templates that they use as base to develop services to clients, they also tailor these services to some degree to clients' needs and specificities. Finally, regarding comprehensiveness, services can be divided into two categories. First, those that address cyber risk management comprehensively, including the establishment of policies, the development of holistic risk management practices and processes, and the interpretation of cyber frameworks and standards. Second, those that focus in assisting clients in conducting a specific phase of a cyber risk management process. This is the phased approach discussed in section 2.3.1.

*How companies operating in the cyber risk field in Finland see the current Finnish market?*

Based on the thematic analysis of the data collected from the interviews, presented in section 4, this study found that there is no agreement among companies operating in the cyber risk field in Finland

about the maturity level of the Finnish cyber risk market. While most see it as an under established, an under advertised, some find it to be well-established, well-developed and prosperous. Moreover, most respondents agreed that the cyber field is still seen as a technical field of IT responsibility. This finding dialogues with the discussion presented in section 1.3 regarding the state of cyber risk management research, in which it was stated that cyber risk management is still an understudied phenomenon, and that the cyber field has been mainly studied from a technical perspective.

In terms of compatibility with international best practices, most companies believe that global organisations operating in Finland have a better knowledge about cyber risk management and a more standardized approach to it. Local organisation, on the other hand, seem to not have the due cyber risk management controls in place and are not perceived as compliant with international best practices. Fewer companies think that most organisations operating in Finland, regardless of their size and origin, already follow international best practices in terms of cyber risk management.

Finally, most companies believe that there is a great demand for cyber risk management services in Finland. They also believe that risk assessment services compose the largest part of the cyber risk management services offered in the country, and that more comprehensive services are needed. This finding is aligned with the discussed presented in section 2.3.1.

*What are the trends that companies operating in the cyber risk field in Finland observe for cyber risk management?*

Regarding trends, some companies operating in the cyber risk management field in Finland believe that the diversity of analytical techniques they have been employing has been increasing. This is seen as a positive trend that will increase efficiency of risk management practices and will raise the interest of clients on cyber risk management.

Another trend identified by the companies is that international standard and frameworks are becoming increasingly relevant. As a result, many more organisations will find themselves formally following and implementing these guidelines and requirements. The possibility that these standards will become mandatory in some fields is expected to foster the demand for cyber risk management services in the country.

Finally, companies operating in the cyber risk management field in Finland believe that Finnish governmental and business spheres are joining efforts and sharing feedback to establish common understanding and guidelines on cyber risk management.

This study has some limitations that should be accounted for when reading these conclusions. First, the sample size of this study was small, as only five interviews were conducted. Second, the answers provided by interviewees might have been biased and dependent on their understanding of the interviewer's question and on their own personal experiences. As a result, they may not represent a homogeneous understanding of the theme throughout the whole Finland. Third, the interpretation of the answers provided by interviewees might have been subjective or subject to misunderstandings from the researcher's side. To tackle the first and the second issues, we would recommend the development of studies in the line of this one, with larger samples of data collected from all over the country. Also, to tackle the second and the third issues, we would recommend the conduction of complementary studies employing a different research method and research design, possibly including quantitative or mixed methods, for example.

Cyber risk research is relatively new and there is a lot to be explored, tested, and improved in the field. As stated by Falco et al (2019) and as highlighted in many sections of this study, terminology, classification and categorization disagreement, and lack of cross-disciplinarity in the cyber risk field makes it hard for studies to advance and for organisations (governmental, private, non-profit ones, among others) to follow and implement frameworks and standards.

In this context, McShane, Eling and Trung (2021) stated that there are several gaps in the cyber risk research that should be filed by future studies, either in terms of cyber risk management processes as a whole or focusing on one of their phases and their respective particularities. The gaps identified by the authors in terms of overall cyber risk management processes refer to the lack of studies attempting to integrate cyber risk into general risk management processes and frameworks, and to the lack of studies about cyber risks that attempt to explore cyber resilience and combine it with cyber risk management.

Throughout this study, we described and discussed general risk management processes, frameworks and standards, as well as cyber risk management processes, frameworks and standards. Some comparisons between them were made, and some observations about the peculiarities of cyber risks in comparison to general risks were presented. The objective of this study was not to understand the relationship and integration possibilities between cyber risks and general risk management processes and frameworks. Still, efforts were marginally made to discuss what sets them apart. In this context, we would recommend the development of studies fully dedicated to the theme, so that data could be collected and analysed, and that deeper understandings about their compatibility and necessary adaptations could be gathered.

In this study, we briefly explored the concept of cyber resilience when we discussed about cyber security risks and cyber security risk management. Nevertheless, in most of this study we kept some distance from cyber resilience topics because, unfortunately, there would be no space to include literature review, standards and frameworks, and discussions about them. We also did not touch topics such as business continuity, incident management and recovery plan from the point of view of cyber. We consider that the relevance of resilience practices has been growing and that studying possibilities to integrate cyber resilience and cyber risk management would be very profitable to the scientific and business communities.

# REFERENCES

## Books


Bayuk, J. L. (2007). *Stepping Through the InfoSec Program*. Information Systems Audit and Control Association ("ISACA").

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook* (1st ed.). John Wiley & Sons.

Bernstein, P. L. (2012). *Against the Gods: The Remarkable Story of Risk* (7th ed.). John Wiley & Sons.

Brandimarte, P. (2014). *Handbook in Monte Carlo Simulation: Applications in Financial Engineering, Risk Management, and Economics* (1st ed.). John Wiley & Sons.

Calder, A., & Watkins, S. (2019). *Information security risk management for ISO 27001/ISO 27002* (3rd ed.). IT Governance Pub.

Cassell, C. (2015). *Conducting Research Interviews for Business and Management Students*. SAGE Publications.

Creswell, J. W. (2007). *Qualitative Inquiry and Research Design: Choosing among Five Approaches* (2nd ed.). SAGE Publications.

Durdella, N. (2019). *Qualitative Dissertation Methodology: A Guide for Research Design and Methods*. SAGE Publications.

Eriksson, P. & Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications.

Hodson, C. (2019). *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls*. Kogan Page.

Kerzner, H. R. (2014). *Project Management Best Practices: Achieving Global Excellence* (3rd ed.). John Wiley & Sons.

Leeuw, D. K. M. M., & Bergstra, J. (2007). *The History of Information Security: A Comprehensive Handbook* (1st ed.). Elsevier.

Petrenko, S. (2019). *Cyber Resilience*. River Publishers.

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management* (1st ed.). Springer International Publishing.

Rothrock, R., & Clarke, R. A. (2018). *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?* (1st ed.). HarperCollins Leadership.

Talabis, M. R. M., Martin, J. L., & Wheeler, E. (2013). *Information security risk assessment toolkit practical assessments through data collection and data analysis* (1st ed.). Elsevier.

Vogt, P. W., & Johnson, R. B. (2015). Trend. In *The SAGE Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences* (5th ed.). SAGE Publications.


## Articles and Chapters in Compilations

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, Vol. 12(1), pp. 1–11. https://doi.org/10.1080/13669870802488883

Aven, T., Renn, O., & Rosa, E. A. (2011). On the ontological status of the concept of risk. *Safety Science*, Vol. 49(8–9), pp. 1074–1079. https://doi.org/10.1016/j.ssci.2011.04.015

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms*, pp. 97–104. https://doi.org/10.1145/508171.508187

Carpenter, D. (2018). Ethics, reflexivity and virtue. In Iphofen, R. & Tolich, M. (Eds.), *The SAGE Handbook of Qualitative Research Ethics*, pp. 35-50. SAGE Publications. https://dx-doi-org.libproxy.tuni.fi/10.4135/9781526435446

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems & Decisions*, Vol. 33(4), pp. 469–470. https://doi.org/10.1007/s10669-013-9484-z

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, Vol. 366(6469), pp. 1066–1069. https://doi.org/10.1126/science.aaz4795

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, Vol. 46(3), pp. 81–85. https://doi.org/10.1145/636772.636774

Johansen, I. L., & Rausand, M. (2014). Foundations and choice of risk metrics. *Safety Science*, Vol. 62, pp. 386–399. https://doi.org/10.1016/j.ssci.2013.09.011

Kloman, H. F. (2009). A Brief History of Risk Management. In J. Fraser & B. J. Simkins, *Enterprise Risk Management*, pp. 19–29. John Wiley & Sons. https://doi.org/10.1002/9781118267080.ch2

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. Wentz. Dulles (Eds.), *Cyberpower and National Security* (1st ed.), pp. 24-42. Potomac Books. https://doi.org/10.2307/j.ctt1djmhj1.7

Liu, X. (2017). Rigor. In M. Allen (Ed.), *The SAGE Encyclopedia of Communication Research Methods*, Vols. 1-4, pp. 1511-1514. SAGE Publications. https://dx-doi-org.libproxy.tuni.fi/10.4135/9781483381411.n530

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, Vol. 20(1), pp. 61–74.

McShane, M. (2018). Enterprise risk management: History and a design science proposal. *The Journal of Risk Finance*, Vol. 19(2), pp. 137–153. https://doi-org.libproxy.tuni.fi/10.1108/JRF-03-2017-0048

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, Vol. 24(1), pp. 93–125. https://doi.org/10.1111/rmir.12169

Proactive vs. Reactive. (2019). In V. L. Burton (Ed.), *Encyclopedia of Management* (8th ed.), Vol. 2, pp. 886-888. Gale.

Rosa, E. A. (2003). The logical structure of the social amplification of risk framework (SARF): metatheoretical foundations and policy implications. In N. Pidegeon, R. E. Kaspersen, P. Slovic (Eds.), *The Social Amplification of Risk*, pp. 47–79. Cambridge University Press. https://doi.org/10.1017/CBO9780511550461.003

Saunders, M., & Townsend, K. (2018). Choosing participants. In *The SAGE Handbook of Qualitative Business and Management Research Methods: History and Traditions*, pp. 480-492. SAGE Publications Ltd. https://www-doi-org.libproxy.tuni.fi/10.4135/9781526430212

Shortreed, J. (2009). ERM Frameworks. In J. Fraser & B. J. Simkins, *Enterprise Risk Management*, pp. 97–123. John Wiley & Sons. https://doi.org/10.1002/9781118267080.ch7

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security*, Vol. 11(4), pp. 33–49. https://doi.org/10.1201/1086/43322.11.4.20020901/38843.5

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, Vol. 38(1), pp. 60–80. https://doi.org/10.1145/1216218.1216224

van der Linden, M. A. (2007). Threat Modeling and Risk Assessment Processes. In *Testing Code Security,* pp. 97–130. Auerbach Publications. https://doi.org/10.1201/9781420013795-9

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

## Standards, Frameworks and White Papers

Alberts, C. J., Behrens, S.G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Framework – Version 1.0*. Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf

International Organization for Standardization. (2009). *Risk management – Vocabulary* (ISO Guide 73:2009). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

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

International Organization for Standardization, & International Electrotechnical Commission. (2018a). *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO/IEC 27000:2018). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

International Organization for Standardization, & International Electrotechnical Commission. (2018b). *Information technology – Security techniques – Information security risk management* (ISO/IEC 27005:2018). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en

National Institute of Standards and Technology. (2011). *Managing Information Security Risk* (Special Publication 800-39). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments* (Special Publication 800-30). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Lachapelle, E., & Halili, R. (2015). *ISO/IEC 27005 – Information technology – Security techniques – Information security risk management* [White Paper]. PECB. Retrieved from https://pecb.com/pdf/whitepapers/31-white-papers-iso-27005.pdf

Renn, O. (2005). *Risk Governance. Towards an Integrative Approach* [White Paper]. International Risk Governance Council. Retrieved from https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf

## Internet Resources

AV-TEST Institute. (2021). *Malware Statistics & Trends Report | AV-TEST*. Retrieved from https://www.av-test.org/en/statistics/malware/

Cybersecurity Ventures. (2021, January 21). *2021 Report: Cyberwarfare in the C-suite*. Retrieved from https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

De Mol, L. (2019). Turing Machines. In *The Stanford Encyclopedia of Philosophy*. Retrieved from https://plato.stanford.edu/archives/win2019/entries/turing-machine/

Finnish Ministry of Defence. (2019). *Finland's Cyber Security Strategy 2019*. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

IBM. (2021). *Cost of a Data Breach Report 2021*. Retrieved from https://www.ibm.com/security/data-breach

Merriam-Webster. (n.d.). Trend. In *Merriam-Webster.com dictionary*. Retrieved June 30, 2021, from https://www.merriam-webster.com/dictionary/trend.

MITRE. (2015a, April 10). Risk Impact Assessment and Prioritization. In *Systems Engineering Guide for Risk Management*. The MITRE Corporation. Retrieved from https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization

MITRE. (2015b, April 10). Risk Mitigation Planning, Implementation, and Progress Monitoring. In *Systems Engineering Guide for Risk Management*. The MITRE Corporation. Retrieved from https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring

National Cyber Security Center. (2021). *Phishing attacks: defending your organisation*. Retrieved from https://www.ncsc.gov.uk/guidance/phishing

National Institute of Standards and Technology. (n.d.-a). Cyber. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber

National Institute of Standards and Technology. (n.d.-b). Cyber-attack. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber_attack

National Institute of Standards and Technology. (n.d.-c). Cyber incident. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber_incident

National Institute of Standards and Technology. (n.d.-d). Cyber resiliency. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber_resiliency

National Institute of Standards and Technology. (n.d.-e). Cyber risk. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber_risk

National Institute of Standards and Technology. (n.d.-f). Cybersecurity. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cybersecurity

National Institute of Standards and Technology. (n.d.-g). Cyberspace. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyberspace

National Institute of Standards and Technology. (n.d.-h). Cyber threat. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/cyber_threat

National Institute of Standards and Technology. (n.d.-i). Denial of Service. In *Computer Security Resource Center Glossary*. Retrieved May 25, 2021, from https://csrc.nist.gov/glossary/term/denial_of_service

National Institute of Standards and Technology. (n.d.-j). Internet Protocol. In *Computer Security Resource Center Glossary*. Retrieved May 25, 2021, from https://csrc.nist.gov/glossary/term/ip

National Institute of Standards and Technology. (n.d.-k). Malware. In *Computer Security Resource Center Glossary*. Retrieved May 25, 2021, from https://csrc.nist.gov/glossary/term/malware

National Institute of Standards and Technology. (n.d.-l). Opportunity. In *Computer Security Resource Center Glossary*. Retrieved June 30, 2021, from https://csrc.nist.gov/glossary/term/opportunity

National Institute of Standards and Technology. (n.d.-m). Phishing. In *Computer Security Resource Center Glossary*. Retrieved May 25, 2021, from https://csrc.nist.gov/glossary/term/phishing

National Institute of Standards and Technology. (n.d.-n). Threat. In *Computer Security Resource Center Glossary*. Retrieved May 25, 2021, from https://csrc.nist.gov/glossary/term/threat

OECD. (2021a). *ICT Access and Usage by Businesses.* Retrieved from https://stats.oecd.org/Index.aspx?DataSetCode=ICT_BUS

OECD. (2021b). *Information and communication technology (ICT) - Access to computers from home - OECD Data*. Retrieved from https://data.oecd.org/ict/access-to-computers-from-home.htm

OECD. (2021c). *Information and communication technology (ICT) - Internet access - OECD Data*. Retrieved from https://data.oecd.org/ict/internet-access.htm#indicator-chart

Police of Finland. (2021). *Cybercrime*. Retrieved from https://poliisi.fi/en/cybercrime

Roser, M., Ritchie, H., & Ortiz-Ospina, E. (2015) - Internet. *OurWorldInData.org*. Retrieved from https://ourworldindata.org/internet

Statista. (2021a, January 25). *Perceptions about the development of cybercrime risks in Finland 2019*. Retrieved from https://www.statista.com/statistics/498192/perceptions-about-the-development-of-cybercrime-risks-in-finland/

Statista. (2021b, April 7). *Worldwide digital population as of January 2021*. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Statista. (2021c, July 5). *Impediments to effective cyber security implementation in companies in Finland 2019*. Retrieved from https://www.statista.com/statistics/1224964/main-impediments-to-effective-cyber-security-implementation-in-companies-in-finland/

Statista. (2021d, July 5). *Major cyber security threats of companies in Finland 2019*. Retrieved from https://www.statista.com/statistics/1224936/major-cyber-security-threats-of-companies-in-finland/

Statista. (2021e, July 5). *Number of information security violations and threats reported in Finland 2020*. Retrieved from https://www.statista.com/statistics/1224712/number-of-reported-information-security-violations-and-threats-finland/

Statista. (2021f, July 5). *Perception of information and cyber security risks in companies in Finland 2014–2020*. Retrieved from https://www.statista.com/statistics/892910/companies-perception-of-information-and-cyber-security-risks-in-finland/

Webroot. (2020). *Webroot Threat Report.* Retrieved from https://mypage.webroot.com/rs/557-FSI-195/images/2020%20Webroot%20Threat%20Report_US_FINAL.pdf

# APPENDICES

## Appendix 1: Interview questionnaire

The interview questionnaire displayed below addresses risk management in a generic way. We highlight that interviewees were always oriented to answer the questions from the cyber point of view.

1. What is your understanding of risk and risk management?

2. What kind of risk management services and/or products do you offer? Are they proactive or reactive?

3. How would you describe your risk management process and steps to me if I were your client?

4. Do you follow a specific methodology, model, norm and/or proceeding to manage clients' risks (e.g., ISO, NIST, PMI, among others)?

a. If yes, please, explain the methodologies followed.

b. If no, please, explain why.

5. Have you developed your own methodology(ies) to manage clients' risks?

a. If yes, please, explain the methodology(ies) developed if you are allowed to.

b. If no, please, explain why.

6. Do you offer customized risk management services and/or products for each client?

a. If yes, please, explain.

b. If no, please, explain why.

7. Do you develop a risk management plan before starting the risk management process per se?

8. Now, I would like you, please, to answer the below question adding the verbs listed from a. to i. to the empty space. Please, answer using all verbs that apply to your risk management proceeding at a time. If any of the verbs do not apply, please, briefly explain why not.

"How do you ____ the risks to which your clients are exposed to?"

a. Identify

b. Assess

c. Analyse

d. Evaluate

e. Prioritize

f. Treat

g. Handle

h. Control

i. Monitor

9. Do you document the risk management process that is conducted?

a. If yes, please, explain.

b. If no, please, explain why.

10. How would you describe the Finnish risk management market today?

11. Do you think that managing the positive impact of risks (opportunities) and not only the negative impact of risks (threats) is a trend in Finland? Please, explain.

12. Which other trends do you see in the risk management market in Finland? Please, briefly comment about them.

13. Please, feel free to add any further ideas or comments you have!