UNIVERSITY OF TAMPERE
School of Management

Cyber Risk Management in the Finnish Healthcare Sector

Insurance Science
Master’s Thesis
January 2018
Author: Hanne Hellstén
Supervisor: Lasse Koskinen

ABSTRACT

University of Tampere	School of Management, Insurance Science
Author:	HELLSTÈN, HANNE KAARINA
Title:	Cyber Risk Management in the Finnish Healthcare Sector
Master's Thesis:	80 pages, 2 appendix pages
Date:	January, 2018
Key Words:	Cyber risk, risk management, cyber risk management, health information system

Advances in technology and digitalization have been widely adopted by Finnish healthcare organizations. This development has led to improvements in the efficiency and outcomes of patient care, but has also exposed healthcare providers to new kinds of risks. Cyber risks are becoming an increasingly common occurrence in the healthcare sector, and can lead to serious consequences for patients and organizations alike. The significance of cyber risks within healthcare has been projected to grow, as internet-enabled applications and medical devices become increasingly ubiquitous in the industry.

This thesis attempts to examine cyber risks and cyber risk management in the context of Finnish healthcare, with a focus on the Pirkanmaa Hospital District. The objective of this thesis is to understand the significance of cyber risks, and to investigate how these risks are managed in the healthcare sector. This thesis was carried out with a qualitative research method, utilizing semi-structured interviews. The interviewees of this thesis included information security and risk management professionals affiliated with the healthcare sector.

The results suggest that cyber risks are very significant within healthcare, and that various techniques are employed in their management. Cyber risks are managed as a part of the risk management process. Operating in the healthcare sector was not found to be significant in terms of how cyber risks are managed.

Table of Contents

1 Introduction

1.1 Research Background

Technological innovation has been a driving force behind improved healthcare and patient outcome. Health information systems have provided many benefits for patients, healthcare providers, and other stakeholders, while helping to manage the rising costs of healthcare. Electronic health records have increased the continuity and safety of care by providing critical information. Internet-enabled medical devices and other automated systems have also proliferated the healthcare industry. While these developments have been a boon for society and the healthcare sector, they come parceled with new kinds of risks. (Luna et al. 2015)

Cyber risks arise from the use of IT, and can undermine the integrity, availability, or confidentiality of services or data (Eling & Schnell 2016). Various kinds of cyber risks involving the healthcare industry have broken the news barrier in recent history, receiving substantial amounts of publicity and attention. Two examples from the summer of 2017 include the WannaCry ransomware attack that disrupted the NHS in the United Kingdom, (BBC 2017) and an FDA recall of nearly 500,000 pacemakers because of hacking vulnerability in the United States (FDA 2017). Cyber events have also caused problems amongst healthcare organizations in Finland as well.

Cyber events afflicting healthcare organizations have become an increasingly common phenomenon. Research on cyber attacks in the healthcare industry suggests that well over 90% of healthcare providers have been the victims of a cyber attack. (Luna et al. 2016) Several common characteristics of healthcare organizations, including tight financial constraints and weaker cyber security infrastructure, have rendered them particularly vulnerable to cyber risks. Cyber attacks in the healthcare sector have been driven by a variety of motives, many of which involve financial gain in one way or another. (HCIC 2017,6-9) Medical information theft has become a lucrative operation, and as such it has become increasingly common. Medical records are worth more than other types of information that have traditionally been targeted for theft, such as social security numbers. (Luna et al. 2016)

Cyber risks can lead to a wide range of unfavorable outcomes for all parties involved with the healthcare sector. These include harm to patients, in addition to financial losses and damaged reputations for healthcare providers. Several jurisdictions, including the EU, have implemented regulation that force healthcare providers to consider the growing risks associated with information security and privacy. As the penalties for non-compliance can be substantial, effective cyber risk management has become a growing concern. (Blanke & McGrady 2016)

In response to the growing significance of cyber risks, new techniques to manage them have been employed. Effective cyber risk management has many elements, including cyber security, employee training, and insurance. While risk management will unlike be completely effective, it can reduce the probability and outcome of cyber risks. (Martin et al. 2017) Various entities, including the Finnish Communications Regulatory Authority and the United States Congress have also become involved in improving cyber risk management in the healthcare industry. (HCIC 2017 & Viestintävirasto 2016)

1.2 Research Problems, Objectives, and Scope

The overall objective of this thesis is to form a comprehensive picture of cyber risks within the Finnish public healthcare system, with a particular focus on the Pirkanmaa Hospital District (PHD). This objective is rather broad, so it has been curtailed with a limited scope and research problems, of which there are two:

Research Problems

1. What is the significance of cyber risks in healthcare and the Pirkanmaa Hospital District and how are they managed?

2. What is the significance of a healthcare setting on cyber risks and their management?

These research problems are related, and in some sense they mirror one another. The first research problem is concerned with how cyber risks and their management are significant for a healthcare organization, with an emphasis on the PHD. The second problem is about understanding what sort of effects (if any) a healthcare setting has regarding cyber risks. To put it in another way, one question asks how healthcare operations are affected by cyber risks, while the other asks how cyber risks are affected by taking place in healthcare. Since these two research problems are intertwined to some extent, some parts of the data analysis and theory concern both research problems.

Cyber risks, even when studied from a healthcare point of view, are a broad subject. In order to properly address the research objective, certain areas have been left out of this thesis. This has been written from a Finnish point of view, particularly focusing on cyber risks in the context of public healthcare. A significant part of the data used in this thesis has originated from the PHD, so the scope is actually limited to a single entity within Finnish healthcare. Healthcare providers like the PHD are involved with a variety of other organizations through subcontracting and other contractual arrangements. Their significance regarding cyber risks will be largely left out of this thesis. The public sector aspects of the PHD in the context of cyber risks will not be analyzed either.

Legal considerations are a central part of cyber risk management, and they are discussed in a general manner. An in-depth legal analysis is not within the scope of this study. Detailed technical information has also been omitted, even though their relevance to the subject matter is obvious. The term healthcare organization is very vague, and can be used as an umbrella term for any entity that has anything to do with health. These include health insurance, pharmaceuticals, and health related mobile application companies. The scope of this thesis covers organizations that produce healthcare services for human patients.

The overwhelming majority of the sources used in the theoretical portions of this thesis are not from Finland, and everything can’t be directly applied to Finnish healthcare. That being said, the academic research body on cyber risks within healthcare is not very large, the Finnish one even less so. It could also be argued that the origins of literature are irrelevant, given the insignificance of national boundaries in the cyber world.

1.3 Key Terms

Many of the concepts and terms relating to risk or risk management have been used to mean a variety of different things. There is a remarkable lack of consensus on even the most basic of concepts within the field. The key terminology will be defined in the next section.

Risk

ISO 31000 (2009) has defined risk as the "effect of uncertainty on objectives." Effects can be either positive or negative deviations from what is expected.

Cyber Risk

Several terms are used somewhat synonymously with cyber risk, including information technology (IT) risk and technology risk. Cyber risks can be defined as risks that can undermine the integrity, availability, or confidentiality of services or data, which arise from the use of IT. (Eling & Schnell 2016)

Risk Management

While various and distinct definitions of risk management can be found, many of them share common elements. ISO 31000 (2009) has defined risk management as "coordinated activities to direct and control an organization with regard to risk."

Healthcare Organization

Healthcare organizations are producers of healthcare services.

Electronic Health Record

Electronic health records (EHR) are records consisting of patient health and medical information, which are generated during encounters with care delivery. Electronic health records can have many different functions, and there is no consensus on a minimum standard of functions for qualification as an EHR. (Collum & Menachemi 2011; Jha et al. 2009)

Health Information System

A health information system (HIS) is a computer system that includes a range of systems and applications that are needed to run a hospital, including clinical, financial, and administrative data. (Sligo et al. 2017)

Information security

Information security can also be referred to as data security. Information security can be defined as the safeguarding of personal information from either intentional or accidental alteration, loss, destruction or unauthorized access. (Susilo et al. 2015)

Information privacy

Information privacy, or data privacy has been defined as the concern over "access to individually identifiable personal information." (Smith, Dinev, & Xu 2011)

1.4 Research Methodology

This qualitative thesis has been conducted using the semi-structured interview as a research methodology. Qualitative research encompasses a wide array of approaches and methods of study. The data collected and analyzed in qualitative research is usually, though not exclusively, non-quantitative in its nature. Qualitative research can have a variety of goals or objectives, which will depend on the object of study at hand. Qualitative research has a long history, and has been employed in a plethora of academic disciplines. (Saldana 2011, 3-4) According to Hirsijärvi, Remes, and Sajavaari, (2009, 160-164) the purpose of qualitative research is to find underlying cause and effect relationships in a phenomenon, and to make sense of what cannot be quantitatively analyzed.

The current thesis is a descriptive one. Descriptive studies can be used in quantitative and qualitative research, in order to ascertain a detailed description of some event, situation, or individual. Descriptive research relies on careful documentation of the key features of the process or subject being studied. (Hirsijärvi et al. 2009, 139) Insurance science research can be divided into three categories. Research in the first category seeks to develop theory and methods within insurance and risk management. The second group consists of applications of those theories and methods, while third category research focuses on insurance institutions and the insurance coverage they provide. (Koskinen, 2017) This thesis belongs in the second category of insurance science research, as it seeks to describe the application of risk management theory within the healthcare sector.

A research method must be selected with the objectives of the research in mind, in order to ensure its suitability (Galletta 2012, 21). Ruusuvuori and Tiittula (2005, 9) have suggested that interviews may be the most widely used method for gathering information in science as well as in everyday life. When confronted with a situation where one person does not know something, but knows somebody who might, the intuitive course of action is to simply ask that person. The objectives of this thesis relate to information that is not publically available, so interviewing those individuals with access to the knowledge is an appropriate method for answering the research problems.

Interviews as a research methodology have several advantages. Interviews are considered a flexible way of gathering information, as the interview process can be adjusted by the ongoing interview itself. The interviewee is given the opportunity to bring up what they consider to be important or worthwhile during the interview, which can differ markedly from what the interviewer had expected. These new viewpoints can provide unforeseen perspective and insight into the subject being studied. Interviews are a widely used methodology if the study concerns a relatively unknown phenomenon. In such research, the advantage of a flexible methodology for data gathering can be particularly beneficial, as it gives the researcher an opportunity to further their understanding at unexpected turns during the interview. (Hirsijärvi et al. 2009, 204-206)

Interviews also have several disadvantages. First of all, they are a slow method of data collection, as ample time for planning and preparing is a prerequisite. The interviewer has to understand what the role and responsibility of an interviewer entails, in addition to the topic of the interview itself. The second limitation of interviews concerns the tendency of many people to present socially acceptable answers, or to tailor their response to what they assume the interviewer wants to hear. Some interviewees might also be nervous or anxious during the interview, which can have a detrimental effect on the outcome. (Hirsijärvi et al. 2009, 204-206)

Interviews can be conducted in several ways. An established way of categorizing different types of interviews is by how prepared the questions are, and by how committed the interview is to those questions. (Ruusuvuori et al. 2005, 11) The semi-structured interview can incorporate an array of different elements, from broader open-ended questions to more detail-oriented questions. Different types of questions are used to illicit particular types of information. The wording and necessity of each question must be considered, as well as the structure of the questions as a whole. (Galletta 2012, 45-49) The questions used in the interviews for this thesis are presented in Appendix 1 and 2. The six interviewees for this thesis include representatives from the Pirkanmaa Hospital District, Granite, and Istekki. The interviewees and the organizations they represent are presented in greater detail in chapter 4 of this thesis.

1.5 Theoretical Framework

The theoretical framework is presented in figure 1. While strategy is a starting point for an organization's risk management process, (Ilmonen et al. 2013, 85) it will also be influenced by external factors as well. Many laws and regulations require risk management within Finnish healthcare organizations. These can pertain to risk management in general, such as in the Local Government Act (410/2015) or to a specific risk, as in the Occupational Health and Safety Act (23.8.2002/738). Many types of risk can affect an organization's operations, including cyber risks, which are highlighted in the theoretical framework. Within healthcare, cyber risks can impact the ability of the organization to produce healthcare services, and affect the outcome of patient care. Cyber risks can also have financial and reputational repercussions.

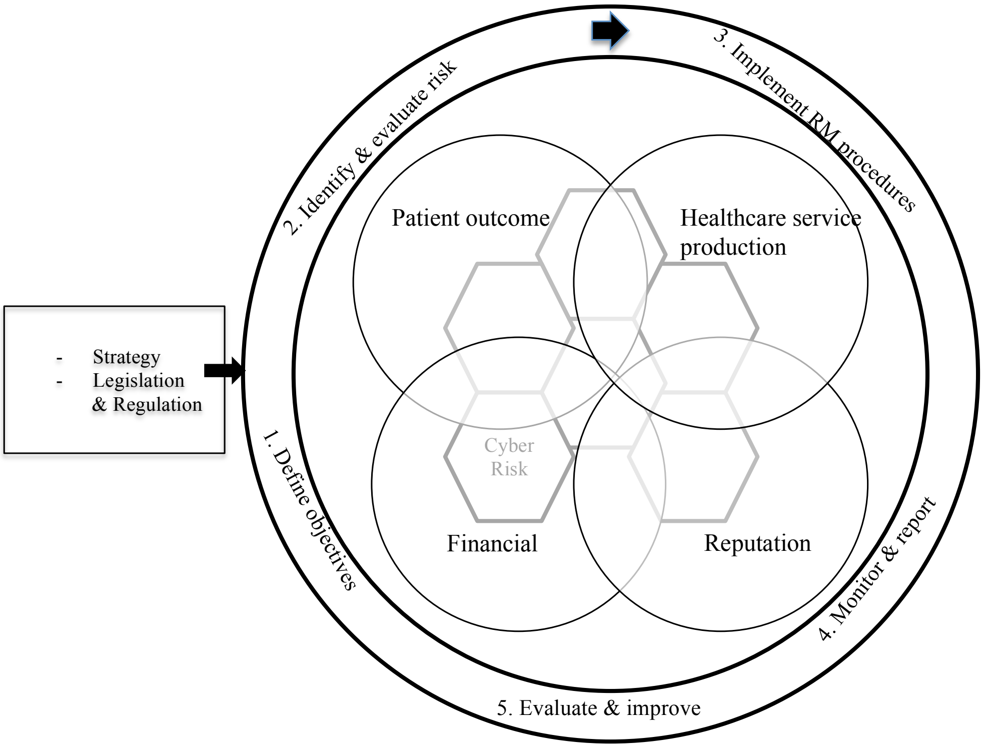

Figure 1: Theoretical framework (Risk management process: Ilmonen et al. 2013, 85)

1.6 Thesis structure

This thesis has been structured and formatted in accordance with the University of Tampere insurance science Master's Thesis guidelines. The first chapter is the introduction, which starts off with the research background. The research problems, objectives, and scope of the study are presented next, followed by key term definitions and methodology. The final parts of the introductory chapter are the theoretical framework and structure. This thesis has two chapters concerning theory of the subject matter. The first one of these addresses risk, risk management, and cyber risks from a general perspective. The second chapter takes a deeper dive into the realm of cyber risks and their management from a healthcare point of view. Chapter four contains the empirical sections of this thesis. It begins by covering the data collection process. Next comes a discussion of Finland's healthcare system and the PHD, followed by an introduction of the interviewees and the organizations they represent. The next section features the data analysis, which is divided into four subsections. The fifth and final chapter is the conclusion, starting with the results and discussion, and ending with study limitations and suggestions for future research endeavors.

2 Cyber Risks and Risk Management

2.1 Risk

All organizations encounter risk, the source of which can attributed to their own conduct or to the environment in which they exist. By acknowledging risk and the uncertainty it entails, organizations can anticipate and equip themselves to deal with various, albeit unpredictable situations. Organizations are made up of the people within them, so the actions and conceptions of these individuals will have significance on how the organization regards risk. Personal views and the understanding of risk will change from one person to the next. The level of risk inherent to some idea or endeavor might be fundamentally different if one were to ask an expert of the relevant field, or a layman. Certain dimensions of a risk can also render it to be viewed as innately riskier. For example, a risk that could potentially endanger children will be deemed more serious than if were to affect adults. (Juvonen et al. 2014, 7-14)

The idea that individuals will have varying views on how some given risk is perceived is further complicated by the fact that there is no consensus on what risk itself means. Risk has been understood in many ways, and the use of the word has changed over the years. In spoken language, the idea of risk usually relates to a threat or danger of some sort, but risk can also connote opportunity or possibility. A common way of defining risk is as a function of its outcome and probability. (Juvonen et al. 2014, 8-9) In academic texts the concept of risk may vary across different disciplines. A key component of risk is uncertainty, i.e. something with an uncertain outcome is risky. Driving is a risk, because there is uncertainty present. (Rejda 2013, 20) Jumping from an airplane sans parachute is not a risk, as the leaper's fate is quite certain and thus entails no risk (Holton 2004).

Many terms are associated with risk, such as peril and hazard. In an everyday conversation, any of the three aforementioned words can be used interchangeably to refer to something dangerous. They are actually listed as synonyms of danger (thesaurus, 2017). They do, however, mean different things. Peril is what causes a loss, such as a fire or theft. A hazard is a condition that can create or increase the severity or frequency of a loss, an icy road or unlocked door, for example. (Rejda 2013, 22)

While individual perceptions of risk will vary, a sensible approach to risk for an organization is based on a realistic impression of probability and outcome (Juvonen et al. 2014, 12-14). One of the objectives of managing risk is improved decision making, so that decision makers are able to consider what sort of impact their decisions may have regarding risk. An informed decision should also include consideration of whether it is an acceptable level of risk. Risk appetite is the amount of risk that an organization is willing to take in the pursuit of its objectives. Risk appetite is a strategic decision, and it should be taken into account when considering new business ventures, as it is useful for determining if a risk is acceptable. Different stakeholders might have varying ideas of what is an appropriate risk appetite. (Fraser & Simkins 2010, 287; Ilmonen et al. 2013, 10-13)

Risk tolerance is the amount exposure that an organization deems acceptable. It does not necessarily have to be a quantitative metric, but it can be expressed through various financial indicators such as operating losses. There is no such thing as a one-size-fits-all way of calculating risk tolerance. Different units within an organization can also have different risk tolerances, and these can also differ in the long and short term. (Fraser & Simkins 2010, 144, 287; Ilmonen et al. 2013, 10-13) Regulation and legal requirements might also be influential determinants of risk tolerance (ISO 2009).

2.1.1 Classifying risk

Several different systems have been used to classify risks, such as basing it on the source of the risk. One established categorization has four classes of risks: operational, strategic, financial, and hazard risks. (Ilmonen et al. 2013, 64) The majority of organizations must deal with all of these different types of risk in one way or another, however the nature and extent of operations will determine what risks are considered to be most relevant. Classifying risks is somewhat problematic because one type of risk can affect another; reducing one type of risk can cause exposure to another kind of risk. Because of this, risk should be approached as a whole rather than as individual parts or silos. (Juvonen et al. 2014, 29)

Operational risks are either directly or indirectly related to an organization's day-to-day functions, which are needed for the execution of its strategic objectives. An operational risk may arise out of a failed internal process or insufficient personnel. Some types of operational risks are similar to strategic risks, such as failed decision planning. Operational risks are involved in all kinds of organizational activity, as these activities can include risk. Operational risks include many types of risks, including cyber and reputation risks. Operational risks can undermine the ability of an organization to carry out its daily functions. (Ilmonen et al. 2013, 66-67; Fraser & Simkins 2010, 280)

Strategic risks involve long-term objectives and their fulfillment; they can hinder an organization's ability to carry out its business plan. Decisions have to be made, and this must be reconciled with the fact that they are based on an uncertain future. Strategic risks can be divided into external and internal factor risks. External strategic risks are related to factors outside of the organization itself, such as competitors and the state of the economy. Internal strategic risks refer to matters within the organization, such as a failure to respond to customer needs. (Ilmonen et al. 2013, 65-66: Fraser & Simkins 2010, 306, 510)

Financial risks involve an organization's use or ownership of financial instruments; they can arise from numerous sources such as foreign currency or extended credit. Financial risks in one organization can translate to problems in other organizations through agreements, which they are unable to fulfill. Financial risks are usually external, and as such, the amount of direct control over them is limited. (Skipper & Kwon 2007, 21; Ilmonen et al. 2013, 68))

Hazard risks are in a sense the clearest category of risks, as accidents are common experiences. Hazard risks can involve people, property, or the environment. Examples of hazard risks include falls and fires. The severity of hazard risks can vary substantially, and can even shut down an organization permanently. Many types of risks can be classified in various ways or may belong in multiple risk categories. (Ilmonen et al. 2013, 69)

2.2 Risk Management

The term risk management has been applied to business since the 1950's, but the use of the term itself was minimal at the time. During the early era of risk management, corporations were mainly concerned with hazard risks and insurance. The ensuing decades saw numerous developments in politics, regulation, and business trends in general, resulting in more efficient yet riskier operations. The need for a more refined understanding of risk and risk management grew, as shareholders and other stakeholders began to increasingly voice their concerns. (Skipper & Kwon 2007, 288-299)

Over the years, risk management has been understood and defined in a many ways, and these have continued to evolve through more recent events such as the financial crisis of 2008. (Skipper & Kwon 2007, 288-289) Risk and risk management often have a negative connotation, and can lead to a focus on the downside. Risk management has shifted to also include the positive side of risk, which is an integral part of the nature of enterprise. Risk management can be used to identify, evaluate, and control opportunities. (Ilmonen et al. 2013, 15) In accordance with this shift, risk management has also been defined as the "intelligent use of risk to promote business opportunities" (Yener 2007, 506)

Risk management can have internal and external drivers. Internal drivers are derived from an organization's own stance and decisions regarding risk management, such as strategy or vision. Internal drivers also include procedural guidelines and other policies. External drivers refer to risk management requirements that originate outside the organization. These can include laws, agreements, and customer demands. External drivers can form a complex framework, as the sources of these drivers are plentiful and can be quite different. (Ilmonen et al. 2013, 18-19)

2.2.1 Benefits of Risk Management

Risk management has been purported to have a wide variety of practical and theoretical benefits. According to Lam (2014, 6) these benefits include reduced earnings volatility and reduced transaction costs. Risk management is also taken into account in credit ratings, which has had an impact on the acceptance of risk management. Credit ratings are used to determine the financial strength of an organization, and their ability to meet debt obligations. Ratings agencies, such as S&P take risk management into account in evaluation. An improved credit rating can drive down the costs of capital, and is beneficial in and of itself. (Moody 2010, 467-477)

However, studying the efficacy of risk management is challenging for a variety of reasons, and research regarding its value creation has been inconclusive. First of all, risk management is difficult to identify, and secondly, it is hard to measure. There are currently many different frameworks of risk management available for organizations to use. Organizations can utilize risk management frameworks in different ways, use several of them together, or not use them at all. As a result, comparing and researching risk management is problematic. There is also a lack of clear indicators of risk management, so researchers have had to rely on proxies such as the presence of a chief risk officer. This can lead to oversimplification and misrepresentation. (Lundqvist 2014)

2.2.2 The Risk Management Process

Many versions of the risk management process have been published and utilized, but these share many common elements and standardized steps (Skipper & Kwon 2007, 22). External and internal drivers of risk management can affect what final shape a risk management process will take. Ilmonen et al. (2013, 84) have defined risk management as a systematic process, where risks are evaluated, controlled, and reported. The following five-step risk management process is illustrated in the theoretical framework (figure 1).

The first phase of the risk management process is defining objectives. At this point, an organization must evaluate the level or maturity of risk management in the current situation. The objectives of risk management at a generic level are too broad and general for them to render themselves beneficial to most organization, so they should be reformulated into concrete and specific objectives. Risk management objectives can be determined for the long and short term. Objectives for the development of the process itself can also be determined, as ultimately risk management should be an integrated feature of all daily functions within an organization. (Ilmonen et al. 2013, 86-87)

Identification and evaluation of risks is the second step in this process. Risk evaluation has two key dimensions: probability and outcome. Risk identification would ideally happen within the context of the goals of the organization. Identified risks can be recorded into a register, along with the root of the risk and possible consequences. Different kinds of software programs can be utilized in this process. While determining the exact outcome of a possible risk may not be possible, it is helpful to measure outcome in financial terms. (Ilmonen et al. 2013, 88-90)

The third step is implementing risk management procedures. In order for implemented procedures to be effective, they have to target the root cause of the risk. The selection of risk management procedures should be focused on keeping a risk at an acceptable level. Methods of managing risk usually fall into one of the following categories: avoidance, reduction, retention, transferring, and sharing. The selection of a suitable method will depend on the probability and outcome of risk. Even after the implementation of risk management procedures, some residual risk may remain. (Ilmonen et al. 2013, 90-93)

The fourth step of the risk management process is monitoring and reporting. Elements of this phase are actually included into the previous steps as well, such as logging possible risks into a register. Many applications are available to make reporting more fluent, and Excel is a popular tool for this as well. Regardless of the tools used to monitor risk management, the important thing is to keep them up to date. (Ilmonen et al. 2013, 93-94)

The fifth and final step is evaluation and improvement. If specific objectives have been defined, these can serve as the basis of the evaluation. Improvement should be a continuous element of risk management, and it should also happen according to the objectives of the risk management process. Risk management can be evaluated for an organization as a whole, or for some specific sector or process. (Ilmonen et al. 2013, 94-95)

2.3 Cyber Risk

As a term, cyber risk is rather broad as it encompasses a wide range out events and outcomes. This has lead to a variety of ways of defining and classifying cyber risks. The word cyber means the involvement of computers, networks, or the internet (Merriam-Webster 2017). “Cyber” has become an increasingly popular prefix for a medley of phenomenon, from cyber warfare, to cyber romance. According to Eling & Schnell (2016), the word “cyber” is characterized by two distinctive elements, which are virtual reality and networks. The presence of virtual reality means that risks arising from it will often be intangible in nature, and thusly more difficult to assess. While the internet is the most likely source of cyber risks, other networks are relevant as well.

Cyber risks are increasingly important for society and organizations alike, as IT has become a critical aspect of the modern marketplace. However, research on the subject has been somewhat limited. The two key problems in researching cyber risks is a lack of information, and difficulties in modeling cyber risks. Finding data on cyber risks can be difficult, as compromised organizations may not be forthcoming about incidents. Cyber risks often include a criminal element, which can further hinder data collection. This group of risks has proved itself difficult to model with the use of traditional tools, so there is little information on probabilities and outcomes of cyber risks. The fast changing nature of technology means that the current approach to modeling cyber risk, whatever it may be, must be updated constantly. (Eling & Schnell 2016)

The available information on cyber risks might also be subject to certain biases, as certain steps must occur in order for information to be available to the public. First, the cyber risk must be detected. If an event occurs undetected, it is unlikely that any record of it will be made available. Assuming that the event is detected, it may or may no be disclosed. The disclosing party may be the organization itself or another party, such as law enforcement. In certain cases, the afflicted organization will have to inform individuals if their private information is compromised in some way. In other cases, there may not be a compelling reason for an organization to be forthcoming about cyber events. Different types of cyber risks might have differing patterns of detection and reporting, causing a bias in public information and any research conducted using that data. In addition, there is no reliable method of estimating the number of unknown cyber risks. (Romanosky 2016)

Cyber risks and their consequences can be interlinked to other types of risk. Certain fundamental characteristics of cyber risk render this approach somewhat problematic, particularly as it could be argued that the academic literature and functional models of cyber risk are less developed than for other areas of risk management. According to Sheppard, Crannell, and Moulton (2013) the losses caused by cyber risks are often likened to those following a natural disaster, because their consequences and business continuity vulnerabilities are known to some degree. Natural and man-made disasters such as terrorism can be impossible to predict with accuracy, but they can be mitigated by geographic dispersion. This has been employed in the case of cyber risks as well, with dispersed IT infrastructure for example.

Modeling cyber risks with the characteristics of other types of risks has several limitations. Most natural disasters have a course of events that are somewhat predictable, while the forms of a cyber risk regarding specificity and severity can be more varied. (Sheppard et al. 2013) Guikema and Aven (2010) point out that there is a fundamental difference with risks associated with random events such as natural disasters and those involving an intelligent adversary. The triggering or likelihood of a random event is not impacted by actions taken to protect against the risk. Guikema and Aven (2010) extend this to technical failures in addition to random events. This is in contrast to risks involving an intelligent adversary, as the probability and severity of a risk can change when protective action is taken. This change is due to the action itself, but also because an intelligent adversary is able to react according to those changes.

2.3.1 The Nature of the Cyber World

According to Limnéll, Majewski, and Salminen (2014, 49) many of the fundamental characteristics of the physical world undergo a drastic change when converted into bitts. In order to navigate and manage risk in the so-called cyber world, one must first be able to understand its characteristics. Limnéll et al. (2014, 49) have found five characteristics that are fundamental in this realm: time, space, anonymity, asymmetry, and efficiency. These characteristics have had an impact on the objective and subjective experiences and safety within the cyber world.

Time is an essential determinant in the physical world and in life itself, as there is a time for most things to take place, and most things take time. Things are very different when dealing with cyber risks, as they can happen instantaneously and without warning, undermining the possibility of obviating the risk. While the events leading up to a cyber event may take ample time, it loses its meaning after the fact. The second characteristic of the cyber world relates to space. Historically, geography has been very relevant for things like commerce and the movement or communication of people. The significance of space has largely been eradicated, as everything is connected via the internet. This also means that it can be next to impossible to determine the physical location of the cause of a cyber risk. (Limnéll et al. 2014, 49-50)

Anonymity is the third fundamental characteristic of the cyber world. A challenge in cyber security has to do with identification of individuals, and the ease with which it is to keep one’s identity a secret. The possibility of remaining anonymous may bolster the temptation to do something illicit, particularly if there is little fear of getting caught. Even if one were to successfully track down the physical location of a computer for example, it does not necessarily mean that the person responsible can be determined. Individuals are also able to have many alternate identities in the cyber world. (Limnéll et al. 2014, 50)

Asymmetry is the fourth element, meaning that actors may have disproportionate size and capabilities. A small group of individuals can cause a remarkable amount of damage to a much larger entity if they are sufficiently skilled and intent on doing so. There is also asymmetry in the resources involved, as it consumes more resources to defend from an attack than to launch one. One success out of many attempts can be considered a success, but for the target this is often the other way around, because even one breach can be construed as failure. Efficiency is the final characteristic of the cyber world, as the associated risks can take on many forms simultaneously. For example, a cyber attack can target many different parts or functions of an organization at the same time. It is also worth reminding, that risk entails both the negative and the positive. These five characteristics are easily allocated as threats that arise out of the cyber world, but these very same elements are the ones that have birthed some of the most significant innovations in recent decades. (Limnéll et al. 2014, 53-55)

2.3.2 Types of Cyber Risk

Many definitions of cyber risks have been made, and the one utilized in this thesis is one of the broader ones, as it includes most of the conceivable forms that cyber risks may take. Cyber risks have been defined more narrowly as business disruption or financial loss caused by malicious electronic intent (Mukhopadhyay et al. 2013). Cyber risks have also been defined as risks arising out of information system failure. The operational risk frameworks in Solvency II and Basel III have been utilized to classify cyber risks into four categories: actions of people, systems and technology failure, failed internal processes, and external events. (Biener, Eling, &Wirfs 2015) These categories are presented in Table 1.

TABLE 1: Categorization of Cyber Risks (Biener et al. 2015; Cebula & Young 2010)

Category	Components	Description of risk source
1: Actions of people		
1.1 Accidental	error, mistake	unintentional actions, no harmful or malicious intent
1.2 Intentional	vandalism, theft, fraud, sabotage	deliberate action with harmful intent
1.3 Inaction	insufficient skills, personnel, knowledge	failing to act or take action in a situation
2: System & technology failure		
2.1 Systems	integration, complexity, specs, design	systems fail to perform as expected
2.2 Hardware	lacking capacity, maintenance, performance	failure of physical equipment
2.2 Software	security, testing, compati-bility, configurations	failure of software
3: Failed internal processes		
3.1 Process controls	review, monitoring, process ownership	process operations with inadequate controls
3.2 Process execution/design	process & information flow, documentation, alerts, agreements	poor execution/design leading to process failure
3.3 Process support	staff, accounting, training, development	supporting process fails to deliver resource
4: External events		
4.1 Business	economy, market, supplier	business environment change
4.2 Catastrophes	unrest, weather, fire, flood	events, without notice, which cannot be controlled
4.3 Legal	litigation, compliance, legislation	legal risks
4.4 Service dependence	transportation, utilities emergency services	dependence on external parties

The terms cyber risk, cyber event, cyber crime, and cyber attack are sometimes used interchangeably. These terms have been defined in many ways; there is no widely agreed upon way of differentiating between. Different views on how to discern a cyber attack from cyber crime, for example, can be based on actors, means, or the objectives of an event. Hathaway & Crootof (2012) have defined cyber attacks as "any action taken to undermine the functions of a computer network for a political or national security purpose." A widely used definition of cyber crime is "any crime that is facilitated or committed using a computer, network, or hardware device." Cyber event is a broader term that encompasses the aforementioned situations. Differentiating between different types of cyber events may not be obvious, if actors and their motives are not readily apparent. (Hathaway & Crootof 2012)

Malware is a broad category, and refers to malicious software that is used with the intent to compromise the integrity, confidentiality, or availability of data. Distributed Denial of Service (DDoS) attacks involve flooding the victim with commands to the extent that it becomes inoperable. Brute force attacks use repeated attempts to guess a password until the correct one is reached, giving access to some information. Phishing refers to techniques that are used to steal information from users by disguising as a trustful source. Social engineering includes techniques that involve human interaction in order to gain unauthorized access to information. (Bendovschi 2015)

Kendrick (2010, 24-26) has organized cyber risks into three categories: technology risks, legal and compliance risk, and operational risk. Technology risks are perhaps the most obvious of cyber risks, as they include risks that arise from the technology itself, such as computer viruses and system failures. Legal and compliance cyber risks refer to risks arising from the failure to comply with internet technology related regulation. A problem with current laws and statutes is that many of them have been formulated with the physical world in mind, and their application to the online world or networks is not always straightforward. Operational cyber risks arise from the manners in which organizations use computers and networks in their operations and practices, such as the use of company email. It is worth noting that this categorization is not always clear-cut and that there can be overlapping cases, as these classes are not mutually exclusive.

Some cyber risks can be attributed to intentional actions taken by an individual or a group. These cyber attacks can be either external or internal in origin. Internal cyber attacks are those perpetrated by individuals from within an organization. Insiders are usually entrusted with varying levels of access and information, which can be taken advantage of for personal gain. External cyber attacks are those caused by parties outside the organization. While these external attacks can take many forms, data breaches have become a particularly common type. An active internet presence is not a prerequisite for being targeted, as simply being connected online can suffice. Many of the prolific cyber attacks have involved large organizations, but small and medium-sized organizations may be more prone to cyber attacks due to lacking security procedures. (Price & Wear 2016)

The European Union Agency for Network and Information Security (ENISA) publishes a yearly report of top threats. The top 15 most prevalent threats are: 1. Malware 2. Web based attacks 3. Web application attacks 4. Denial of service 5. Botnets 6. Phishing 7. Spam 8. Ransomware 9. Insider threat 10. Physical manipulation/theft/loss/damage 11. Exploit kits 12. Data breaches 13. Identity theft 14. Information leakage 15. Cyber espionage. There was also a clear trend of improved cyber-crime monetization efficiency, meaning increased profitability for these types of activities. 2016 has also seen an improvement in cyber threat prevention through coordinated operations, certain weaknesses in anonymization tools and virtual currency, and valuable experience from undergoing serious attacks. (ENISA 2017) Other entities, such as the Ponemon Institute (2016) have published similar lists as well, which have varied to some degree.

2.3.3 Costs and effects of Cyber Risks

It is difficult to determine the actual cost of cyber risks, and the estimates that have been made vary substantially. The costs caused by cyber risks will naturally depend on what sort of definition of cyber risk is used, as different definitions will mean a different set of resulting costs. For example, if the scope of cyber risks is limited to criminal activity, the price tag will be lower than if other classes of cyber risks are included as well. Another note is that some forms of cyber risks, such as spreading social injustice may incur costs that are difficult to measure in financial terms. (Eling & Schnell 2016)

The cost of cyber risks can be attributed to multiple cost drivers, which can be traced to internal or external sources. The Ponemon Institute (2016) has published a framework of cyber event costs and cost drivers. This framework deals with cyber crime specifically, but it can be applied to other types of cyber events as well. The first of these cost drivers is usually detection, which is any activity that enables an organization to detect and even deter a cyber event, such as the overhead costs of detection technology. The second internal cost driver is investigation, which includes all activities needed to uncover the extent and source of the risk. Containment is the third cost driver, which entails activities aimed at stopping or minimizing the damage of the event. The fourth cost driver is recovery, with the aim of repairing systems or processes, such as the restoration of information assets. The fifth and final internal cost driver is the ex-poste response, the goal of which is to minimize the chance of such an event in the future. These also include costs to restrict possible business disruption and the loss of information.

In addition to the aforementioned internal cost drivers of cyber risks, external consequences are possible as well. The Ponemon Institute (2016) framework has four such external cost drivers, the first of which is the cost of lost or stolen information. Organizations may have sensitive or confidential information, which can be lost or stolen during a cyber event. This includes intellectual property, trade secrets, and customer information. In the event of lost personal information, the organization might have to notify those parties whose information has been wrongfully acquired by another entity. The second external cost driver is the cost of business disruption. Cyber risks can lead to unexpected downtime or outages, which can keep the organization from functioning as planned. Equipment damage is the third cost driver, which includes costs from infrastructure or equipment remediation. The final cost driver is lost revenue, as customers and other stakeholders might be less inclined to do business in the future.

The Ponemon Institute (2016) has studied the economic impact of cyber crime on companies, and their research results have been widely quoted. This particular study involved 237 companies in 6 countries. The average annualized cost was US$ 9,5 million (mean) or US$ 6,7 million (median). The numbers varied substantially across different countries and industries. The study also found that healthcare sector organizations had an average of US$ 7,35 million in annualized costs. The Ponemon Institute (2017) recently published a study on the cost of data breaches, involving 419 companies in 11 countries and two regions. Their results suggest that the cost of data breaches had gone down since the last year, and this is largely attributed to currency fluctuations and a strong US dollar. They found that the total cost of a data breach was US$ 3,62 million, and the cost per record was US$ 141. Data breaches involving healthcare records were pricier, at an average US$ 380 per capita.

A McAfee (2014) report on the impacts of cybercrime estimates that their annual costs are US$ 445 billion. This figure includes direct and indirect costs associated with cyber crime worldwide. According to this report, the rates of cyber crime have been on the increase as organizations, nations, and individuals are ever more connected and reliant on computer networks. The rates of cyber crime vary across the globe, and it is more prevalent in high-income countries. A significant portion of these costs are made up of intangible losses, including stolen intellectual property, lost consumer confidence, and lost business. These are inherently difficult to value and are subject to underreporting. The aftermath of cyber crime can be more expensive than the attack itself, as companies may be subject to reimbursements, legal fees and reduced valuation of the company.

A report by Norton (2016) estimated the global direct costs of cyber risks to be US$ 126 billion. Kshetri (2010, in Eling & Schnell 2016) has a much wider range of costs, between US$ 100 and 1000 billion. While the estimates that have been presented have varied quite extensively, most of them represent the views of security companies. As Eling and Schnell (2016) suggest, these types of organizations might have a biased view on the perceived threat of cyber risk. Either way, with estimates varying to such a degree, it is likely safe to conclude that the current methods of estimating the costs of cyber risk are yet to be perfected.

Romanosky's (2016) study on cyber risks has come up with a more modest estimate of US$ 8,5 billion. However, it is unclear whether his estimate is given for the US or on a global scale. He has also called into question the often-cited claim that the prevalence of cyber risks is increasing at such explosive rates. In this particular study, four types of events are categorized as cyber risks. These include personal information data breaches, malicious attacks, violations of consumer privacy, and individual financial crimes, such as phishing. Data breaches were found to be the most commonly occurring cyber risk. The most usual types of breached data consisted of names, birthdays, credit card numbers, and medical information. Compromised medical data has seen the sharpest rate of increase during the years of the dataset.

Events caused by malicious intent as opposed to accidents have not increased over the ten-year data set, and have remained somewhat stable at 60 %. Cyber risks overall have increased over the time period, but at a decreasing rate. Different types of events have seen a varying profile of growth. Data breaches have increased four-fold between 2005 and 2014, malicious attacks have risen very sharply since 2012, while privacy violations have become slightly more common. It is difficult to determine whether these patterns show an increase of actually occurring events, or just improved reporting. (Romanosky 2016)

The majority of actualized cyber risks that are reported in popular media outlets and industry publications often include a criminal element. Prolific examples from recent years can be found from most parts of the world, examples include Sony, (Elkind 2015) Osuuspankki, and Nordea. (MTV 2015) Malicious attacks represent only one sort of cyber risk, and the estimates as to their significance within all cyber events vary. As mentioned before, Romanosky's (2016) results stated that intentionality played a role in about 60 % of cyber events. The estimate provided by Marsh & HM Government (2015) suggests that over 60 % of events were accidental events in nature.   While non-malicious events were more frequent, the consequences of malicious cyber attacks were much more severe.

Cyber risks can cause different kinds of damage or consequences to organizations. These include the unavailability of IT services or information. Many organizations are highly dependent on other companies, as operations are often tied to software or platforms. Vulnerability to cyber risk can exist at several points, and failure of a large software firm such as SAP can impact a significant number of people and organizations. As more operations become reliant on networks, business interruption via cyber risk can become increasingly common. This can be exacerbated further by the fact that firms are interlinked in networks in order to take advantage of efficient strategies such as just-in-time production. While these have been a boon for many businesses, they do involve new kinds of risk. (Eling & Schnell 2016)

Data breaches and other cyber events can have a damaging effect on an entity's reputation. Confidentiality of customer information is a cornerstone of many services, including healthcare and the financial sector. These events can lead to costly financial repercussions in the form of fines and restitution. Legal considerations can also bind an organization to certain expectations, and cyber events may undermine an organization's ability to abide by the standards set by authorities. Legal consequences can lead to additional financial and reputational losses, to the extent of criminal negligence. (CRO Forum 2014)

Ensuring data integrity is critical for many types of operations. Cyber risks may weaken the ability of an organization to maintain information in its accurate form, leading to substantial economic losses, and misappropriated operations. Depending on the organization in question, loss of data integrity can lead to regulatory consequences. Cyber events concerning data integrity can be problematic, as they may not be evident because everything is otherwise functioning just fine. Cyber risks can also lead to consequences in the physical world, as key infrastructure is reliant on and controlled through networks. Examples of these can include the water supply, factories, power grids, and transportation. There have been several cases where these types of facilities have been deleteriously affected by cyber events. (CRO Forum 2014)

2.4 Cyber Risk Management Strategies

According to Ilmonen et al. (2013, 116-117) risk management strategies can be roughly divided into two types: internal risk management controls and risk transferring. The starting point of managing risk should be the use of strategies that are available within an organization; if these are insufficient, risk can be transferred to another entity with insurance, for example. Appropriate insurance is an essential part of risk management, but insurance cover should not be used as a substitute for other methods of managing risk (Kendrick 2010, 138). As stated by Ulsch (2014, 72), prevention of cyber events is always preferable to undergoing them. That being said, organizations should also prepare for their occurrence. It is not feasible or sensible to control for every risk that an organization encounters, so some sort of prioritization will take place. The costs and benefits of risk management should be aligned with the associated risk and risk tolerance for the strategy to make sense. (Ilmonen et al. 2013, 116-117)

Managing cyber risk calls for a variety of skills and areas of expertise, these include information security, regulatory or legal issues, business operations and administration, and risk management. Managing cyber risk should not happen in a vacuum, but should also take other aspects of risk and risk management into account. Refraining from the silo mentality of risk management entails a cross-functional understanding of other areas of expertise, in order to assess how cyber risks and other risks are connected. (Kendrick 2010, 133)

According to Kendrick (2010, 126-127), effective cyber risk management strategies involve the adoption of five principles. The first of these is an informed method of decision making, which includes a through understanding of the functioning, scope, and limitations of the chosen risk management strategy. Secondly, the organizational culture should include an awareness of risk and a sense that risk should not be avoided. A risk awareness culture has to be developed throughout an organization. The third principle is developing the skills needed to assess the potential costs and opportunities associated with risk. For example, analyzing the costs of acquiring a new security technology versus its provided benefits, such as improved client perception. Fourthly, the wider implications of the risk management strategy have to be understood. Cyber risks can arise from many areas, and risk management implementation effects in these should be understood simultaneously. Finally, the organization should be able to handle and appreciate the changes that come with a shifting environment. Rapid change is particularly relevant in the case of cyber risks, and newly employed risk management strategies might mean new regulatory and other considerations.

Technical solutions are a critical element of cyber risk management, and these have become a mainstay for ensuring information security and privacy. Different types of security systems can be used to protect computer systems and networks from disruptive events. Technical solutions can be implemented to conceal the content and ensure the integrity of communications. The adoption of technical solutions will largely depend on the nature and operations of the organization in question, and the type of information that needs to be secured. The level or quality of security can be analyzed with penetrative testing, which can identify possible weaknesses. (Kendrick 2010, 161-179)

2.4.1 Behavioral Perspectives on Cyber Risk Management

While technical solutions are a prominent feature of cyber security, they can prove to be ineffective if personnel are unaware or insufficiently trained (Kendrick 2010, 173). According to an IBM (2014) report, over 95% of all cyber events included human error as a contributing factor. The single most common error was opening contaminated attachments or websites, but other prevalent ones include poor password selection, lost computers, and unregulated e-mail communications. The figures that are offered for the prevalence of human error as a contributing error vary somewhat, for example Kendrick (2010, 100) writes that 70% of cases are can be attributed to human error. The research by Biener et al. (2015) shows that actions by people were behind about 90 % of cyber risk incidents. This category, however, encompasses a full spectrum of human activity, from hacking attacks to employee errors and manipulation.

While the exact figures on the significance of human behavior remain elusive, it does warrant acknowledgement within cyber risk management. Lessons from behavioral science have been utilized to gain insight and improve cyber risk management. In addition to the technical and human aspects of cyber risk, the human to machine interface is a third perspective that needs to be addressed regarding cyber risks. (Pfleeger & Caputo 2012) As told by Biener et al. (2015) a negligibly small portion of cyber incidents are attributable to pure technical failure or external events. It could be argued that people represent the weakest and strongest link in cyber risk mitigation. That being said, consideration of human behavior is crucial for successfully dealing with cyber risks. (Case 2016, 60-61)

According to Pfleeger & Caputo (2012) people are generally aware that security breaches might have consequences, but simultaneously many resist appropriate responses to security measures. For example, individuals delay mandatory password changes and perceive these requests as an annoyance. Security is usually not the primary task or focus of individuals when they are using a computer system. Instead, systems are used in order to execute some other objective, such as find information or produce documents. Security measures can be seen as an interference of the primary task at hand, which can lead to circumvention of technical risk reduction strategies. Security technology might also be mistrusted, misunderstood or misinterpreted. If users of security technology view it as a burden, they may actively seek to override it.

The solutions to human related problems in security measures have traditionally been strict control and training. These measures have been viewed as ineffective, and there have been calls for a shift towards more human-centric security and technology. The last decades have seen a significant amount of research on the cognitive abilities and biases that humans typically possess. Many of the standard security technologies utilize methods that are counterintuitive with the ways that people learn and process information. People have a much easier time recognizing something rather than recalling it. The working memory of humans can only handle a certain amount of information, and memory overload can interfere with performance. If somebody is focused on their primary task, they may not notice extraneous albeit necessary security related matters due to inattentional blindness. There is also an extensive list of cognitive biases that may have cyber security related implications. (Pfleeger & Caputo 2012)

Schneier (2016) believes that users are not the problem. Rather, the underlying problem is that cyber security design demands impractical behavior from its users. The examples he lists include the extensive number of passwords people are expected to remember and warning signs that are so common that they only cause habituation. Victim blaming is also a common phenomenon. Educating and training users is an important step of cyber risk mitigation, and training should take human behavior into account. Systems should be designed to work with human cognition and behavior, rather than against them. (Schneier 2014)

Korpela (2015) suggests that culture and society are growing increasingly dependent on information, and that information systems will continue to face risks. Education and training can be used as a method to mitigate these risks. Training often takes the form of an awareness campaign, where the objective is to focus attention on cyber risk related issues. The training is often presented in a uniform format for all, which does not allow for personalized training or identification of users with high-risk behavior. Personalized training can be accommodated to fit an individual's learning needs and their day-to-day job related activities. Korpela (2015) also mentions that certain profiles and behaviors are associated with higher cyber risk susceptibility. An individual's position within an organization might also be indicative of associated risk, but this may not be straightforward to determine. She suggests that organizations use data analytics to determine an optimal allocation of resources for cyber risk training and mitigation.

2.4.2 Cyber Risk and Insurance

Insurance policies have typically excluded cyber events from coverage. This has changed to some extent in recent years as new insurance products are being introduced to the market, particularly from the US. Insurance coverage for cyber risks has been low in all parts of the world, with around 6 % of US and 10% of European corporations having purchased cover. These numbers fluctuate substantially from one sector to another. The insurance products and the coverage they provide, including definitions and exclusions, vary amongst different insurance providers. The underwriting process in cyber insurance is a challenge, as in most cases the product needs to be customized. An organization's web presence, type of information handled, and size of customer base will factor into the pricing and terms of the insurance policy. (Biener et al. 2015)

Risks must fulfill certain criteria in order to be considered as insurable risks. Several frameworks for these axioms of insurability have been presented. Biener et al. (2015) have analyzed cyber risks in the context of Berliner's (1982 & 1985) criteria of insurability, which are presented in table 2. Each one of the nine criteria is necessary, and any one cannot be replaced by the remaining eight (Berliner 1985).

TABLE 2: Requirements of insurable risk (Berliner 1985 & Berliner 1982 in Biener et al. 2015)

Criteria	Requirement
Actuarial-mathematical criteria	
1. Randomness of loss occurrence	predictability and independence of loss exposures
2. Maximum possible loss	not catastrophic
3. Average loss per occurrence	moderate
4. Loss exposure	large enough
5. Information asymmetry	no excessive moral hazard or adverse selection
Commercial criteria	
6. Insurance premium	reasonable premium and cost recovery
7. Cover limits	acceptable
Societal criteria	
8. Public policy	socially acceptable
9. Legal restrictions	coverage is legal

Baer and Parkinson (2007) have suggested that the interdependence and correlation of cyber risks may be a barrier to the expansion of cyber insurance. Many systems use the same elements and are designed in similar ways, making them susceptible to the same losses. Certain types of cyber events are also designed to spread through various systems. Biener's et al. (2015) analysis contradicts this logic, as in their study less than 17% of cyber incidents were related to losses from other organizations. The second criterion concerning maximum possible losses does not appear to be as problematic. While the historical record of cyber risks is arguably short, it suggests that losses from cyber risks are much lower than the losses from other types of operational risks. Insurance companies are also able to protect themselves with coverage limits. Cyber risk data is scarce, and insurers have dealt with the ensuing uncertainty by setting low coverage limits.

As mentioned in section 2.3.3, various estimates of cyber risk losses have been presented in the literature. Biener et al. (2015) have found that the costs of cyber risks can vary, depending on factors including firm size and sector. They conclude that average losses per event are not an obstacle to insurance. The study also found that cyber risks have increased in number over the last years, but the levels of increase vary according to the underlying causes of risk. Loss exposure depends on the industry, but in general it should not present a problem for cyber insurers.

Information asymmetry includes moral hazard and adverse selection, both of which are problematic for the insurance market and could impede the development of cyber insurance. Moral hazard refers to a phenomenon where an individual, having purchased insurance, now lacks the incentive to exercise precaution or self-protective measures that would reduce the severity or probability of loss. (Biener et al. 2015) Baer & Parkinson (2007) mention that moral hazard can be problematic for cyber insurance, but that this problem is pertinent to all types of insurance. Over time, insurance providers have developed ways to remedy moral hazard, resulting in functioning insurance markets. This sort of learning process could take place in the cyber insurance industry as well.

Adverse selection means that high-risk individuals will have a higher demand for insurance at some given premium than lower risk individuals. This will lead to a growth in losses for the insurance company and drive up insurance premiums, which in turn will encourage low-risk individuals to opt out of the insurance pool. The lack of public data on cyber risks can make it difficult to ascertain the level of risk of a given entity. There is also some evidence that those organizations that have encountered losses due to cyber risk are more likely to purchase cyber insurance. This could lead to heightened adverse selection and hinder the cyber insurance market. (Biener et al. 2015)

As mentioned in this section, providing cyber insurance involves certain challenges. Cyber risks mean a great deal of uncertainty on behalf of the insurance companies, which has driven up cyber risk insurance premiums. (Biener et al. 2015) According to Shackelford (2012) the premiums of cyber insurance have come down in recent years, particularly for small and medium sized companies. Cyber risk insurance policies usually come with a cover limit, and these will vary among providers. The acceptability of the cover limit will depend on the policyholder's cyber risk exposure and risk tolerance. Certain types of losses from cyber risks may also be excluded from coverage, leading to very complex policies. There is also the problem of the dynamic nature of cyber risks, so it can difficult to determine if an existing policy will be worth its premiums in such an uncertain landscape. (Biener et al. 2015)

Several concerns pertaining to cyber insurance have been raised in the literature. One such concern is that access to cyber insurance may lead to an increase in some types of crime, such as hacking and insurance fraud. If organizations use insurance at the expense of other forms of cyber risk mitigation, it could lead to losses of social welfare. Research on cyber insurance suggests that it is associated with other types of cyber risk management, such as improved security measures. It has also been suggested that cyber security has positive externalities and that it has the characteristics of a public good. Cyber risk insurance involves a number of legal considerations, which will change from one jurisdiction to the next. For example, insurance for regulatory fines is illegal in some countries. Laws and regulation are also subject to change. (Biener et al. 2015)

2.5 Legal Environment of Cyber Risks

There is no law making body for the international community. However, states may consent to being bound to an obligation with either actual or implied consent. Actual consent can consist of signing a treaty, while implied consent refers to general principles of law and custom. These sources of law are not static, as they evolve to accommodate changing circumstances and situations. Intentional cyber attacks have been analyzed in the context of various conventional principles, such as prohibition on the use of force and the principle of non-intervention. While it has been held that cyber attacks can be considered as violations of some of these conventional principles, the analysis is highly nuanced and far from clear. This analysis has also raised some interesting questions, concerning matters such as territorial sovereignty in cyber space. Suffice to say, cyber space is a particularly nebulous part of international law. (Payne 2016)

According to Johnson (2016), cyberspace governing can be likened to a highly industry specific patchwork of national and international regulation. This approach has led to substantial gaps in regulation and oversight, in addition to a wide range of practices on a global scale. The nature of cyber risks and the cyber world itself render it somewhat problematic to regulate. Traditionally, a nation may regulate the activities that go on within its borders, but this conventional wisdom is difficult to apply as national borders have become increasingly insignificant. Furthermore, no single regulator has the authority to address lapses in regulation because of limited jurisdiction. This trend can be seen in other sectors as well, such as international financial markets. While no international law for governing cyber space exists now, several entities such as the United Nations and the Council of Europe have initiated efforts to do so.

2.5.1 European Union Regulation

The notion of privacy as a fundamental right became established during the post-World War II era in Europe. The right to privacy was recognized in multiple pieces of legislation across the continent; laws have been redrafted periodically to accommodate the changing landscape of privacy. For example, in 1981 the European Council enacted a convention that took the increasing use of computers in personal data handling into account. Since the creation of the EU in 1993, data privacy activity and regulation has increased substantially. The result has been a diverse legal framework of data privacy amongst EU member states, as application and enforcement of EU regulation has been inconsistent. This existing patchy framework has been seen as detrimental for business growth and citizens' rights. It has also been difficult to apply to certain fixtures of the cyber world, such as social networks and pervasive data collection. The ongoing reform can be seen as the latest evolutionary step in European data protection law. (Rotenberg & Jacobs 2013)

The European Commission published a proposal for data protection reform in 2012, the objective of which was "to make Europe fit for the digital age." The rules and framework for the reform were agreed upon in 2015, and were adopted by the European Parliament and Council in 2016. (EC 2017) The reform includes two parts: the General Data Protection Regulation (GDPR) (2016/679), and the Data Protection Directive (2016/680) for the criminal justice and police sector; these are referred to as the Regulation and the Directive. Both have entered into force in 2016; as of May 2018, the Regulation will apply and the Directive must be transposed into national law. This reform will repeal certain pieces of existing legislation. (EC 2017)

A detailed description of the reform is beyond the scope of this thesis, but some of its key elements will be presented next. The GDPR has redefined, and in effect, expanded the meaning of personal information by including new types of data into its realm, such as genetic information and online identifiers. The burden of responsibility has been shifted from consumers to the controllers of the data, who must obtain some form of explicit consent for a specific purpose. The intention behind this is to strengthen the individual's control over their personal data. Furthermore, an individual's rights to erase, correct, or access their personal information will be increased. The GDPR will also obligate data controllers to implement plain language transparency principles and policies. (Rotenberg & Jacobs 2013)

The result of these changes is that controllers of personal data will be considered responsible and liable for it. In the event of a security breach, a data controller will be obligated to notify those people whose information could be affected in addition to the supervisory authorities. (Rotenberg & Jacobs 2013) The rules imposed by the GDPR are more stringent than some of the other regulatory frameworks that can be found in other parts of the world. The GDPR will have an impact on parties outside the EU as well. The Regulation applies to data controllers, who collect information or offer goods and services to European citizens, even if the organization is located outside the EU. The objective is to level the playing field with regard to data privacy regulation for companies on an international scale and enhance business efficiency. Improved consumer confidence will have a positive impact on economic activity. (EC 2017a)

The EU has also taken legislative action against cyber crime, including the 2013 Directive on attacks against information systems. The objectives of this directive include defining criminal offences, appropriate sanctions, and improved cooperation between authorities. The Directive also mentions that criminal activity in the cyber world is becoming increasingly problematic and that attacks are happening on a larger scale. The language of the Directive is vague regarding exactly what sort of actions and tools are tantamount to criminal activity. This is expressed in the Directive itself, as technological development happens so quickly any rigidly defined set of cyber crimes might become outdated fast. As a Directive, this piece of legislation represents an approximation of the legislation that member states will have to enact in their respective jurisdictions. (2013/40/EU)

2.5.2 Finnish Cyber Space Regulation

The central piece of a national legislation concerning information privacy is the Personal Data Act (523/1999). This is a general law and it includes the general principles of data privacy. However, hundreds of other laws also involve information privacy or protection in some capacity. The GDPR is a regulation, and as such it will be applied as is in all EU member states, including Finland. As a regulation, the GDPR will override any national laws that are about the same subject matter, in this case information privacy. That being said, countries do have some discretion concerning EU regulations. As of 2016, the Ministry of Justice will be going over this extensive body of legislation in order to determine whether the laws conform to the GDPR. Any discrepancies between existing national legislation and the GDPR will have to be addressed. (Oikeusministeriö 2015)

Finland does not have a cohesive body of legislation concerning many aspects of cyber risks. Different elements of cyber risks are addressed in a variety of laws, and these have taken on many perspectives. The result is a myriad of definitions and levels of authority that are situation and sector specific. Rights that are laid out in existing laws, such as the Constitution of Finland (731/1999) can be extended to include things like freedom of speech online. The objectives of developing national regulation include the consideration of international cooperation, EU law, and the fast changing nature of cyber risks. (Valtioneuvosto 2013)

3 Healthcare Cyber Risks and Risk Management

3.1 Relevance of Cyber Risks in Healthcare

Cyber risks of various sorts have been on the increase within the healthcare sector during the last years. A steady increase in these events has been reported by academic sources as well as regulatory agencies. 2016 has been considered the worst year on record for healthcare cyber events in terms of recorded breaches. (HIPAA 2017; Rubenfire 2017) It has been speculated that medical information theft in particular will continue to grow due to its financial incentives. The two most common reasons behind intentional cyber attacks include financial gain and disgruntled employees. Unlawfully obtained medical information can be sold, used for identity fraud, illegitimate medical practice, or insurance fraud. (Luna et al. 2016) Information housed by healthcare organizations can also be used to access patients' financial and billing data, or to obtain prescription drugs illegally (World Medical Association, 2016). Politically or ideologically driven cyber attacks have also been recorded (Lehto & Lehto 2017). Other possible motives include disruption of patient care or hospital systems, stock manipulation, and supply chain interference (HCIC Task Force 2017, 6).

Cyber attacks can be untargeted, rather than being planned for some specific victim. These types of untargeted attacks will inevitable impact healthcare organizations as well. There has also been a hike in the number of targeted attacks specifically for healthcare providers. (Lehto

& Lehto 2017) Luna et al. (2016) also report that these events can be intentional and strategically planned. The banking and finance sector has traditionally been a target for cyber attacks, and cyber risks continue to be an important matter in that field. According to Lehto and Lehto, (2017) there has been an increasing shift towards the healthcare sector because of its vulnerabilities and potentially higher profits.

A Ponemon report (2016a) states that nearly 90% of healthcare providers surveyed had dealt with a data breach within the last two years, and half of these organizations had more than five breaches in that time period. Another study found that 94 % of healthcare providers had fallen victim to a cyber attack (Luna et al. 2016). A study by Lehto and Lehto (2017) analyzed 59 cyber attacks within the healthcare sector worldwide during the years 2013-2017. Many of the cases in their study involved the personal information of millions of individuals, with one case totaling 80 million people.

The WannaCry malware attack during the spring of 2017 made international headlines as it disrupted hundreds of thousands of computers in 150 countries, including 61 NHS organizations in the UK (BBC, 2017). This attack was not directed at the healthcare sector, but it compromised patient safety and affected care delivery. Other attacks have been orchestrated for healthcare organizations in particular. In 2016, a hospital in Los Angeles, California was prevented from accessing medical files or using medical equipment until a ransom was paid. During that same year, a hospital in England had to transfer patients and cancel operations because of ransomware. (Martin et al. 2017) Another scheme involved hacking a plastic surgery clinic and blackmailing celebrity patients with nude photographs (Lehto & Lehto 2017).

The previous examples have been driven by a financial motive, but others have been reported as well. In 2016, the Australian Red Cross Blood Service had over 1.28 million records of donor data stolen. The information, a lot of which concerned at-risk behavior of donors, was posted on a public website for the sake of highlighting weak security. Other examples that have been made public have been driven by political or propaganda purposes, such as the Islamic State attack on the NHS. (Martin et al. 2017)

Examples can be found from Finnish healthcare organizations as well. In 2015, the Hospital District of Southwest Finland experienced two ransomware events. In both cases, a single computer was affected from using Facebook and Internet Explorer. The affected computers were located quickly, but 30,000 files and the appointment notification system were damaged. The hospital district did not agree to pay the ransom. (VSSHP 2015) The Hospital District of Helsinki and Uusimaa has also experienced 4 ransomware events, which effected internal files in the spring of 2016. Ransom demands were not met in this case either. (Yle 2016) The Patient Data Repository has encountered several distributed denial of service (DDoS) attacks in 2016 and 2017, which have taken down the patient information database, medication database, and the Prescription Centre. (HS 2017 & MTV 2016)

In the United States, Congress has established the Health Care Industry Cyber Security Task Force (HCIC) with the Cyber Security Act of 2015. The motivation behind this new task force is to address the mounting cyber threats that the healthcare sector has to encounter. While cyber risks may lead to a wide variety of poor outcomes, including identity theft and fraud, the most significant of these according to the HCIC Task Force is the disruption of patient care. (HCIC Task Force 2017, 1) The Finnish Communications Regulatory Authority has also published a guide to cyber security in the healthcare sector. This report is intended to start a cyber risk dialogue in healthcare management and highlight the significance of these risks in healthcare. (Viestintävirasto 2016)

3.2 Healthcare equipment and information systems

The last decades have seen advances on many fronts, which have been harnessed into improved healthcare and medical outcome for a variety of diseases. For example, the rapidly declining rate of stroke mortality has led to improved population health, and has been heralded as one of the top ten public health achievements. While the exact reasons are not clearly known, they are generally attributed to improvements in the following areas: better diabetes and hypertension intervention, reduced smoking, better pharmacological agents, and technological advances in care systems and treatment. Improved organization of stroke care delivery may have had the greatest impact on stroke mortality decline. (Lackland et al. 2014) The so-called gold standard of stroke treatment is the prompt administration of clot dissolving medication. At Tampere University Hospital, the initiation of this treatment takes 20 minutes on average, and four out of five treated patients will return to an independent life. This is made possible by the seamless coordination of emergency dispatch, medical imaging, inpatient care, and many other units. (PSHP 2015a) While this necessitates a lot of the right people, doing the right things, in the right place, at the right time, it would not be possible without today's healthcare equipment and information systems.

Health information systems have brought substantial benefits for improved quality of care and cost efficiency. Electronic health records (EHR) have helped in the management of chronic conditions and critical care. In the ideal situation, an EHR would contain all of an individual's health related information over the course of their entire life. This includes medications, laboratory results, images, diagnosis, and a plethora of other personal information. The popularity of health related mobile applications as well as medical devices is on the rise, meaning that there are more potential points for failure or entry into systems containing health information. Cyber risks of various sorts can impede information security and privacy of health information systems. (Luna et al. 2016)

Luna et al. (2016) estimate that about 95 % of eligible hospitals utilize EHRs and other health information technology. In Finland, all public sector healthcare providers, and almost all private healthcare organizations have adopted electronic health records. The prevalence of this type of technology is higher in Finland than in most other parts of the world. In addition to the health information systems that are utilized by healthcare providers for recordkeeping and communicating with one another, the role of the patient as an active participant is a growing trend. Patients are able to view their information, such as in the Patient Data Repository and in some cases upload their own medical data, such as blood pressure measurements taken at home. (Lääkäriliitto 2016)

EHRs represent about 10 % of a hospital's information systems, and these are often deemed as the most critical. Individual specialties and departments, such as medical imaging or anesthesia, also have their own systems. A healthcare provider will also need applications for administrative work, billing, human resources, communications, productivity software, and security, among other tasks. Depending on the organization in question, these can add up to 400-800 systems in total, with 500 connections between them. (Lehto & Lehto 2017)

A modern hospital relies heavily on a variety of infrastructure and medical devices that are increasingly connected and internet-enabled. These include infusion pumps that are used to administer medications, pacemakers, and anesthesia machines. These devices facilitate smoother and more automated care. An update in a patient's drug dosage information in their EHR can automatically be adjusted at the infusion pump. A patient can be hooked up to many devices and monitors at a single time. The development of these connected medical devices has been a very positive one for patient care, and their prevalence is projected to grow substantially in the future with new technical advances. Medical devices can be considered as the most significant source of cyber risk within healthcare. (Lehto & Lehto 2017) Luna et al. (2016) also point out that medical devices contribute largely to healthcare data breaches. Hundreds of malicious attempts have been tracked, such as ransomware on radiology equipment. These have caused substantial costs and disruption for healthcare providers and patients. Fortunately patients have not been harmed. (Fox-Brewster 2017; Perakslis 2014)

Medical devices involve information security and privacy risks, but more significantly they can cause physical effects, such as injury, illness, or death to their user. Security features should be considered in the design and making of these devices, but this can be difficult due to the quick evolution within technology. (HCIC Task Force 2017, 18) The security features of medical devices have traditionally not been in the forefront during their development and acquisition (Lehto & Lehto 2017). So-called legacy devices refer to older pieces of equipment. These machines in particular have not been designed with modern cyber security issues in mind, and in many cases are no longer supported with software updates and are difficult to replace. Healthcare providers can also have very modern information systems and equipment, resulting in a complicated technical infrastructure. (HCIC Task Force 2017, 2,22-23)

New types of medical devices are being developed that are used outside of a hospital setting. While this is beneficial for patients and their healthcare providers, it does mean that special precautions regarding the functioning and security of the devices and networks will be warranted. (Lehto & Lehto 2017) An insulin pump can be connected to a blood glucose monitor, which can be tracked in the patient's blood sugar record. This is very convenient for the patient, and beneficial from a clinical perspective point as well. The connectivity of these components must be reliable, or it may harm the patients. It also leads to a higher rate of dependence on this technology. (HCIC Task Force 2017, 10)

The use of mobile devices in healthcare is also on the rise. Mobile devices are very convenient and confer many benefits to their users. These advantages are, however, problematic from a risk perspective. Mobile devices are easily lost or stolen, and they can be used in an inappropriate location. Their security features are not as fully developed as their traditional counterparts. (Lehto & Lehto 2017)

3.3 Cyber risk vulnerability in healthcare

The primary objective of the healthcare sector and healthcare providers is very patient-centered. Resources are typically allocated in a manner that makes it possible to help the most patients. While healthcare providers do have other objectives, including security considerations, these can often be given less priority in the daily operations of the facility. Precautions that are necessary to ensure cyber security can be interpreted as a hindrance. For example, workstations can be left unlocked in order to respond to clinical issues as fast as possible. Typing in a password and waiting to log on can take a few moments, which can delay the primary objective of taking care of patients. Unlocked workstations can save some time, but it can also lead to unauthorized access or alteration of information. (HCIC Task Force 2017, 9)

Many healthcare providers are also very public entities. Many of them are open all day, every day, and there are few, if any, restrictions on who is allowed to enter. Even for the personnel, it is not always possible to tell if somebody is not supposed to be there. The hospital staff itself changes on a fairly swift basis as well. Temporary staff and rotating shifts are also commonplace. (HCIC Task Force 2017, 9)

Healthcare organizations also tend to spend fewer resources on cyber security compared to other sectors. In other sectors, 5-15 % IT resources are spent on security, while the figure is 3% in healthcare. (Lehto & Lehto 2017) Healthcare organizations have been found to lag behind other sectors in other aspects as well. Outdated technology and a lack of information security processes have been found to be more predominant in healthcare. (KPMG 2015) Many hospitals must also operate under tight budgetary constraints. Financial reasons are also a key reason for the large amount of legacy devices that are currently used by healthcare providers, as it is not feasible to replace expensive equipment because of updated operating systems. (HCIC Task Force 2017, 28)

There tends to be an assumption of cyber security amongst healthcare providers and workers (HCIC Task Force 2017, 2). A study done by the Sans Institute (2014) also found there seems to be a gap between perceived security and reality, which is indicated by a high level of security breaches. Healthcare organizations must take certain steps to ensure compliance, but this does not necessarily mean the same thing as security. Another Sans Institute (2013) study found that regulatory compliance was the most important driver for security in the healthcare sector. Regulatory issues were also found to be the top cyber security concern for healthcare providers in a KPMG report (2015). Using the standards set by the regulatory framework may not be sufficient to maintain security (Sans Institute 2014).

3.4 Particularities of Health Information Privacy

Ensuring the privacy of health information is one of the objectives of cyber risk management within the healthcare sector. While information privacy is an important consideration for most, if not all, types of organization, the nature of health information and healthcare has some unique qualities regarding the notion of privacy. At some level, awarding health information special privacy considerations makes intuitive sense. After all, one might be hard pressed to come up with an area of information more private than health. Health records document intimate details about mental and physical status, relationships, lifestyle, and can give away financial information (Nass, Levit & Gostin 2009). This perception of specialness is also supported by the fact that some jurisdictions have legislation in place to specifically bolster health information privacy. But why is this, what is it about the nature of health information that special precautions are warranted to ensure its privacy?

Health information privacy can be justified using the principles of bioethics. According to the principle of nonmaleficence, patients should not be intentionally harmed or injured. While mistakes unfortunately can, and do happen, this principle confirms the need for sufficient competence in healthcare. The principle of beneficence states that healthcare providers have a duty to benefit the patient. Actions should be taken to prevent harm from occurring. This principle affirms that patients can trust that the main objective of their healthcare provider is to help them. The provision of benefit and protection from harm can be applied at the individual and societal levels. Certain measures, such as vaccination programs can be beneficial to a specific patient, but they also provide benefits to public health in general. (McCormick 2013)

The principles of bioethics have been extended to healthcare privacy. Breaches in privacy can cause significant harm and loss of dignity to a patient. Personally identifiable health information can cause stigma, discrimination, and embarrassment, and it can be used to the disadvantage of the person. Health information can have a detrimental impact on an individual's relations with their employers, insurers, family members and other parties. As such, healthcare providers must take steps to ensure that privacy can be maintained. The repercussions of mismanaged health information and a breach in privacy can be so significant, that people would not be willing to disclose certain types of information to their healthcare provider. An assurance of privacy is necessary for a patient to be candid about their personal information. (Nass et al. 2009)

If patients feel that they cannot be forthcoming to their healthcare provider, it can cause a negative impact on their own health, and have ramifications at a societal level as well. For example, people may feel less inclined to allow researchers to use their medical information if they have privacy concerns. It is important to note that two people may feel very differently about what sort of information they consider to be private. Research suggests that cultural background, age, and health status will have an impact on what health information privacy expectations an individual will have. For example, a teenager seeking medical attention for substance abuse or reproductive health matters will probably be very concerned about information privacy. (Nass et al. 2009)

3.5 Legal Considerations of Health Information Privacy and Security

Healthcare related information security and privacy are regulated in Finland with national and EU laws. Some of the national laws and regulations are specific to the healthcare sector, but general laws are applicable as well, such as the Personal Data Act (523/1999). The Act on the Status and Rights of Patients (785/1992), among others, sets the guidelines for healthcare record keeping and patient confidentiality. A series of other laws address matters pertaining to the creation and storage of medical records, and electronic medical records in particular. (STM 2017i)

The GDPR has not been designed for health information specifically, but it does mean changes to the legal landscape of health information privacy and security. The new regulation has defined “data concerning health” as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”. Article nine of the GDPR prohibits the processing of certain types of personal data, including genetic and health data. The regulation includes a list of exceptions or circumstances where this prohibition does not apply. (Regulation EU 2016/679)

Healthcare organizations will have to make sure that their operations fall into one of the categories where the prohibition of processing health information does not apply. Some of the circumstances outlined in the GDPR include explicit consent from the data subject, processing deemed necessary for public health, information that data subject has made public, and protection of a data subject’s vital interest. Member states are also allowed to introduce further conditions for health information processing, which will also have be taken into consideration by healthcare organizations. (Regulation EU 2016/679)

3.6 Managing Cyber Risks in Healthcare

Various types of cyber risk management guidelines and checklists have been published in the academic literature as well as in industry and government publications (ex. Blanke & McGrady 2016; KPMG 2015; HCIC Task Force, 2017). These different publications have taken a variety of approaches to managing cyber risks. On one extreme are itemized checklists of fairly detailed instructions for reducing cyber risks. Examples from the other extreme call for multi-sector cooperation to risk management and other broad tactics. These different approaches do not necessarily negate the need for other types of guidance, as they are so contrasting in their nature. It could be argued that there most certainly is a need to address cyber risks on many levels, and that different approaches aim to do just that. What does become clear after comparing different types of risk management strategies is the need to consider the technical and human factors involved.

For the most part, these healthcare specific guidelines are very similar to generic versions and could be applied to most types of organization. That being said, certain features and particularities of the healthcare industry should be taken into account. Risk analysis includes the analysis of vulnerabilities and hazards, which will involve some of the sector specific factors of healthcare. Research of actual cyber events within healthcare is also of value for the management of these risks. Awareness of potential problem areas can lead to increased vigilance and help management respond to these types of risks. (Blanke and McGrady 2016)

KPMG (2015) has suggested several steps to mitigate cyber risks in the healthcare sector, which are reminiscent of the principles of ERM. The organization should be analyzed from a broad perspective with regard to cyber risks. Healthcare organizations work with various other entities within their value chain, which must be considered as well. Third parties should be engaged in order to understand and mitigate possible risks associated with them. Cyber security awareness should also be increased in all levels of an organization, and not just as an IT department issue. There should also be a coordinated and well-prepared team charged with cyber security. Cyber security should also be incorporated into the design of technology that is used in healthcare.

Blanke and McGrady (2016) suggest beginning with an overall assessment of the current security practices, and ensuring that they are in compliance with regulation. Existing security practices should be compared to best practice standards for possible gaps. The entire organizations must be educated and trained in security awareness, with a particular focus on the most relevant matters. Education must be augmented with regular reminders of cyber security matters. Blanke and McGrady (2016) found that the most common cyber risks in healthcare were related to portable devices and malicious insiders. They suggest that cyber security and training should particularly focus on these two problem areas, as actualized cyber events have usually involved them.

The use of mobile devices has become proliferated in the healthcare sector, and steps taken to curb risks associated with the use of these devices should be planned according to what they are used for. For example, if a mobile device is used to handle confidential data, encryption will be needed. Automatic logging off and password-protected screensavers can also be used to curb some of the security shortcuts that might be taken in a healthcare setting. (Blanke &

McGrady 2016) Filkins et al. (2016) point out that these traditional types of security measures, such as complicated passwords, are becoming insufficient for the current environment, and that user awareness is the most important factor. Passwords, for example, are the most commonly used method of secure authentication, even though they have been shown to be the weakest link in security for over twenty years. Managing malicious insider related cyber threats is challenging, and should be considered during all phases of employment (Blanke & McGrady 2016). The healthcare industry's personnel profile can make this challenging, because many different types of employees and volunteers are used (HCIC Task Force 2017, 9).

The HCIC Task force (2017, 21) has come up with six imperatives for managing cyber risks within healthcare: 1. Healthcare industry cyber security expectations, governance, and leadership must be streamlined and defined 2. Medical device and health IT need increased security and resilience 3. A healthcare workforce capacity to ensure cyber security awareness and capabilities should be developed 4. Improved security awareness and education to increase readiness 5. Protect intellectual property and R&D from attacks 6. Better information sharing of threats, risks, and mitigation within the industry. This list of imperatives comes with many recommendations, which cover a range of issues and relevant parties. This guideline can be considered as one of the most holistic and broad spectrum of the available publications.

The HCIC Task Force (2017, 83) has worked in conjunction with representatives from other critical infrastructure industries to gain a better understanding of cyber risks, and learn best practices. While healthcare shares some common features regarding these risks with industries like finance and energy, certain unique aspects were uncovered as well. These must be taken into consideration in cyber risk management strategies, and make it difficult to adopt best practices in their exact form from other industries. The key findings include the following: healthcare organizations vary considerably in terms of size and types of activities. There is also a lot of pressure to digitize operations, while being forced to rely on legacy systems. Threats tend to be noticed with substantial delays. Healthcare also uses a lot of very interconnected systems. By comparing different industries, it is possible to highlight the unique aspects of each one. This information can be useful for modifying and implementing best practices that have been learned elsewhere.

Webb and Dayal (2017) argue that the responsibility to manage healthcare cyber risks is shared amongst various stakeholders. This view has expressed by the US Food and Drug Administration (FDA) and the Australian Therapeutic Goods Administration (TGA). Mitigating these risks is important for all stakeholders involved, including patients, providers, and manufacturers. Successful cyber risk management will have to involve all of these stakeholders, each working in their respective capacities in a collaboration of sorts. Medical device manufacturers should use a lifecycle approach to risk assessment for their products. Security considerations and risk assessments should be kept up to date. These principles apply to healthcare providers as well. While manufacturers and service providers have the largest obligation in risk management, end-users should also play a role. This includes installing updates as they are released. The government also has its share of responsibilities, such as appropriate guidance and regulation.

One aspect of cyber risk management is preparation for worst-case scenarios, so that an organization is able to function offline if a significant cyber event were to occur. Some have taken steps to reduce their dependence on online operations. Some healthcare providers in Germany and the US have taken this course of action, where certain critical systems are taken offline if connectedness is not required. Pen and paper methods of past years are also maintained in order to ensure that the organization is able to function even if digital operations are not available. (Herbolzheimer 2016, 13)

Technology companies like IBM have also developed tools to manage cyber risks, which have been used in the healthcare industry. The cognitive computing platform Watson has been used to evaluate security threats and analyze natural language reports on topics like software vulnerability. This beta phase product has been used in the University of Rochester Medical Center. Watson can use a many types of information, including FDA and medical device manufacturer reports, research papers, and online writing, in order to offer insight on cyber security. Predictive analytics applications have also been developed for the healthcare sector. Cognitive computing products are still being developed, but it is hoped that they will help to parse through the vast amounts of data that security specialists encounter, and help them make more informed decisions. These new applications can be prohibitively expensive, which may hinder their installation. (Rubenfire 2017)

Industries that store and rely on large volumes of personal data, such as healthcare, have been considered as the most likely candidates to purchase cyber risk insurance (Allianz 2015, 25) A Ponemon Institute survey (2013, 13) found that 29 % of respondents in the healthcare and pharmaceutical industry had procured a cyber insurance policy. They represented the industry with the second lowest rates of cyber insurance. For comparison, the highest rates were in technology and software (41 %) and lowest in the public sector (19 %). Even though healthcare organizations were less likely to have purchased a cyber insurance policy, they were among the most satisfied with the product.

The rates of cyber insurance suggested by the Ponemon Institute (2013) are very different from the findings of Willis (2013, 9). This study found that 1 % of healthcare organizations reported purchasing cyber insurance. They do, however, comment that this finding is surprising given their experience of healthcare as one of the largest buyers of these insurance policies. The authors suggest that this low number may be due to under-reporting. The insurance industry has developed an array of products and services specifically for healthcare organizations.

4 Cyber Risks in Finnish Healthcare and the Pirkanmaa Hospital District

The first empirical section of this thesis will describe the data collection and analysis process. The interviewees are presented next, followed by brief descriptions of the organizations they represent. The next section contains a discussion on the Finnish healthcare system and Pirkanmaa Hospital District. The chapter then concludes with data analysis.

4.1 Data Collection

The data for this thesis includes five semi-structured interviews and a series of publically available and private publications from the Pirkanmaa Hospital District concerning risk management and cyber risks. These publications include annual reports, the risk management policy, the information security policy, and internal risk management reports. The interviewees were selected for this thesis with the aim of answering the research questions.

The interviewees in this thesis included four representatives from the Pirkanmaa Hospital District. The Chief Security Officer, Anna Tamminen and Information Management Director Antti Jokela were interviewed together on 24.3.2017. Data Privacy Officer Jaana Riikonen was interviewed on 2.5.2017. Information Security Manager Markus Markkinen's interview took place on 10.5.2017. These three interviews took place at the Tampere University Hospital. The Chief Commercial Officer of Granite, Janne Viljamaa was interviewed on 26.4.2017 at the Granite office in Tampere. Marko Ruotsala is the Business Manager of Istekki, and his interview took place on 17.5.2017 at the Tampere Torni Hotel. PHD, Granite, and Istekki will be presented more fully in the next section. Ruotsala and Viljamaa gave their interviews on a general level; their interviews and statements do not apply to any specific organizations.

All the interviews were conducted in Finnish, and recorded with the permission of the interviewees. Semi-structured interviews were prepared in advance, and these were slightly adjusted for each interview. The questions have been roughly categorized into five groups, which are echoed in the results chapter of this thesis. The interview questions are presented in Appendix 1. They have been translated from Finnish to English. The interview questions were not presented in order, and each interview took a different course as the interviewees brought up new themes and viewpoints during the dialogue. The interviews were transcribed carefully, after which they were analyzed. The interviews have not been translated into English, with the exception of excerpts used as direct quotes.

The different parts of the data have been analyzed together, in accordance to four themes. These themes are 1. Cyber risks in healthcare and the Pirkanmaa Hospital District 2. Managing cyber risks in healthcare and the Pirkanmaa Hospital District 3. Unique aspects of cyber risk management in healthcare 4. Future developments. The interviews and publications have been analyzed from these four perspectives in order to gain a deeper understanding and answer the research questions. Three of the interviews are from PHD representatives, and the data from these interviews is used to give a more detailed image of cyber risks and risk management within this organization. The other interviews provide a general view of the thesis subject. These two parts have not been separated in the data analysis portion into distinct sections. Rather, the data analysis aims to produce on overview of a subject, and then bring it to sharper focus with the examples provided by the PHD material. The result is more descriptive than having these two portions in isolation.

The original timeframe for the healthcare reform was to have the new system implementing by the beginning of 2019. In July 2017, this original plan was postponed to January of 2020. The interviews for this thesis had taken place before the announcement of the postponed timeframe.

4.2 The Finnish Healthcare System

The state has a responsibility to promote the health of the population, and to arrange social and health services. This responsibility is based on the Constitution of Finland (731/1999), and has been largely transferred to local government, the 311 municipalities. The Social Welfare Act (1301/2014) and other laws stipulate and define what services the municipalities are obligated to produce. (STM 2017) Municipalities are responsible for the arrangement and funding of healthcare services, which are organized into primary and specialized medical care (STM 2017a). Municipalities have several options as to how they provide their population with health services. They can produce the services on their own, or purchase them from another organization, such as other municipalities or private corporations. Municipalities can also provide services together. (STM 2017b)

Primary healthcare is mainly provided in approximately 160 health centers. Health centers provide a substantial array of services, including inpatient, outpatient, and home care services. Some of the key services are health counseling, vaccinations, maternity health, and general practitioner consultations. (STM 2017c) Specialized healthcare is provided by hospitals, and it consists of treatment or examinations by medical specialists. The objectives of healthcare organization include smooth care chains and enhanced cooperation between different sectors. (STM 2017d)

Every municipality must belong to a hospital district, of which there are 21. Hospital districts are responsible for organizing specialized healthcare and coordinating with primary healthcare. Hospital districts must also take care of certain primary healthcare services, which are not appropriate to organize at a municipal level. Examples of these include medical imaging and clinical laboratories. Hospital districts are further organized into five special responsibility areas. (STM 2017e)

In 2014, public financing made up 75.6% of healthcare expenditures, and the remaining 24.4% was funded privately (THL 2017). Approximately 9% of healthcare costs are paid with client fees (STM 2017f). The total expenditures were about 19.5 billion euros, which means 3,576 euros per capita. Healthcare spending made up 9.5% of the 2014 GDP. A breakdown of healthcare expenditures is shown in Figure 2. Specialized and primary healthcare are the two most expensive components of the healthcare system, and together they represent just over half of the total expenditures.

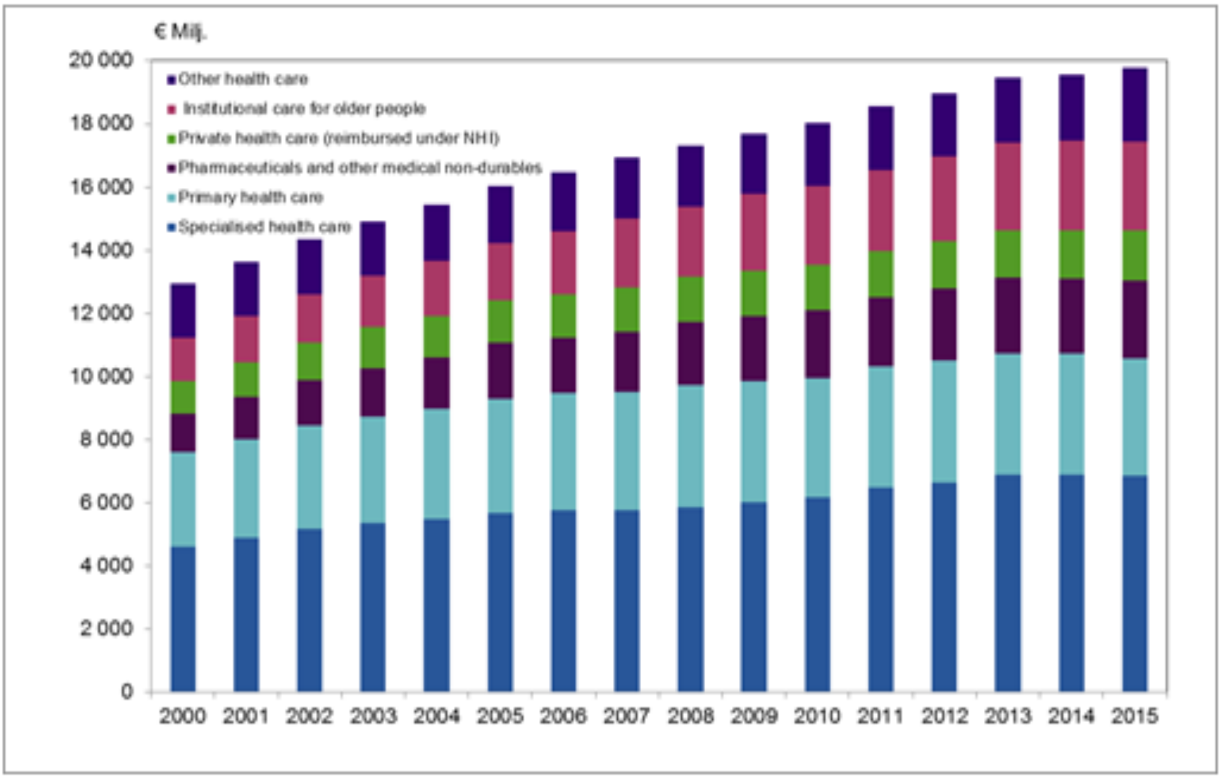

Figure 2: Healthcare expenditures (THL 2017)

While the public sector plays a very large role within the Finnish healthcare system, occupational health and private healthcare are important as well. Occupational health is a joint effort of employers, healthcare professionals, and employees. Employers have an obligation to offer preventative occupational healthcare services to their employees, and the Finnish Social Insurance Institute participates in the financing of these services. (STM 2017g) Private healthcare is considered supplementary, and they produce about 25% of healthcare services. This portion has continued to grow over the last 15 years. It has been projected that the demand for private healthcare will continue to expand due to an aging population and their growing healthcare needs. Private healthcare providers are particularly prevalent in the urban hubs in Southern Finland. (STM 2018h)

4.2.1 Health and Social Services Reform

Any contemporary discussion of the Finnish healthcare system would be starkly incomplete without a mention of the ongoing health and social services reform. For the sake of brevity, this will be referred to as the healthcare reform. This reform is one of the largest administrative overhauls in the history of Finland, and will change how health and social services are organized, produced and financed. A key element of the reform is the reorganization of public administration into a three leveled model: municipalities, county, and state. Counties, as larger autonomous regions, will have the responsibility of organizing and funding social and healthcare services. (Alueuudistus 2017)

Healthcare financing will also be simplified from the current multisource financing system. In addition, the healthcare reform will strengthen a patient’s right to choose their care provider. The objectives of this reform can be considered somewhat ambitious, considering that the post-reform services should be up and running by the start of 2020. Some of these include better, more customer-oriented services, health inequity reduction, and reducing the sustainability gap by 3 billion euros. (Alueuudistus 2017)

The health and social services reform will also have a significant impact on health information systems. One aspect of the reform is bringing a large number of municipalities and their healthcare and social service provider together into one entity. Most, if not all, of these smaller organizations have utilized a variety of information systems to keep track of electronic health records and manage operations. The Valvira (The National Supervisory Authority for Welfare and Health) register of electronic health record information systems currently has 102 items (Valvira 2017)

A part of the reform includes the construction of new information systems for these organizations, which must be compatible with existing systems in order to ensure data security. The new information system has to be compatible with many different kinds of healthcare providers, which will have a variety of requirements for an information system. The objective or definition of compatibility is not to have every service provider using the same information system, but to standardize the data flowing within these systems so that it may be used at any healthcare service provider. In the current model, the data within an electronic health record is bound to that record, and so it is can't be used elsewhere. According the new line of thinking, health records will be stored in a manner where different healthcare providers will be able to utilize them in a manner that suits their needs. (Korhonen 2016)

4.2.2 Pirkanmaa Hospital District

The Pirkanmaa Hospital District (PHD) is a joint municipality authority that is owned by its 23 member municipalities. Over half a million residents live in the areas within the PHD, which produces specialized healthcare and disabled care services. On an annual level, about 190,000 different patients use the services provided by the PHD. The district employs nearly 7,000 workers. Healthcare services are provided by the Tampere University Hospital (Tays), which includes several hospitals and other units. The hospital district also owns several limited liability companies, where services are also produced. These include the Tays Heart Hospital for the treatment of cardiac patients, and the Hospital for Joint Replacement Coxa. The most common diagnosis in 2015 was childbirth (4039), and the most common procedure was cataract surgery (3792). (PSHP 2017 & 2017f)

The organizational structure of PHD is shown in Figure 3. The highest level of authority resides in the Council, which is made up of 67 members chosen by the municipalities and Tays. (PSHP 2017a) The Council chooses a 13-member Executive Board, which represents the joint municipality authority. The Executive Board is responsible for executing the decisions made by the Council. (PSHP 2017b) PHD also has a number of other representative bodies and boards. One of these hospital support service bodies is information management and technology, which are responsible for overseeing and ensuring information security and privacy. (PSHP 2017c)

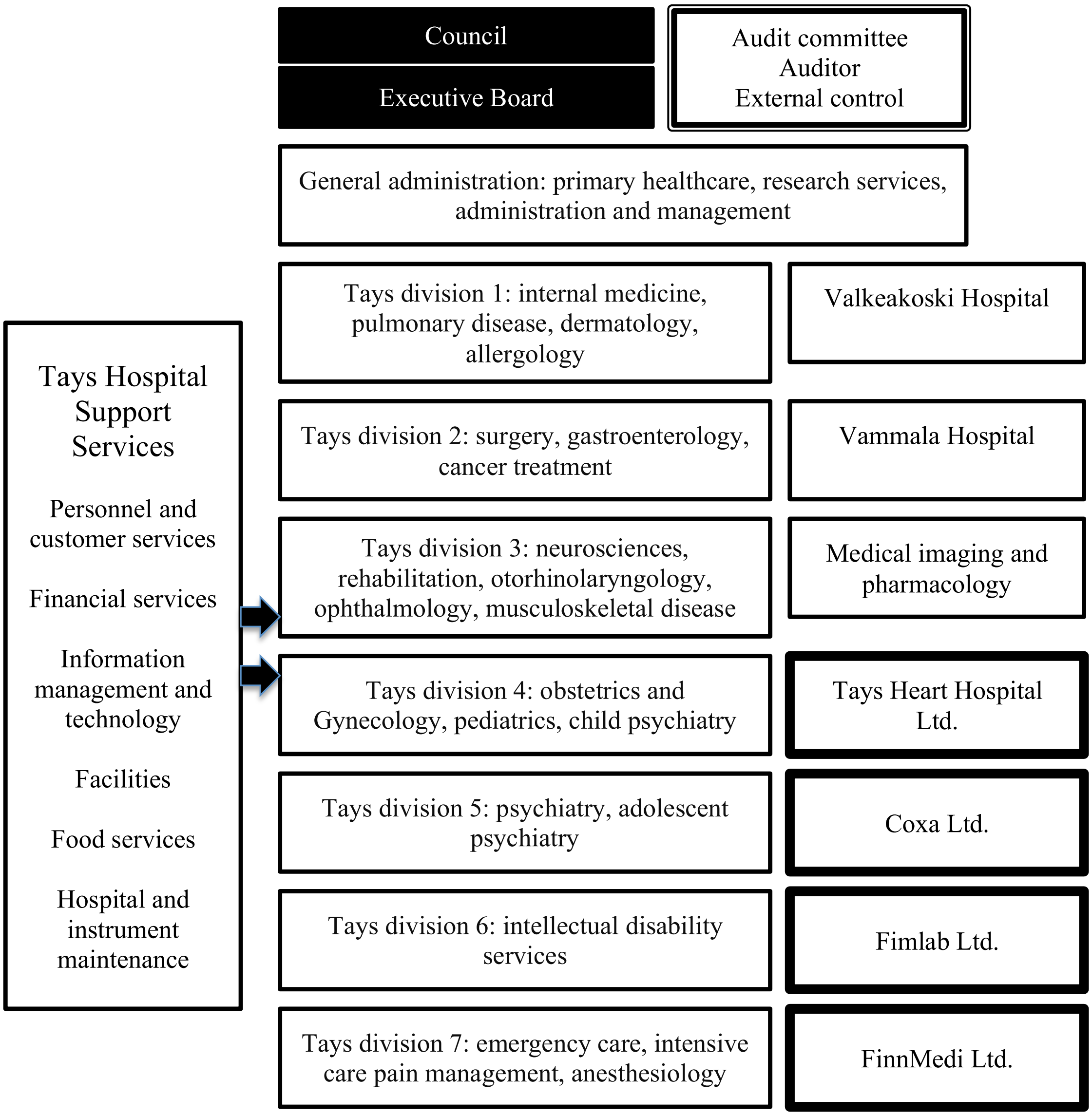
Council
Executive Board
Audit committee
Auditor
External control
General administration: primary healthcare, research services, administration and management
Tays Hospital Support Services
Personnel and customer services
Financial services
Information management and technology
Facilities
Food services
Hospital and instrument maintenance
Tays division 1: internal medicine, pulmonary disease, dermatology, allergology
Tays division 2: surgery, gastroenterology, cancer treatment
Tays division 3: neurosciences, rehabilitation, otorhinolaryngology, ophthalmology, musculoskeletal disease
Tays division 4: obstetrics and Gynecology, pediatrics, child psychiatry
Tays division 5: psychiatry, adolescent psychiatry
Tays division 6: intellectual disability services
Tays division 7: emergency care, intensive care pain management, anesthesiology
Valkeakoski Hospital
Vammala Hospital
Medical imaging and pharmacology
Tays Heart Hospital Ltd.
Coxa Ltd.
Fimlab Ltd.
FinnMedi Ltd.

Figure 3: Pirkanmaa Hospital District organizational chart (PSHP 2015)

Operations and budgets are based on strategic outlines, and they are planned for the following three years and the upcoming year. Service contracts with the municipalities are a key element of budgeting. Budgetary and operational goals are defined using several indicators, and the success of meeting these goals is measured annually. (PSHP 2017d) The district's operating income for 2016 was 815,5 million euros, the majority of which consists of service sales to member municipalities. A breakdown of the sources of income is presented in figure 4. Operating expenses in 2016 were 755,2 million euros, with personnel costs representing the largest portion of expenses, as shown in figure 5. The PHD profited 6,6 million euros in 2016. (PSHP 2017e)

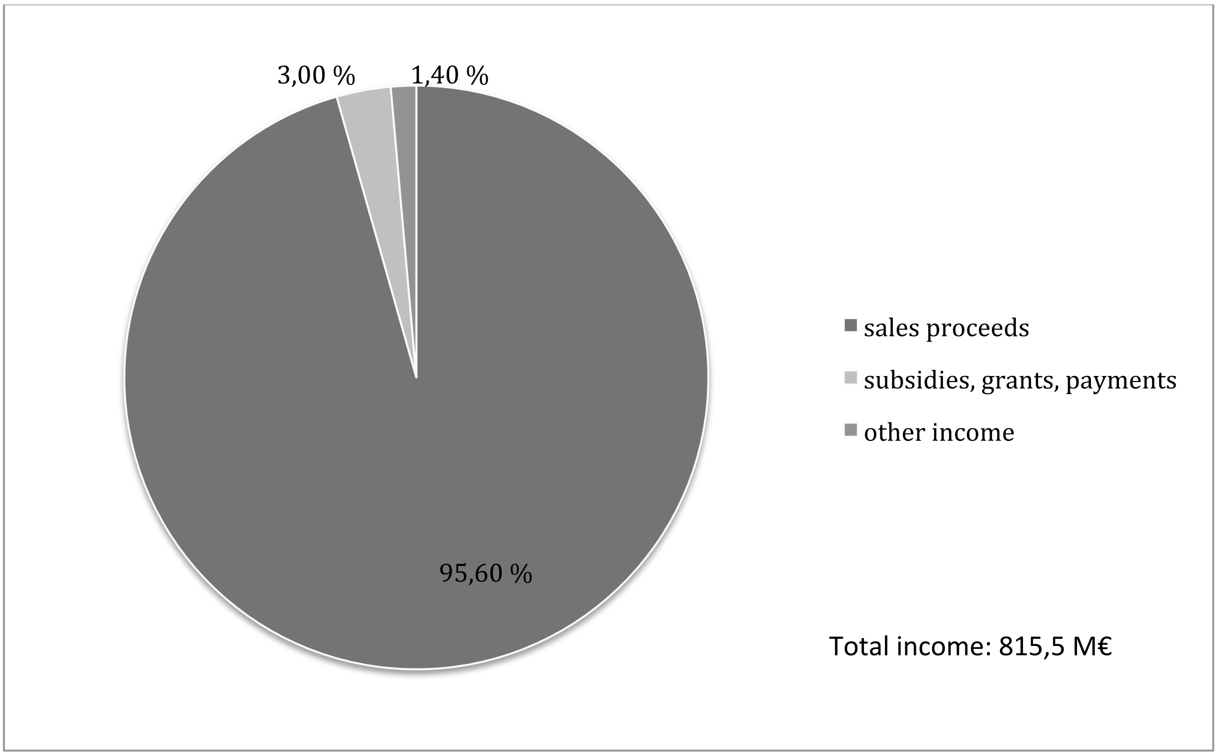

Figure 4: Pirkanmaa Hospital District operating income distribution 2016 (PSHP 2017e)

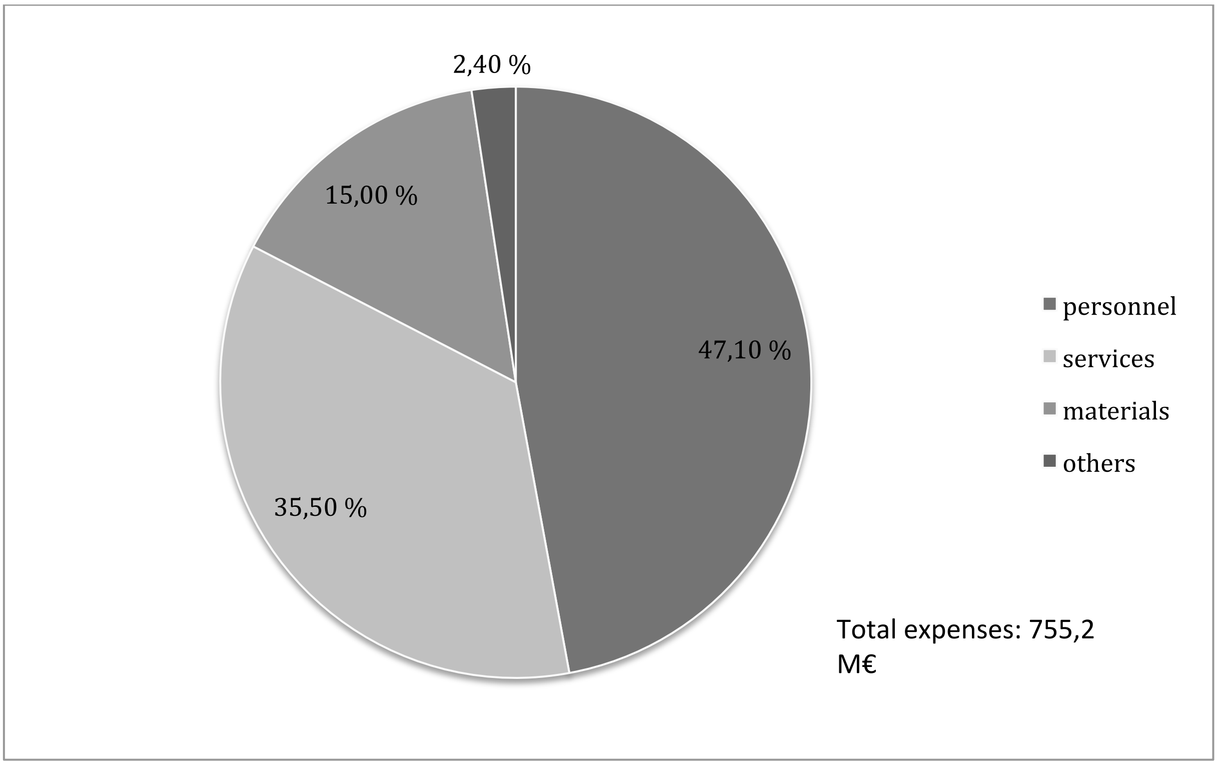

Figure 5: Pirkanmaa Hospital District operating expense distribution 2016 (PSHP 2017e)

4.3 Granite

Granite is a risk management and information security software company that was founded in Tampere, Finland in 2005. The initial objective of the founders was to create a product that would help put information security into an understandable form for all personnel of an organization. Since its establishment, Granite has grown and systematically expanded. The clients of Granite are public and private sector organizations from a variety of industries, such as healthcare, finance, and chemicals. Several Finnish hospital districts from different parts of the country, including the Pirkanmaa Hospital District, are clients of Granite. (Granite 2017 & 2017a)

The Granite tool is a browser-based risk management software program, which consists of individual modules. The Granite tool can be used to develop risk management, work safety, and information security. It includes functions for the identification of risks, corrective actions, compliance maintenance, and personnel awareness. The tool is made up of different modules that are either ready-made or customized for specific client needs. (Granite 2017b)

The enterprise risk management module can be used to document risks and their control measures. Automatic reporting can be used to create risk maps and analyze trends and changes across different parts of an organization. (Granite 2017c) Granite also offers online information security training. The contents of the training can be customized according to client needs and compliance standards, and focuses on employee actions rather than technical matters. (Granite 2017d)

Granite representatives were asked to participate in an interview for this thesis because of the unique insight the company has to offer. Granite has had many years of experience in risk management and information security, both of which are important themes in this thesis. Their customer base also factored into the selection of Granite for an interview, as they have had experience with the risk management needs of many kinds of organizations. This thesis focuses on the Finnish healthcare sector, one that is well represented within the Granite customer base. The wide range of customers, however, means that Granite has a special perspective on the risk management and information security of the healthcare sector. As the Granite tool and information security training are modified according to customer needs and regulation requirements, sector and organization-specific matters or the lack thereof become apparent.

4.4 Istekki

Istekki is a publically owned company that is headquartered in Kuopio, Finland. Its owners include municipalities, hospital districts, and strategic partners from different parts of Finland. They are a non-profit organization that provides its owners with a variety of technology, information, and security related services. Istekki was founded in 2009, and since then has grown and developed into an organization that currently employs over 400 people. Istekki has seven Finnish hospital districts as clients, including the Pirkanmaa hospital district. (Istekki 2017 & 2017a; Kauppalehti 2017)

Istekki provides consulting and other types of services to its clients. These include infrastructure solutions and end-user services and equipment. Istekki also provides security services, which are based on a risk evaluation done in cooperation with the client. Their expertise on security related matters is also utilized to develop the client’s strategic and operative functions. Some of the services that Istekki provides have been specifically designed to meet the needs of healthcare providers and hospital districts. These include electronic health record system maintenance and support services. Istekki is also specialized in medical technology, and the integration of medical devices and electronic health records. (Istekki 2017b)

Istekki was approached to participate in an interview for this thesis because of their expertise on the information security and privacy aspects of the Finnish healthcare system. Information security and privacy are key concerns within cyber risks in the healthcare sector, so the expertise of Istekki in these matters could be valuable for this thesis. Istekki is also involved with risk management and other security considerations of healthcare providers. Istekki's specialized experience in medical technology and information systems is also unique, and relevant to the objectives of this thesis. As their client base is not limited to organizations within the healthcare sector, they may also be privy to the particular needs of healthcare organizations.

4.5 Cyber Risks in Healthcare and the Pirkanmaa Hospital District

Cyber risks in healthcare at the PHD are considered as information security and privacy related risks. Cyber risks are not in the forefront of risk management in their own right, but rather they are viewed as an important aspect of security in general. (Jokela 2017; Tamminen 2017) The PHD has categorized risks into strategic, financial, operational, and hazard risks (PSHP 2015b). Cyber risks are classified under operative risks, but Tamminen (2017) adds that they also play a role in strategic, financial and hazard risks as well.

An important aspect of risk is the effect that it may have, and failure of information security and privacy are significant effects of cyber risks within the organization. Cyber risks and the word cyber itself are very broad and vague topics, and these terms do not reveal what sort of effects they can have. Because of this, the PHD has taken the approach of "dividing it under information security and information privacy." (Tamminen 2017) According to Viljamaa (2017), cyber risks are understood in many different ways, and organizations can have their own way of defining them.

Information security and privacy have been defined in the PHD information security policy. “The objective of information security is to secure information, information systems, and information transmission confidentiality, integrity, availability, usability, and irrefutability.” “Information privacy is a subsection of information security, which means preventing unauthorized access to information, the confidential storage of information, and the protection of personal information from unauthorized or harmful use.” (PSHP 2016a)

Information privacy is a part of information security, but because of the nature of health information, the significance of information privacy is emphasized (Markkinen 2017). Information security and privacy are generally accepted as important values in a healthcare setting, but they can also be seen as a tradeoff between other objectives that are also important to healthcare (Jokela 2017). An important aspect of information privacy is the extent of access to medical information that personnel are granted (Riikonen 2017). Individuals will have different priorities regarding access to information, “some people think that nobody better be able to see this, and for some it’s important that it’s fast, and it doesn’t really matter if there is a bit extra there.” (Jokela 2017) This is related to two objectives, that can be opposed at times, “you need to make sure that nobody can see anything that they are not supposed to see, but then everything that you need, you have to get…”(Jokela 2017). “And quickly, and easily” adds Tamminen (2017).

The significance of cyber risks has grown in recent years at the PHD and in the healthcare sector overall. Cyber risks in healthcare have become much more diverse, as the surface area for these types of events has grown substantially. There are many devices, and wireless networks are becoming increasingly common, creating more opportunities for risks to occur than in the past years. (Markkinen 2017) Devices can be accessed remotely, and cases of medical device hacking have taken place, causing various problems. Digitalization is happening in the healthcare sector, so it is likely that different types of cyber risks will become more of an everyday occurrence as well. (Riikonen 2017) Ruotsala (2017) also believes that people and decision makers are becoming more interested and aware of cyber risks within healthcare. This awareness he attributes partially to cyber events that have taken place, such as the recent WannaCry attack. An unfortunate trend is that “it looks like something has to happen before we learn.” (Ruotsala 2017)

The PHD compiles an annual list of the most significant risks as a part of their risk management process. Seven risks were included in the 2017 list, one of which is the endangerment of patient safety or information security due to information system or data transmission disturbances. (PHSP 2016) This risk is broad, and the PHD does not keep an official list of most significant cyber risks. They do however prepare for specific risks, such as denial of service attacks. (Jokela 2016) The year 2016 most significant risks also included an information system related risk, but it concerned inefficient care caused by poor usability and problems with information systems (PSHP 2017e, 36). The most significant risks are determined with the perspective of the whole organization, but each division of the district must also consider their most significant risks as well. Information security and privacy related risks have been raised every year by the divisions during this process. (Tamminen 2017)

> *"When the divisions are asked what are their most significant risks, every year it is either through usability issues or making working more difficult due to system problems. ... Or risks from sudden problems, it can be caused by something internal or external. But if the information system is not accessible, patient safety is endangered most certainly."* (Tamminen 2017)

Being connected to networks is not optional in the modern world, and it is not possible to sever these connections (Jokela 2017). Public sector organizations are under increasing pressure to have more of an online presence as well. This has meant opportunities, but risks as well. (Tamminen 2017) The PHD has also had its share of cyber events of various kinds in the last years. These include things like spam and computer viruses, which are considered as constant, everyday occurrences. Several years ago they were subjected to a denial of service attack, which had clearly been targeted at the PHD. The motive for this attack, and the location of the attackers is not known for certain. One of the PHD service providers was also a target of a denial of service attack more recently, which impacted the functions of the PHD. (Jokela 2017) One cyber event involved an employee misfortunately clicking on something. The individual noticed their mistake, but some damage had already been done (Tamminen 2017).

Malfunctions of the PHD health information system are detailed in the annual report. The more serious ones in 2016 included a telecommunication network failure, which caused wide problems in the information system for the duration of five hours throughout the PHD.

Alterations at a data center also caused data transmission problems, resulting in a severe restriction of service for the duration of three and a half hours. The PHD voice network also experienced four short periods of malfunction. Problems have also occurred in individual applications. (PSHP 2017g, 37)

Information leaks due to things like malware are a big risk in healthcare. In addition to the problems associated with the leak itself, it can also take a long time to become aware of the situation. Healthcare organizations like the PHD are not only responsible for patient information. They must also secure information pertaining to personnel, suppliers, and other stakeholders. (Riikonen 2017) One particular concern is about outsiders trying to access medical information.

> *"Because it is more likely to be happening on a larger scale, and usually the point is to somehow ... turn into money. ... It is not necessarily about peeking into some person's information ... but it is much broader, to make money in one way or another."* (Riikonen 2017)

Jokela (2017) also believes that the prime motive behind cyber attacks is financial. For the people that are putting in the most effort into these types of criminal enterprises, it most likely driven by financial gain. The potential profits in attacking a Finnish hospital district, however, might not make it the ideal target because there are more lucrative ones out there. Governments have also participated in these types of activities, but Jokela (2017) does not believe that they would be particularly interested in public sector hospitals in Pirkanmaa, Finland either. These are, however, global phenomena so they will be seen in Finland as well. Markkinen (2017) is surprised that there haven't been more attempts to unlawfully obtain medical information for extortion.

Ruotsala (2017) believes that there are several noteworthy cyber risks in healthcare. Cyber events that can damage the integrity of medical information can be particularly dangerous for patient safety. Another risk deals with the legacy systems that are so common in the industry.

> *"For example an imaging device that was acquired 20 years ago ... with Windows 95 ...is problematic, ...because you can't really update it or change it. It is a medical device that has been delivered to you as it is, and if you change it*

> *... the supplier is no longer ... responsible for it. The one making the changes is."* (Ruotsala 2017)

The use of mobile devices is becoming increasingly common in a healthcare setting, and Markkinen (2017) points out that they have some particular information security challenges. These new mobile solutions are designed to be very easy to log on to and provide fast access to health records, but still remain secure. The proliferation of "IoT (internet of things) and everything else is an information security risk, a significant one, … as their protection tends to be weaker than at workstations." Cyber risks form a broader group when you take indirect effects into account. "For example, if some hacker gets into the Tampere power plant, it could affect us … it is a risk even though not directly involving our data transmission, but indirectly." (Markkinen 2017)

Viljamaa (2017) believes that the healthcare sector may have some advantages regarding cyber risks, because they are required to take more steps to mitigate them. Because of these demands, "… things are done, and it's a lot. In many private sector companies things are not taken care of because there is no requirement that they do so." (Viljamaa 2017) Matters relating to cyber risk management in healthcare, such as information security and privacy are subject to a large body of regulation. Some points found in the body of regulation can also be contradictory, or at least subject to various interpretations. Certain areas of health information, such as psychiatric health and genetic diseases may also be held to higher standards of information privacy. This is a difficult area to legislate and to write appropriate laws for.

> *"With cyber threats, ... if laws tell you what to do, then everybody knows what everybody else has done. ... There also has to be leeway for alternative solutions, because this changes constantly. If it is very specific and you make it now, publish it tomorrow, it can be obsolete the day after."* (Jokela 2017)

4.6 Managing Cyber Risks in Healthcare and the Pirkanmaa Hospital District

The starting point of risk management at the PHD is the risk management policy, which was updated in 2015. This document outlines the principles and objectives of risk management, in addition to describing the risk management process. (PSHP 2015b) The policy is presented at a general level for the various types of operations taking place at the PHD, so it is not a detailed guide. The risk management policy is for the whole hospital district (Tamminen 2017). It serves as a guide for considering risk and risk management in all types of functions, "… and then it is applied to your own area." (Riikonen 2017)

According to Viljamaa, (2017) risk management in healthcare usually follows the same principles and frameworks that are used in other industries. The processes and frameworks usually do not differ in any meaningful way, but they may have some industry-specific component such as patient safety included in them. Risk management often uses generally accepted best practices that may be slightly accommodated.

> *"The changes can be very small, things that are appropriate for that specific client. What they may want relating to processes, for example, ... how the risk management process works, and the ... information system is adjusted according to their operations."* (Viljamaa 2017)

Risk management should not be a "glued on process, or it may be viewed as a necessary evil, without much benefit." Risk identification and evaluation must be done with care, and with enough professional expertise. For most organizations this part of the risk management process is not the challenge, but rather the ability to ensure that the right techniques have been utilized and that they are effective enough. (Viljamaa 2017) Personnel should also be involved in risk management if they are so inclined, because

> *"... they can offer ... solutions for controlling risks that experts ... may not come up with. This can be cost efficient, as a person who is very familiar with some particular process ... may be able to suggest a risk management technique ... which may not even be expensive, just by making some slight adjustment to the process."* (Viljamaa 2017)

Risks are evaluated by guidelines provided in the risk management policy. This evaluation includes the determination of probability and outcome. Probability is rated 1-4, with one meaning events that are extremely rare but theoretically possible. A probability of four is given to events that are common and may happen repeatedly. The guideline used for evaluating outcome is presented in table 3. Outcome is determined using several parameters and effects. (PHSP 2015b)

TABLE 3: Risk outcome evaluation (PSHP 2015b)

		1 Slight	2 Moderate	3 Significant	4 Major
Customer	Effect on reliability/ reputation	Basic communications suffice/ stakeholders making unofficial inquiries	Communication and other procedures required/ stakeholder inquiries	Publicity or public opinion restricts key employee work/ significant procedures required	Loss of clients/ changes in personnel or operating models required
Process	Effect on patient safety	Mild harm to patient	Moderate harm to patient	Permanent and significant harm to patient	Patient death
	Providing services endangered	Non-urgent care disrupted	Urgent care disrupted	Serious disruption in critical functions	Emergency care disrupted
Personnel	Effect on professional abilities	Slight shortage of ability	Shortage of ability in different areas	Constant insufficient abilities	Permanent loss of critical abilities
	Effect on working ability	Temporary harm	Sick leave extending	Many long leaves of absence	Permanent disability/ death
Financial	Group level effect	0,5-1 MEUR	1-7 MEUR	7-14 MEUR	Over 14 MEUR

The occurrence of cyber events can have a negative impact on the various dimensions outlined in table 3. Riikonen (2017) believes that information privacy failure can have critical effects by damaging their reputation and causing a loss of trust. A damaged reputation can have an impact on the relationship with customers and other stakeholders as well. This will become more significant in the future, as the healthcare reform will grant patients a greater right to choose their healthcare provider.

Ruotsala (2017) pointed out that evaluating the actual numerical value of medical information is extremely difficult. It is much easier to calculate the value of other effects of cyber events. For example,

> *"A CryptoLocker attack happens and production stops. What does it mean in euros if the staff is twirling their thumbs because they can't take care of patients. Patients have to be moved elsewhere, schedules and procedures reorganized. You can calculate all this, but determining the value of the lost information is the hardest."* (Ruotsala 2017)

Managing cyber risk is usually "baked into the risk management framework, so that cyber risks are a component". (Viljamaa 2017) Efforts have been made at the PHD to bring a stronger risk management perspective into information privacy. This undertaking is related to the GDPR, and it involves a survey of the most critical systems and the risks that are potentially involved. These risks are analyzed regarding their probability and outcome. Potential risk management techniques and documentation are also considered. The information security policy was updated in 2016; implementation of the new policy and training of personnel took place the following year. (Riikonen 2017) Risk management relating to information security has also been brought to focus in the last couple of years. The objective has been to have a systematic way of managing risk, increase preparation, and to have plans in place. Risk management is a unified process involving the whole hospital district, but "we contribute to it … with input on information security risks." (Markkinen 2017)

Cyber risk management techniques typically involve a mix of technical solutions and personnel training. Things like firewalls and SIEM software are an important part of managing cyber risks. (Markkinen 2017) These various technical solutions are constantly improved upon, so that they operate as well as possible, and that as many functions can be kept out of bounds in the case of a cyber event. Documentation of near misses also improves these techniques. Everything, including workstations, servers, and software has to be kept up to date at all times. There is also an extensive amount of testing that has to be done. The health information system of on organization like the PHD has a wider range of applications, and changes can lead to disturbances in their functioning. One part can be updated, and cause a problem in some other application. Software providers test their products, but everything is further tested in-house if it is at all possible. (Jokela 2017)

While technical solutions are able to prevent a lot of things from happening, the actions of personnel are critical as well. As Riikonen (2017) puts it, “80 % is how the employees work, how they use their usernames, how the handle the health records ”. The right kind of training is instrumental, as it has to given in a form so that it is processed and understood properly; merely showing up is not enough. The information privacy training of healthcare personnel begins when they are still in school, where it is given more attention than other security considerations (Tamminen 2017). Information security training should start at employee orientation; the information has to be internalized and be reflected in their actions. (Markkinen 2017)

> *“It is not enough that somebody signs their name onto an agreement. We want that person to understand how to work in an information secure manner, and to actually work in an information secure manner.”* (Markkinen 2017)

Cyber risk management and different parts of the process are continuously improved at the PHD. This involves the written policies, practical aspects, and the process itself. (Jokela 2017) They have also organized a larger drill, where the situation included a cyber event. The drill was used to test how the existing operational models functioned in a simulated cyber event. It is also important to learn from mistakes and oversights that have been made. There are tools available to report on various problems, and these reports can be useful as a learning device. Learning from incidents that have taken place elsewhere are also an important part of risk management development. “Fortunately it doesn’t always have to happen to us, but we can wake up when it happens elsewhere.” (Tamminen 2017) Cyber insurance has also been used to mitigate risk by Finnish healthcare organizations (Ruotsala 2017). “Nobody has managed to come with one super idea that would solve everything.” (Jokela 2017)

Cyber risk management is influenced by many factors. Financial considerations are important as well. Decisions that influence the PHD from a financial perspective are made by the district itself, and by politicians as well. There is a limited amount of euros to be spent, and these have to be allocated by priority. "Is it homecare for seniors, is it emergency care, picking up patients with a helicopter, or cyber security?" (Ruotsala 2017) Within the resources allocated to mitigating cyber risks, decisions still have to be made and prioritization will take place. It is not feasible to do everything, and financial considerations are a part of the equation. (Jokela 2017)

> *"You have to prioritize, risks are evaluated according to their probability and outcome. What can you afford to do, what is it possible to do, and what should you do? You can't close everything."* (Tamminen 2017)

Cyber risk management is also affected by certain contextual factors. These can be related to the organization itself, or to the operating environment in a broader sense. Being a public sector healthcare provider can influential in some aspects. This may include an obligation to file a report if an organization is a victim of a criminal act. Public sector organizations are also restricted from paying ransom or other criminal demands. (Ruotsala 2017) The significance of Finland and Finnish language also raises some interesting points. Viljamaa (2017) believes that the high level of education of the Finnish population is beneficial. "People are highly educated, and through that they gain an understanding of information security and cyber risks. … The awareness and level of doing might be better." (Viljamaa 2017)

Regulation surrounding information security and privacy is something that has been around in Finnish healthcare for some time now. Certain requirements brought along by the GDPR have already been mandated in Finland by national law. This will make achieving an acceptable standard relatively easier for Finnish healthcare providers, as compared to some other countries where they represent something totally new. (Riikonen 2017)

During the era of online translators, understanding something in Finnish can happen in a matter of instants. (Viljamaa 2017) Ruotsala (2017) has come across many examples of targeted malware written in very good Finnish, along with things clearly written with an online translator. Finnish isolation in terms of location and language does not serve as a means of protection.

Suppliers and regulatory authorities are also involved in cyber risk management. Various entities, such as ministries and other organizations regularly publish guidelines that are utilized at the PHD. (Jokela 2017) Patients are not seen as having a role or any responsibilities in cyber risk management, as it is up to the organization to ensure that it is taken care of (Riikonen 2017). Markkinen (2017) does not count on patients' awareness or participation in cyber risk management. But this could undergo a change at some point through new kinds of healthcare practices, such as telemedicine that takes place at the patient's home.

There are some challenges relating to cyber risk management, and these are not necessarily specific to the healthcare industry. From a technical perspective, medical devices and a hospital setting do not differ significantly from other types of industries. One challenge is the limited amount of information security and privacy related expertise that is available in Finland. (Ruotsala 2017) Another difficult area involves change management, and the many ongoing changes that will have an impact on the PHD. As with risk management in general, it should be a part of other operations and be considered in the planning phase and evolve according to the ongoing changes. (Tamminen 2017) There is also a culture of silence surrounding cyber events, and they are not openly and publically discussed (Markkinen 2017). Even though challenges exist, Markkinen (2017) is optimistic that risk management has provided some benefits:

> *"In some sense, you can tell that it has helped because not much has happened. Maybe it has helped us succeed in preventing something from occurring. But we don't actually know if we have succeeded. ... No such logging exists that you could know for sure."* (Markkinen 2017)

In Viljamaa's (2017) experience, the overall cyber risk management situation within Finnish healthcare organizations is good, particularly in the public sector. Ruotsala (2017) believes that the healthcare cyber risk management situation is improving, but there are still considerable differences between different organizations; in most cases, larger healthcare providers have taken risk management further. Markkinen (2017) has compared cyber risk management to a never- ending footrace of constant questioning and development:

> *"It is like being awake at all times, and preparing for things you could not have believed to be possible. ... It is like a footrace, they say that criminals and hackers are always a step ahead. ... You can't stop in your tracks for a moment and have faith that now we have enough mechanisms in place to prevent these threats from happening."* (Markkinen 2017)

4.7 Unique Aspects of Cyber Risk Managements in Healthcare

The fundamentals of cyber risk management are the same in healthcare as in other industries, but there are certain qualities about the sector that are a bit unique. One of these is the attitude regarding this matter in the first place. A common belief is that nobody could possibly be interested in stealing health information. This is a misconception, as there have been many documented cases of unauthorized procurement of electronic health records. A unique aspect of health information is that it can't be changed or made obsolete in the event of theft, as can be done rather easily with a credit card number, for example. Once health information gets leaked out, it can stay there forever. It can be used for nefarious purposes for a very long time, targeting either the patient or the organization where the information came from. (Ruotsala 2017)

> *"I still find myself having to explain to people. They laugh and wonder why someone would want to break into a hospital, what ... reason could they possibly have for doing that? Pretty often money is enough of a motive."* (Markkinen 2017)

Many healthcare organizations like the PHD must provide services around the clock. This sets a higher standard for the availability of information, as it must be ensured at all times. Everything must be accessible and correct, at every moment. Anything short of this can lead to significant and immediate consequences. (Ruotsala 2017) The nature of health information is also a unique factor. Health information can be very sensitive in nature, and is usually regarded as rather important. The consequences of a data breach can be serious, and can potentially lead to many kinds of misuse and fraud. The scale of the breaches can also be broad, as healthcare organizations can be very large entities with vast quantities of data on a substantial number of people. (Riikonen 2017)

A positive aspect of the healthcare sector regarding risk management is the transparency involved. The discussion about risks is more open than it is in many other types of organization. In some industries, information about risk management and the contents of the risks in particular is kept secret. Public knowledge of this type of information can be thought to reflect poorly on the organization. But healthcare organizations, especially in the public sector are more open about these matters. This is a more modern attitude, and can potentially be beneficial as well. This can also increase transparency from the employees' point of view, as they can gain a fuller sense of the operations they are a part of, and the risks they involve. (Viljamaa 2017)

4.8 Future Developments

According to Viljamaa, (2017) risk management in general is developing at a fast pace. There has been a certain eagerness to implement the principles of risk management, and it is becoming increasingly visible. The ongoing organizational and regulatory changes within the Finnish healthcare sector have lead to a higher awareness of risks and risk management. Another important driver of changes in the healthcare sector is the development of healthcare itself. Digitalization, the IoT, and other advancements in medical technology offer a lot of potential, but they entail risks as well. (Riikonen 2017)

> *"As every ... medical device goes online, ... there will be more holes and places to attack. ...Think about remotely monitored medical devices, of course there is the risk that they will be hijacked and be subject to interference. ... I think it's also worth considering if it makes sense to have everything on the internet."* (Riikonen 2017)

The healthcare reform will involve large organizational and structural changes for healthcare providers. Health information systems will be influenced as well. The municipalities and cities can have very different situations and operational models relating to risk management and information security. It will be challenging to merge a large number of organizations into one. (Riikonen 2017) The PHD has included the healthcare reform as one of their most significant risks (PSHP 2016).

> *”Changes are coming. Now, we don’t exactly know yet what that change will be, or what it will involve. ... When cyber threats can enter the picture, it is usually when there are data transmission problems or mistakes. Almost every time, it involves a change in something. Something has happened somewhere; someone has done something. ... With this reform, there will probably be a lot of changes happening, and we will need to pay really close attention.”*
> (Jokela 2017)

The healthcare reform will mean a new era of health information system management. The GDPR means that certain considerations will have to be made, and these have to be incorporated into this new health information system management. A substantial number of users will be accessing the new information systems after the healthcare reform. The county will have the responsibility to be able to demonstrate that each user has an appropriate level of access. Personnel must only be able to access what is needed, given their employment position. This is difficult from a management perspective, in addition to the accountability to demonstrate compliance. The reform means a lot of “changes that must be managed, so that they are done according the standards of the Regulation and other requirements.” (Riikonen 2017)

Tamminen (2017) believes that the healthcare reform is one of the most pressing issues in cyber risk management in the near future. The atmosphere of anticipating the healthcare reform was likened to the situation before the year 2000. “We didn’t really know what could happen, which ended up being mostly nothing. … But it could be something we could never even imagine.” (Tamminen 2017) The timeframe of the healthcare reform has also raised some concerns, as it is very fast from the ICT point of view. New health information systems must be designed and built in time for the reform. Many aspects of the healthcare reform are still up in the air, so there is no clear image of what the end result will look like. Planning, building, and implementing an information system for such a large, open-ended structure is a difficult and time-consuming task. (Jokela 2017)

> *"It will be difficult, as the architecture of the current system is built so that these large organizations use the systems internally. These same systems should now be available for ... smaller healthcare providers. ... How do we safely get these systems into their use, and can we ensure that their environment doesn't endanger the ... actual system?"* (Ruotsala 2017)

The GDPR will most likely not have an impact on the day-to-day functions and patient care at the PHD. The new Regulation will mean that information privacy training will be increased, so that the standards of the GDPR are understood and adhered to. (Riikonen 2017) There is an inspection underway to ascertain what the Regulation means for the PHD, and to uncover any potential problem areas and ensure compliance in time (Markkinen 2017). Regulatory cyber risk management will become more relevant via the GDPR, as the sanctions are so significant. This means that organizations will have to be prepared and ensure compliance. (Jokela 2017) The situation regarding GDPR compliance might be very different in other organizations and municipalities, a matter that might become quite relevant given the ongoing healthcare reform. (Riikonen 2017)

The GDPR will help to "set a price tag on" cyber risks. The hefty fines that can be imposed for non-compliance will draw more attention from senior management and decision makers. Recent events like the WannaCry attack will likely have the same effect, and highlight the importance of risk management in information security. Cyber events in healthcare will become more commonplace, and this will lead to changes in how these risks are managed. Information security considerations will have a bigger role in the design and acquisition of equipment and information systems.

> *"The outcome will be improved cyber and information security throughout the world; as a consequence of events. That is what I personally believe*."
> (Ruotsala 2017)

5 Conclusion

The final chapter of this thesis has three parts. The first part will present the research findings, and answer the research problems. This is followed by a brief discussion. The final section will address the limitations of this study, and suggest potential areas of interest for future research.

5.1 Results

The research problems of this thesis are:

1. What is the significance of cyber risks in healthcare and the Pirkanmaa Hospital District and how are they managed?

2. What is the significance of a healthcare setting on cyber risks and their management?

Cyber risks were found to be very significant for the PHD and the healthcare sector. Risk management has an important role within the PHD organization. This is evidenced by how the principles of risk management have been applied and utilized within the organization. Cyber risks are not considered as being in a vacuum, but they are viewed as a relevant component of risks that the organization must contend with. This is very much in line with the ideas of enterprise risk management. The PHD does not really consider cyber risks as a single, cohesive issue, but rather as information security and privacy risks. This demonstrates that cyber risks have been approached from what the organization considers the most relevant perspective. As was made very clear during the PHD interviews, the whole notion of cyber risks is very broad and vague, and as such, it is inherently useless. Reframing cyber risks as risks to information security and privacy shows that it has been refined to a more relevant and specific form.

Cyber risks are included as one of the most significant risks for the hospital district, and individual divisions have raised them as important risks as well. The PHD has taken on a broader perspective on cyber risks, while the divisions within the organization tend to focus on the poor usability of information systems. Cyber risks in one form or another have been included in the most significant risks for some time now, but the wording has changed. The focus used to be on poor usability and possible inefficiencies. Now it is the effect of information system disturbance and its effects on patient safety. These two aforementioned things are closely related, and in some sense differentiating between them might seem like splitting hairs. This does however reflect the changing attitudes regarding healthcare cyber risks in general.

The significance of information security and privacy risks has increased within the PHD in recent years. This is evidenced by the fact that more efforts have been made to manage these risks. These include assessments and surveys done at the PHD, the new policy that has been implemented, and the plans to further train personnel. The trends within healthcare, such as increased virtual healthcare services and medical devices have also raised a lot of thoughts within the interviewees, and they are considering the cyber risk perspectives of these phenomena.

Several interviewees commented how the importance of cyber attacks is increasing rapidly within the healthcare industry in general. This has been due to changes in the regulatory environment, particularly the GDPR, and cyber events that have taken place. Certain cyber events have had a lot of media coverage, and these have raised the general awareness levels among healthcare decision makers and the public as well. Research seems to suggest that healthcare cyber events are a growing trend due to the financial incentives involved. If so, it is likely that healthcare organizations will weigh in more heavily on this topic and take steps to manage cyber risks in the future.

The PHD uses a variety of risk management techniques, which involve the various technical and human elements described in the literature. The PHD seeks to include different sections of the organization into the risk management process, and to make it relevant within each part of the organization. Having drills involving a cyber attack can also make the idea of cyber risks more relevant to personnel, and to highlight their role in risk management. Some of the steps taken to manage cyber risks at the PHD are outlined in table 4. This table includes the same categories as presented in table 1.

TABLE 4: Cyber risk management at the PHD (Categories based on Biener et al. 2015; Cebula & Young 2010)

Category	Addressed	Management techniques mentioned
1: Actions of people	yes	Training starting from beginning of employment; appropriate level of access to information systems; technical solutions; updated policies and instructions; reminders of cyber security; drills; checking compliance
2: System & technology failure	yes	Technical solutions; regular updates; lifecycle planning of equipment; coordination with suppliers; reporting; following best practice and other guidelines; outsourcing; outside expertise
3: Failed internal processes	yes	Continual improvement; projects, analysis and surveys; training personnel; technical solutions; monitoring; reporting
4: External events	yes	Awareness of environment; compliance; observing regulatory changes; consider role of external parties; planned processes

While the interviewees did not give any specific information on how they manage information security and privacy risks, such as technical specifications, several important themes came up. The first of these is the continual improvement of the risk management process, which involves vigilance of the environment and reflecting current risk management practices against it. This includes things like software updates and increased training for personnel. Another important theme was the interaction of people with technology. Technical perspectives are important, but the interviewees also focused on the people working with that technology and how risk management must take this into account as well. A third theme to arise out of the data was change management, and the role change has for cyber risk management. These changes can involve the information systems, the regulatory environment, or the organization itself.

While the healthcare setting has some unique features, the industry itself was not found to be very meaningful for cyber risk management. The healthcare sector has traditionally not addressed cyber risks to the extent seen in some other industries. The financial sector, for example, has been a more conventional target for this kind of criminal activity. As cyber events become more commonplace within healthcare, managing these risks will become more important. The experience and lessons in managing cyber risks that have originated in other types of organizations can also be utilized within healthcare. Entities with an interest in managing cyber risks within healthcare have actively sought out expertise from other fields, and are applying it to healthcare.

Organizations will have different attitudes regarding risk, how risk is tolerated, and how risk is managed. Even if two different entities utilize an identical risk management process, the end results won't be the same, because the context and environment of a given organization will be reflected on how the process is carried out. For example, a risk management process will usually involve the determination of objectives. The risk management objectives of a hospital will be different from those of a power plant. The same can be said for the evaluation of risks, which will be influenced by the types of operations that are taking place, and how meaningful a given type of risk is in that particular context. There are many dimensions to information security, all of which can be considered as very necessary. But it may not be possible to make everything a number one priority. In healthcare, the accuracy of information is especially important. Organizations in different industries might have some other aspect of cyber security as paramount.

The fundamentals of cyber risks and their management appear to be the same across different sectors of industry. These have to be utilized in an organization specific way, rather than as they are. The operations and prevailing circumstances should be taken into account in managing risk. With healthcare, these can include the 24-7 nature of providing services and existing legacy systems. The circumstances in which many healthcare organizations function are not really unique to healthcare, as these can be readily seen in other sectors are well.

Rather than having an impact on the actual principles or processes surrounding risk management, the healthcare context was found to increase the need for risk management. Healthcare organizations must deal with cyber risks, as do most other organization as well. Three reasons were found in the data to support the idea that cyber risk management should have an important role in the healthcare sector.

First, the repercussions of cyber risk management failure can have significant consequences on patients and the organizations themselves. Cyber events can render a healthcare organization incapable of executing their primary task of providing healthcare services, or make this much more difficult. The effect of this on patients and society in general is obviously quite bad. Actualized cyber events can lead to a myriad of negative outcomes for the healthcare providers as well, these include financial repercussion and loss of reputation. Particularly in the day and age of increased patients' freedom to choose their healthcare provider, a hospital's reputation is very valuable.

Secondly, the regulatory standards that are applied to Finnish public healthcare providers are fairly stringent regarding information security and privacy. This includes national and EU laws. Guidelines and accepted best practices are published by various entities, and while they are not mandatory, compliance is highly recommended. The GDPR highlights this further and can mean large economic consequences. Managing these risks really cannot be considered optional.

The third reason is the changing landscape of cyber risks within healthcare, and the changing nature of healthcare itself. Cyber events appear to be becoming more common occurrences due to the financial incentives involved. Assuming that cyber attacks are directed at healthcare organizations because of a perverse interest in medical information is usually incorrect. The more likely situation is that a cyber event has been employed as a business strategy. Many healthcare providers have been around for some time, meaning that their equipment and information systems can be old. These legacy systems represent a challenge from an information security and privacy perspective. Several trends within healthcare, such as the increased use of remotely accessed medical devices, telemedicine, and mobile applications mean that the surface area for cyber risks is growing. More devices, more systems, and more connections mean more potential weaknesses. This, particularly in conjunction with higher motives to find these potential weak spots can become more problematic in the future.

5.2 Discussion

Cyber risk management in healthcare has not been studied extensively, but data from this thesis suggests that the sector is not the most important factor when it comes to cyber risk management. Rather than requiring industry specific methods for managing cyber risk, generic principles of risk management can be utilized effectively by the healthcare sector. The findings suggest that certain features that are common amongst healthcare organizations, such as legacy systems, should be taken into account in cyber risk management. It could be argued that certain features of an organization or its operational environment rather than the sector, are more relevant for cyber risks.

Dealing with legacy systems and quickly evolving technology is not limited to the healthcare sector. All types of organizations that are facing these challenges will have to contend with associated risks, but the exact nature of those risks and their significance will differ across various industries. Many types of critical infrastructure, such as power plants and the water supply also have components that can be classified as legacy systems that are relied upon around the clock. As with healthcare organizations, these systems must be able to function in their current environment, and failure to do so would cause significant damage. It is beyond the scope of this thesis to compare the importance of reliable power, water, and healthcare but needless to say, they are all important for modern society to function.

Cyber risk management is like aiming at a moving target. The most state of the art system today will become outdated at some point in the future. At this point in time, we do not have a way of knowing what sort of unforeseeable cyber risk considerations today's innovations will have tomorrow. Healthcare equipment and information systems are designed with many objectives in mind. A key feature of technological development in this field should be resilience, so that it may adapt to the only scenario we can accurately predict: constant change.

One of the challenges in healthcare cyber risk management includes the chronic budgetary constraint, which is not unique to healthcare. With healthcare needs projected to grow in the future, the financial considerations might become even more significant. Cyber risks in healthcare have also been projected to grow in the upcoming years. If these events do become more common, they will probably raise more discussion in the public domain. This discussion and attention might be influential on how cyber risks are managed in healthcare, and how they are viewed in society in general.

Cyber risk management within healthcare, or any other industry for that matter, is interesting because it involves certain qualities that can almost be considered as oppositional at first glance. These include the irrelevance of national borders and languages in the cyber world, while they are very influential for organizations and individuals that operate in it. Cyber events will probably have an origin somewhere, but that origin might be an inconsequential aspect of the event itself. Of course the origin of a cyber event can have implications, such as political ramifications, but this may not necessarily affect the event itself. Geography related considerations of cyber risks might be of secondary importance in their management. But organizations exist in a world where issues relating to national origin are very relevant, as they dictate some of the key operating parameters, such as regulation.

Another idea that seems to embody some sort of contrast is the human versus technology aspect of cyber risks. Dividing phenomena into their human and technology counterparts might be intuitive, but the interface of these components might actually be even more important. Concrete examples of this are cyber risk management techniques that focus on reducing risk through how people utilize various technologies. Ideally, technical solutions for cyber risk management would take advantage of human behavior and cognition, rather than work against them.

The third and final interesting aspect of cyber risks in healthcare (and in general) is the merging of the old and the new. In a healthcare context, this is embodied by the decades old piece of equipment that should remain as is, but must somehow be geared to deal with its new environment. Organizations that have been around for a long time are adopting new processes and technologies at a fast rate. It may not be economically feasible or sensible to update everything at once, so this modernization will have to take existing systems and equipment into account.

5.3 Study Limitations and Recommendations for Future Research

Research results and the process by which they have been obtained must always be evaluated as part of the study. Reliability of a study refers to the repeatability of its results, which should not be a one-time finding. If the study were to be repeated, it should lead to similar results. Research validity means that the chosen measures or indicators truly measure what they are intended to. Evaluating validity and reliability in qualitative research is not always straightforward, but the quality of the study should still be addressed. A detailed description of the research methodology and data collection can enhance the credibility of the study. This includes describing the circumstances and possible problems or disruptions of data collection. (Hirsijärvi, Remes & Sajavaara 2015, 231-233)

Several steps have been taken during the research process and data collection to improve the credibility of this study. These include providing the reader with a detailed account of the data and how it was acquired. The research questions used during the semi-structured surveys are also included in the study. Certain parts of the data collected during this thesis are not available to the general public, as requested by study participants. To improve the transparency of the research results, an ample amount of direct quotations from the study participants has been included in the data analysis chapter. This grants the reader a direct line of sight into the data that serves as the basis of the research results. The interviews were transcribed shortly after the interviews had taken place, and this phase was carried out with care and meticulousness. The transcriptions were checked for accuracy. Particular attention was paid to the translation of selected portions of the transcript, so that they embody the original intent and tone of the speaker as closely as possible. The analysis and conclusions of this thesis rest on the interpretations of an individual person, which can weaken the quality of research. As suggested by Hirsijärvi et al., (2015, 233) the credibility of research findings can be improved by including a larger number of participants in the process.

This study has several limitations. A large portion of it focuses on one healthcare organization, so the findings are not necessarily applicable to other organizations. Healthcare organizations, particularly on the global scale, represent a massive array of varying entities.

Any meaningful comparison of them regarding cyber risk management would be a daunting task, given the significance of contextual and environmental factors. The data about PHD cyber risk management has been collected from participants that are affiliated with the organization. A limitation of interviews as a research method is the possibility that interviewees may present what they perceive to be acceptable answers (Hirsijärvi et al. 2009, 206). The study participants hold positions at the PHD that enable them to offer the best available information on the subject at hand. The views expressed in the interviews are in accordance with one another, and with publically available information as well.

The research body surrounding cyber risks at this particular time is somewhat incohesive. This is exemplified by the high level of discordance amongst research results, regarding things like what cyber events cost, and what are their key drivers. The research body itself is not very extensive, especially when compared to other areas of risk management theory. Academic studies on cyber risks in healthcare are very few in number. This thesis has partly relied upon industry publications, which are not considered as the most rigorous of sources. Many of the available academic studies have also referenced various industry reports. Eling and Schnell (2016) have commented on the possible biases that information presented by security or consulting firms might contain. A lot of the available studies involve small samples and self-reporting. Making generalizations based on this kind of research might not be straightforward. For example, the Ponemon (2017) study of data breaches included 419 organizations from 17 industries. Healthcare represents 2 % of the sample, so the results regarding this sector are based on about 8 organizations. How meaningfully can these results be extrapolated to an organization like the PHD? Cyber risk management research within Finnish context is difficult to find, but certain examples do exist. This branch of risk management theory is much newer, so this is an understandable situation. It also makes it much more interesting, as many questions are still without clear answers.

Cyber risk management in healthcare represents a subsection within a broader field of study, and is yet to be fully explored. This leaves plenty of questions open to consideration in the future. This thesis was very general in its nature, so further research could involve a smaller scope, such as the significance of a cyber risk process, or individual risk management techniques. An interesting area of study would also be the public perception of healthcare cyber risks, and their impact on actual health outcome. The US FDA issued a recall of nearly half a million pacemakers due to cyber risk fears in August 2017. This will not involve surgical replacement of the devices, (FDA 2017) but it has received a fair amount of media attention nonetheless. What sort of real-world health repercussions could these events lead to, and how would this impact the decision-making process to undergo medical procedures? Other important but unaddressed areas also involve the economic impacts on healthcare spending and how resources are allocated. Cyber risks in healthcare are also interesting from an insurance perspective. If the 500,000 pacemakers had been publicized because of a terrorist attack or an act of warfare rather than a recall, what would have been the insurance implications? A final area of future research involves new strategies of cyber risk management, and the accommodation of old strategies to these new types of risk. Cyber risks appear to be a significant source of uncertainty, and as such there will probably be a growing market for risk management solutions. Perhaps the ingenuity of the securities market will be harnessed to help meet this demand, in the form of financial product and other innovations.

References

Literature

Baer, Walter & Parkinson, Andrew. 2007. Cyberinsurance in IT Security Management. IEEE Security and Privacy. 2016:5(3) DOI: 10.1109/MSP.2007.57

Bendovschi. Andreea. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, Vol. 28, 24-31

Berliner, Baruch. 1982. Limits of Insurability of Risks. Englewood Cliffs, NJ: Prentice Hall.

Berliner, Baruch. 1985. Large Risks and Limits of Insurability. The Geneva Papers on Risk and Insurance – Issues and Practice 10:4, 313-329

Blanke, Sandra & McGrady, Elizabeth. 2016. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. Journal of Healthcare Risk Management 36(1); 14-24

Biener, Christian, Eling, Martin & Wirfs, Jan Hendrik. 2015. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice 40:1, 131-158

Collum, Taleah & Menachemi, Nir. 2011. Benefits and drawback of electronic health record systems. Risk management and Healthcare Policy 2011:4 47-55

Eling, Martin & Schnell, Werner. 2016. What do we know about cyber risk and cyber insurance? The Journal of Risk Finance [1526-5943] v:2016 vsk/osa:17 iss:5 s:474

Filkins, Barbara, Kim, Young, Roberts, Bruce, Armstrong, Winston, Miller, Mark, Hultner, Michael, Castillo, Anthony, Ducom, Jean-Cristophe, Topol, Eric & Steinhubl, Steven. 2016. Privacy and security in the era of digital health: what should translational researchers know and do about it? American Journal of Translational Research 8(3); 1560-1580

Fraser, John & Simkins, Betty. 2010. Enterprise Risk Management-Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ: John Wiley & Sons Inc.

Galletta, Anne. 2012. Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication. New York: NYU Press

Guikema, Seth & Aven Terje. 2010. Assessing risk from intelligent attacks: a perspective on approaches. Reliability Engineering and System Safety 2010, 95:5, 478-483

Hathaway, Oona & Crootof, Rebecca. 2012. The Law of Cyber-Attack. Yale Law School Faculty Scholarship Series. Paper 3852

Hirsijärvi, Sirkka, Remes, Pirkko & Sajavaara, Paula. 2009. Tutki ja Kirjoita. Helsinki: Kustannusosakeyhtiö Tammi

Hirsijärvi, Sirkka., Remes, Pirkko. & Sajavaara, Paula. 2015. Tutki ja Kirjoita. Helsinki: Kustannusosakeyhtiö Tammi

Holton, Glyn. 2004. Defining Risk. CFA Institute. Financial Analysts Journal, volume 60, 6

Ilmonen, Ilkka, Kallio, Jani, Koskinen, Jani & Rajamäki, Markku. 2013. Johda riskejä- Käytännön opas yrityksen riskienhallintaan. Vantaa: FINVA

Jha, Ashish, DesRoches, Catherine, Campbell, Eric, Donelan, Karen, Rao, Sowmya, Ferris, Timothy, Shields, Alexandra, Rosenbaum, Sara & Blumenthal, David. 2009. Use of Electronic Health Records in US Hospitals. New England Journal of Medicine 2009; 360:1628-1638 April 16, 2009 DOI: 10.1056/NEJMsa0900592

Johnson, Kristin. 2016. Managing Cyber Risks. Georgia Law Review, 50:2, 547-592

Juvonen, Marko, Koskensyrjä, Mikko, Kuhanen, Leena, Ojala, Virva, Pentti, Anne, Porvari, Paavo & Talala, Tero. 2014. Yrityksen riskienhallinta. Vantaa: FINVA

Kendrick, Rupert. 2010. Cyber Risks for Business Professionals: a Management Guide. Cambridgeshire: IT Governance Publishing

Korpela, Karina. 2015. Improving Cyber Security Awareness and Training Programs with Data Analytics. Information Security Journal. 2015:24

Kshetri, Nir. 2010. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin: Springer

Lackland, Daniel, Roccella, Edward, Deutsch, Anne, Fornage, Myriam , George, Mary, Howard, George, Kissela, Brett, Kittner, Steven, Lichtman, Judith, Lisabeth, Lynda, Schwamm, Lee, Smith, Eric & Towfighi, Amytis. 2014. Factors Influencing the Decline in Stroke Mortality. Stroke. 2014; 45:315-353

Lam, James. 2014. Enterprise Risk Management: From Incentives to Controls. Hoboken, NJ: John Wiley & Sons Inc.

Limnéll, Jarno, Majewski, Klaus, & Salminen, Mirva. 2014. Kyberturvallisuus. Jyväskylä: Docendo

Luna, Raul, Rhine, Emily, Myhra, Matthew, Sullivan Ross & Kruse, Clemens. 2016. Cyber Threats to Health Information Systems: A Systematic Review. Technology and Health Care. 2016:24, 1-9

Lundqvist, Sara. 2014. An Exploratory Study of Enterprise Risk Management: Pillars of ERM. Journal Of Accounting, Auditing & Finance, 29(3), 393-429. doi:10.1177/0148558X14535780

Martin, Guy, Martin, Paul, Hankin, Chris, Darzi, Ara, & Kinross, James. 2017. Cyber Security and Healthcare: How Safe are we? British Medical Journal 2017;358:j3179

Moody, Micheal. 2010. Rating Agencies' Impact on Enterprise Risk Management. In: Fraser, John. & Simkins, Betty. 2010 Enterprise Risk Management-Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ: John Wiley & Sons Inc.

Mukhopadhyay, Arunabha, Chatterjee, Samir, Saha, Debashis, Mahanti, Ambuj & Sadhukhan, Samir. 2013. Cyber-risk decision models: To insure IT or not? Decision Support Systems, Volume 56, December 2013, 11-26

Nass, Sharyl, Levit, Laura & Gostin, Lawrence. 2009. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Institute of Medicine. Washington DC: National Academies Press

Payne, Thomas. 2016. Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. Lewis and Clark Law Review 2016:20 (2), 683-715

Perakslis, Eric. 2014. Cybersecurity in Health Care. New England Journal of Medicine 371:395-397

Pfleeger, Shari & Caputo, Deanna. 2012. Leveraging Behavioral Science to Mitigate Cyber Security Risk. Computers and Security. 2012: 31(4)

Price, Jeffrey & Wear, Justin. 2015. Claims Made and Insurance Coverage Available for Losses Arising out of or Related to Electronic Data. Tort Trial & Insurance Practice Law Journal, vol. 51(1), 51-90

Rejda, George. 2013. Principles of Risk Management and Insurance. Pearson series in Finance

Romanosky, Sasha. 2016. Examining the Costs and Causes of Cyber Incidents. Journal of Cyber Security 2016: 2(2), 121-135

Rotenberg, Marc & Jacobs, David. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. Harvard Journal of Law & Public Policy. 2013; 36(2):605-652

Rubenfire, Adam. 2017. A smarter anti-hacker defense. Modern Healthcare 47(4)

Ruusuvuori, Johanna. & Tiittula, Liisa. 2005. Haastattelu - tutkimus, tilanteet ja vuorovaikutus. Tampere: Vastapaino

Saldana, Johnny. 2011. Fundamentals of Qualitative Research. USA: Oxford University Press

Schneier, Bruce. 2014. Carry on: Sound Advice from Schneier on Security. Indianapolis: John Wiley & Sons Inc.

Schneier, Bruce. 2016. Stop trying to fix the user. IEEE Security and Privacy. 2016:14(5) DOI: 10.1109/MSP.2016.101

Sheppard, Ben, Crannell, Mary, & Moulton, Jeff. 2013. Cyber first aid: proactive risk management and decision-making. Journal of Environmental Systems and Decisions 2013, 33:4, 530-535

Shackelford, Scott. 2012. Should your firm invest in cyber insurance? Business Horizons, 55(4), 349-356

Skipper, Harold. & Kwon, Jean. 2007. Risk Management and Insurance – Perspectives in a Global Economy. Malden: Blackwell Publishing

Sligo, Judith, Gault, Robin, Roberts, Vaughan & Villa, Luis. 2017. A literature review for large-scale health information system project planning, implementation and evaluation. International Journal of Medical Informatics. 97; 86-97

Smith, Feff, Dinev, Tamara, & Xu, Heng. 2011. Information Privacy Research: An interdisciplinary review. MIS Quarterly, 35:4, 2011, 989-1015

Susilo, W., Rezaeibagha, F., Khin Than, W. 2015. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal, 44(3), 23-38. doi:10.12826/18333575.2015.0001

Ulsch, MacDonnel. 2014. Cyber Threat – How to Manage the Growing Risk of Cyber Attacks. Hoboken: John Wiley & Sons Inc.

Valtioneuvosto. 2013. Suomen kyberturvallisuusstrategia – Valtioneuvoston periaatepäätös 24.1.2013. Forssa Print

Webb, Timothy & Dayal, Sumer. 2017. Building the wall: Addressing cyber security risks in medical devices in the U.S.A. and Australia. Computer Law & Security Review. 33(4); 559-563

World Medical Association. 2016. WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure. 2016;62(4):145-146

Yener, Dener. 2010. Establishing ERM Systems in Emerging Countries. In: Fraser, J. & Simkins, B. 2010 Enterprise Risk Management-Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ: John Wiley & Sons Inc.

Online References

Allianz: A Guide to Cyber Risk- Managing the Impact of Increasing Interconnectivity. 2015 (27.9.2017) http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Alueuudistus: Health and social services reform. (28.4.2017) http://alueuudistus.fi/en/social-welfare-and-health-care-reform/about-the-reform

BBC: WannaCry ransomware cyber-attacks slow but fears remain. 2015 (15.9.2017) http://www.bbc.com/news/technology-39920141

Case, Elizabeth. Marsh & McLennan Companies: MMC Cyber Handbook 2016 – Increasing resilience in the digital economy (15.5.2017) https://www.rims.org/RiskKnowledge/RISKKnowledgeDocs/MMC-Cyber-Handbook_2016-web-final_222017_103116.pdf

Cebula, James & Young, Lisa: A Taxonomy of Operational Cyber Security Risks. Technical note SEI-2010-TN-028. Software Engineering Institute, Carnegie Mellon University. 2010 (10.4.2017) http://www.sei.cmu.edu/reports/10tn028.pdf

CRO Forum: Cyber Resilience – the cyber risk challenge and the role of insurance. 2014 (9.5.2017) http://www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf

EC: Reform of EU data protection rules (5.5.2017) http://ec.europa.eu/justice/data-protection/reform/index_en.htm

EC: Communication From the Commission to the European Parliament and the Council - Exchanging and Protecting Personal Data in a Globalized World. 2017 (5.5.2017a) http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm

Elkind, Peter. Fortune Magazine: Inside the Hack of the Century. 2015 (17.4.2017) http://fortune.com/sony-hack-part-1/

ENISA: ENISA Threat Landscape Report 2016 15 Top Cyber-Threats and Trends. 2017 (20.9.2017) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

FDA: Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2017 (4.10.2017) https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

Fox-Brewster, Thomas. Forbes: Medical Devices Hit By Ransomware For The First Time In US Hospitals. 2017 (27.9.2017) https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#348f39b1425c

Granite: Riskienhallinnan ohjelmistoyritys (28.4.2017) https://www.granite.fi/tietoa/

Granite: Asiakkaat (28.4.2017a) https://www.granite.fi/asiakkaat/

Granite: About (28.4.2017b) https://granitegrc.com/info/#granite-tool

Granite: Risk Management (28.4.2017c) https://granitegrc.com/modules/

Granite: Information Security Training (28.4.2017d) https://granitegrc.com/informationsecuritytraining/#description

HCIC Task Force: Report on Improving Cyber Security in the Health Care Industry. 2017 (19.9.2017) http://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

Herbolzheimer, Claus. Marsh & McLennan Companies: MMC Cyber Handbook 2016 – Increasing resilience in the digital economy (25.9.2017) https://www.rims.org/RiskKnowledge/RISKKnowledgeDocs/MMC-Cyber-Handbook_2016-web-final_222017_103116.pdf

HS: Palvelunesto-hyökkäys kaatoi Kelan Kanta.fi-palvelun – terveystietojaan ei pääse katsomaan. 2017 (19.9.2017) http://www.hs.fi/kotimaa/art-2000005238478.html

HIPAA: Largest Healthcare Data Breaches of 2016. 2017 (27.9.2017) https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/

IBM: IBM Security Services 2014 Cyber Security Intelligence Index. 2014 (13.5.2017) https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

ISO 31000: ISO/Guide 73:2009 Risk Management and Vocabulary. 2009 (29.3.2017) https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

Istekki: Istekki yrityksenä (18.5.2017) https://www.istekki.fi/istekki-yrityksena

Istekki: Asiakasomistajamme (18.5.2017a) https://www.istekki.fi/asiakasomistajat

Istekki: Palvelut terveyden- ja sosiaalihuollon sekä julkishallinnon ammattilaisille (18.5.2017b)

https://www.istekki.fi/ammattilaiset/palvelut

Kauppalehti: Istekki Oy (18.5.2017) https://www.kauppalehti.fi/yritykset/yritys/istekki+oy/22926330

Korhonen, Marita: Yhteentoimivat sote-tietojärjestelmät mahdollistavat toiminnan uudistamisen. 2016 (28.4.2017) http://alueuudistus.fi/blogi/-/blogs/yhteentoimivat-sote-tietojarjestelmat-mahdollistavat-toiminnan-uudistamisen

KPMG: Health Care and Cyber Security: Increased threats require increased capabilities. 2015 (24.9.2017) https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf

Lehto, Martti & Lehto, Miikael: Kyberturvallisuus sairaalajärjestelmissä: Osa 1. 2017 (19.9.2017) https://www.jyu.fi/it/julkaisut/tekes_2/Kyberturvallisuus

Lääkäriliitto: Terveydenhuollon tietotekniikka. 2016 (16.9.2017) https://www.laakariliitto.fi/koulutus/erityispatevyydet/tietotekniikka/

Merriam-Webster: Cyber (9.4.2017) https://www.merriam-webster.com/dictionary/cyber

Marsh & HM Government: UK Cyber Security 2015 (16.4.2017)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf

McAfee: Net Losses: Estimating the costs of cybercrime. (16.4.2017)
https://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf

McCormick, Thomas: Principles of Bioethics. 2013 (22.5.2017)
https://depts.washington.edu/bioethx/tools/princpl.html

MTV: Nordean palvelut toimivat, OP edelleen hyökkäysten kohteena. 2015. (17.4.2017)
http://www.mtv.fi/uutiset/kotimaa/artikkeli/nordean-palvelut-toimivat-jalleen/4662094

MTV: Kela oli jälleen nettihyökkäyksen kohteena: "Laaja häiriö". 2016 (19.9.2017)
https://www.mtv.fi/uutiset/kotimaa/artikkeli/kela-jalleen-nettihyokkayksen-kohteena-laaja-hairio/6120164#gs.SGdneJg

Norton: 2016 Cyber Security Insights Report. (16.4.2017)
https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf

Oikeusministeriö: 2015 Henkilötietojen suojaa koskevan kansallisen lainsäädännön tarkistaminen (7.5.2017)
http://oikeusministerio.fi/material/attachments/om/valmisteilla/lakihankkeet/informaatio-oikeus/qkm9pWnGJ/EU_tietosuoja.pdf

Ponemon Institute: Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age. 2013 (27.9.2017)
https://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf

Ponemon Institute: 2016 Cost of Cyber Crime Study & the Risk of Business Innovation. (16.4.2017)
http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Ponemon Institute: Sixth Annual Benchmark Study of Privacy and Security of Healthcare Data. 2016a (21.5.2017)
https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf

Ponemon Institute: 2017 Cost of Data Breach Study. 2017 (4.10.2017) https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

PSHP: Aivoinfarktin hoidossa nopeus on aivojen pelastus. 2015a (21.5.2017)
http://www.pshp.fi/fi-FI/Toimipaikat/Tays_Keskussairaala/Hoitoyksikot/Aivoverenkiertohairioyksikko/Aivoinfarktin_hoidossa_nopeus_on_aivojen(45077)

PSHP: Pirkanmaan sairaanhoitopiiri (27.4.2017) http://pshp.fi/fi-FI/Sairaanhoitopiiri

PSHP: Pirkanmaan sairaanhoitopiirin organisaatio. 2015 (27.4.2017) http://pshp.fi/fi-FI/Sairaanhoitopiiri/Organisaatio

PSHP: Riskienhallintapolitiikka. 2015b (30.9.2017) http://www.pshp.fi/download/noname/%7BC61296ED-2BF2-4F0E-B43C-2FD98EB507D3%7D/45190

PSHP: Valtuusto. (27.4.2017a) http://pshp.fi/fi-FI/Sairaanhoitopiiri/Hallinto_ja_paatoksenteko/Valtuusto

PSHP: Hallitus. (27.4.2017b) http://pshp.fi/fi-FI/Sairaanhoitopiiri/Hallinto_ja_paatoksenteko/Hallitus

PSHP: Tietohallinto ja teknologia (27.4.2017c) http://pshp.fi/fi-FI/Sairaanhoitopiiri/Organisaatio/Palvelukeskus/Tietohallinto_ja_teknologia

PSHP: Operations and budget (13.9.2017d) http://pshp.fi/en-US/Hospital_District/Operations_and_Budget

PSHP: Vuosikertomus 2016. 2017e (13.9.2017) http://www.pshp.fi/download/noname/%7BAA4A344D-10AD-4CA9-B632-E9BBD8DABCB6%7D/63722

PSHP: Pirkanmaan sairaanhoitopiiri potilashoidon tunnusluvut (14.9.2017f) http://pshp.fi/fi-FI/Sairaanhoitopiiri/Potilashoidon_tunnusluvut

PSHP: Pirkanmaan sairaanhoitopirin tilinpäätös ja toimintakertomus 2016. 2017g (3.10.2017) http://www.pshp.fi/download/noname/%7B3F32876C-4172-4F8D-A1BD-8BC03A08225B%7D/65841

Sans Institute: Inaugural Health Care Survey. 2013 (24.9.2017) https://www.sans.org/reading-room/whitepapers/analyst/inaugural-health-care-survey-34855

Sans Institute: Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. 2014 (24.9.2017) https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

STM: Legislation. (28.4.2017) http://stm.fi/en/social-and-health-services/legislation

STM: Health services. (28.4.2017a) http://stm.fi/en/primary-health-care

STM: Social welfare and health care system in Finland, responsibilities. (28.4.2017b) http://stm.fi/en/social-and-health-services/responsible-agencies

STM: Primary health care. (28.4.2017c) http://stm.fi/en/primary-health-care

STM: Hospitals and specialized medical care. (28.4.2017d) http://stm.fi/en/hospitals-and-specialised-medical-care

STM: Sairaanhoitopiirit ja erityisvastuualueet. (28.4.207e) http://stm.fi/sairaanhoitopiirit-erityisvastuualueet

STM: Social and health care client fees. (28.4.2017f) http://stm.fi/en/client-fees

STM: Occupational health care. (28.4.2017g) http://stm.fi/en/occupational-health-care

STM: Private social and health services. (28.4.2017h) http://stm.fi/en/private-health-care

STM: Lainsäädäntö ohjaa asiakas- ja potilastietojen hallintaa. (7.6.2017i) http://stm.fi/asiakas-potilastietojen-hallinta

Thesaurus.com: Danger (31.3.2017) http://www.thesaurus.com/browse/danger?s=t

THL: Health expenditure and financing. (28.4.2017) https://www.thl.fi/en/web/thlfi-en/statistics/statistics-by-topic/finances-in-the-health-and-social-services-sector/health-expenditure-and-financing

Valvira: Tietojärjestelmät, tietojärjestelmien rekisteri. (28.4.2017) http://www.valvira.fi/terveydenhuolto/terveysteknologia/tuotteen_markkinoille_saattaminen/tietojarjestelmat

Viestintävirasto: Terveydenhuoltoalan kyberuhkia. 2016 (25.9.2017) https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

VSSHP: Tietokonevirus torjuttu sairaanhoitopiirin tietoverkossa. 2015 (19.9.2017) http://www.vsshp.fi/fi/sairaanhoitopiiri/media-tiedotteet-viestinta/tiedotteet/Sivut/tietokonevirus-torjuttu.aspx

Willis: Willis Fortune 1000 Cyber Disclosure Report. 2013 (27.9.2017) http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf

Yle: Verkkorikolliset tunkeutuvat sairaalan verkkoon, lukitsevat tiedostoja ja vaativat rahaa – Ovatko tietoni turvassa?. 2016 (19.9.2017) https://yle.fi/uutiset/3-8904018

Interviews

Jokela, Antti. PHD Information Management Director. Interview 24.3.2017

Markkinen, Markus. PHD Information Security Manager. Interview 10.5.2017

Riikonen, Jaana. PHD Data Privacy Officer. Interview 2.5.2017

Ruotsala, Marko. Istekki Business Manager. Interview 17.5.2017

Tamminen, Anna. PHD Chief Security Officer. Interview 24.3.2017

Viljamaa, Janne. Granite Chief Commercial Officer. Interview 26.4.2017

Legal References

Act on the Status and Rights of Patients (785/1992)

Constitution of Finland (731/1999)

Directive 2013/40/EU on attacks against information systems

Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

Local Government Act (410/2015)

Occupational Health and Safety Act (23.8.2002/738)

Personal Data Act (523/1999)

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data

Social Welfare Act (1301/2014)

Other References

Koskinen, Lasse. 2017. KATVRS40 Vakuutustiede ja vakuutustutkimus. Lecture: University of Tampere (10.1.2017)

PSHP: Raportti PSHP riskit 2017. 2016

PSHP: Tietoturvapolitiikka. 2016a

Appendix 1: Interview Questions for the PHD

Tamminen, Anna, Jokela, Antti, Markkinen, Markus, and Riikonen, Jaana

Definition and significance of cyber risks

1. What is the significance of cyber risks in your work?
2. How have you defined cyber risks?
3. Have different types of cyber risks been categorized, how?
4. How do you identify significant cyber risks?
5. What are the most significant cyber risks?
6. How have these evolved over time?
7. Are you aware of cyber crime being actively directed at Finnish healthcare organizations?

Cyber risk management

1. How is cyber risk management organized?
2. What factors impact cyber risk management?
3. What are the most important risk management methods?
4. How do you take different parts of the PHD into account?
5. What is the significance of regulation?
6. Are external parties involved in cyber risk management?
7. What sort of policies and directions do you have?
8. What is the role of the patient in cyber risk management?
9. What is the significant of personnel training?

Cyber risks as a part of ERM and healthcare

1. How do cyber risks relate to other risks?
2. What is the role of the risk management policy in cyber risks?
3. Does operating in the healthcare sector matter?

Future development and improvement

1. How do you develop cyber risk management?
2. How do you see this in the future?
3. What is the significance of the healthcare reform?
4. Have you observed any benefits?
5. Have you observed any problem areas?
6. Are there any strengths or weaknesses in cyber risk management?

Miscellaneous

1. Anything else that you would like to bring up?

Appendix 2: Interview Questions for Granite and Istekki

Granite: Viljamaa, Janne

Istekki: Ruotsala, Marko

Cyber risks in healthcare

1. How do you take cyber risks into account in your product and services?
2. Do you have any services specifically for the healthcare sector?
3. Do cyber risks differ in healthcare?
4. Is healthcare protected from certain types of cyber risks?

Cyber risk management in healthcare

1. Does healthcare have any significance for cyber risk management?
2. What is your view of cyber risk management in healthcare?
3. What is the significance of Granite in healthcare risk management?
4. Are you aware of any problem areas or strengths that healthcare may have in terms of cyber risk management?

Healthcare organizations as clients

1. How do hospital districts differ as clients?
2. How aware are healthcare representatives of cyber risk management?
3. Do you see these possible differences as being due to healthcare or other factors?
4. How do you take legal perspectives into account?
5. Have you learned anything from the healthcare sector that has been useful elsewhere?

Future developments and improvement

1. How do you develop your services regarding cyber risks?
2. What is the significance of the healthcare reform?
3. How do you see this developing in the future?

Miscellaneous

1. Anything else that you would like to bring up?