Tero Haukilehto

Cybersecurity management in healthcare

Policies, awareness and incident reporting

ACTA WASAENSIA 532

Vaasan yliopisto
UNIVERSITY OF VAASA

ISBN 978-952-395-139-6 (print)
978-952-395-140-2 (online)

ISSN 0355-2667 (Acta Wasaensia 532, print)
2323-9123 (Acta Wasaensia 532, online)

URN https://urn.fi/URN:ISBN:978-952-395-140-2

Hansaprint Oy, Turenki, 2024.

ACADEMIC DISSERTATION

To be presented, with the permission of the Board of the School of Technology and Innovations of the University of Vaasa, for public examination on the 12th of June, 2024, at noon.

Monograph, School of Technology and Innovations, Information Systems Science

Author	Tero Haukilehto
Supervisors	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science
	University lecturer Timo Mantere University of Vaasa. School of Technology and Innovations, Automation Technology
Custos	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science
Reviewers	Professor Dorothea La “Chon” Abraham Raymond A. Mason School of Business, William & Mary
	Professor Clements Scott Kruse Texas State University, School of Health Administration
Opponents	Professor Clements Scott Kruse Texas State University, School of Health Administration
	Professor Kimmo Halunen University of Oulu and National Defence University of Finland

Tiivistelmä

Terveydenhuolto on digitalisoitunut nopeasti, minkä ansiosta tehokkuus, reagointikyky sekä potilashoidon saatavuus ovat parantuneet. Samaan aikaan digitalisaatio on altistanut terveydenhuoltosektorin vakaville kyberturvallisuus-riskeille, kuten kyberhyökkäyksille, jotka ovat lamauttaneet terveydenhuollon organisaatioiden toimintaa ja vaarantaneet potilasturvallisuuden. Tänä päivänä terveydenhuolto tarvitsee kyberturvallisuutta enemmän kuin koskaan.

Kuitenkin tutkimus kyberturvallisuuden hallinnasta terveydenhuollossa on ollut puutteellista ja sopiva malli kyberturvallisuuden hallinnan parantamiseen terveydenhuollossa on puuttunut. Tämä tutkimus esittelee PAR-mallin, joka on suunniteltu kyberturvallisuuden hallinnan kehittämiseen terveydenhuollon organisaatioissa.

PAR-malli käsittää kolme vaihetta: politiikat, tietoisuus ja poikkeamaraportointi. Malli luotiin tässä interpretivistisessä tutkimuksessa tutkimalla jokaista vaihetta hyödyntäen sekä laadullisia, että määrällisiä tutkimusmenetelmiä. Politiikkoja tutkittiin analysoimalla 21:tä terveydenhuolto-organisaation tietoturvapolitiikkaa, kyberturvallisuustietoisuutta tutkittiin kyselyin, joihin osallistui yli 1200 terveydenhuollossa työskentelevää henkilöä, ja poikkeamaraportointia tutkittiin analysoimalla 275:tä kyberturvallisuuteen liittyvää poikkeamaa, jotka oli raportoitu terveydenhuollossa.

Tämä tutkimus lisää ymmärrystämme terveydenhuollon kyberturvallisuudesta. Lisäksi PAR-malli antaa meille uutta tietoa kyberturvallisuuden hallinnasta terveydenhuollossa sekä selittää yhteyden kyberturvallisuuteen liittyvien politiik-kojen, käyttäjien tietoisuuden sekä poikkeamien raportoinnin ja käsittelyn välillä. PAR-mallia voidaan hyödyntää niin tulevissa tutkimuksissa kuin kyber-turvallisuuden parantamisessa terveydenhuollossa.

Asiasanat: Kyberturvallisuus, hallinta, terveydenhuolto, tietoturva, kriittinen infrastruktuuri

Abstract

Healthcare has been digitalized rapidly resulting in improved effectiveness, responsiveness, and accessibility of patient care. At the same time, the digitalization has exposed the sector to serious cybersecurity risks such as cyberattacks, that have impacted the operation of healthcare organizations and risked patient safety. Healthcare needs cybersecurity more than ever now.

However, the research on cybersecurity management in healthcare has been lacking and a proper model for improving cybersecurity management in healthcare has been missing. This study introduces PAR model designed to improve cybersecurity management in healthcare organizations.

The PAR model consists of three phases: Policies, Awareness and Incident Reporting. The model was created by studying each phase in this interpretive research with qualitative and quantitative research methods. Policies were studied by analyzing information security policies of 21 healthcare organizations, cybersecurity awareness of users was investigated with surveys, in which more than 1,200 people working in healthcare organizations participated in. Incident reporting was investigated by analyzing 275 cybersecurity related incidents reported in healthcare.

This study enhances our understanding of cybersecurity in healthcare and the PAR model gives us new information of cybersecurity management in healthcare and explains the relationship between cybersecurity related policies, user awareness, and reporting and handling of incidents. The PAR model can be used both in future studies and in improving cybersecurity in healthcare.

Keywords: Cybersecurity, management, healthcare, information security, critical infrastructure

ACKNOWLEDGEMENT

I would like to thank my supervisors Professor Tero Vartiainen and University Lecturer Timo Mantere, pre-examiners, Professor Dorothea La “Chon” Abraham and Professor Clements Scott Kruse who was also my opponent and I thank my opponent Professor Kimmo Halunen.

I also thank Susann Brunell, Susanne Salmela, Mari Plukka, Tuija Viitala, Tuija Ikonen and Tero Piikkilä from Vaasa Central Hospital.

My loving gratitude goes to my wife and my children.

Finally, I am very grateful to the Finnish education system that offers equal educational opportunities for all, and which has made my career possible.

Seinäjoki, April 2024

Tero Haukilehto

Contents

Figures

Tables

Abbreviations

CISA	Cybersecurity & Infrastructure Security Agency
CSF	Cybersecurity Framework
GDPR	European General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IS	Information system
ISO	International Organization for Standardization
ISP	Information security policy
IT	Information technology
NIST	National Institute of Standards and Technology
OECD	Organization of Economic Co-operation and development
SPTY	The Finnish Society for Patient Safety
VAHTI	Government Information Security Management Board of Finland
VTT	Technical Research Centre of Finland
WHO	World Health Organization

1 INTRODUCTION

1.1 Background and research environment

The healthcare sector is a part of critical infrastructure. This means that it belongs to a group of sectors that are critical for society. If the healthcare sector were damaged, it would have a major negative impact on the whole of society. (Church et al., 2003; European Commission, 2019).

Today, the healthcare sector is more dependent on cybersecurity than ever. The sector has been digitalized rapidly during the past decades and this has led to a situation where it needs reliable operation of information systems that must be protected against malfunctions and cyberattacks (Jalali & Kaiser, 2018). The healthcare sector is also an interesting target for adverse actors and cyberattacks are known to be targeted on healthcare organizations and their employees (Jalali et al., 2020). At worst, cyberattacks and malfunctions have had serious negative impacts on the operation of healthcare organizations and have risked patient safety (Ghafur et al., 2019; Choi et al., 2019).

The U.S Department of Health and Human Services (HHS) maintains a website listing breaches of unsecured protected health information affecting 500 or more individuals. The site lists all reported breaches withing the last 24 months that are currently under investigation by the Office for Civil Rights. In the beginning of 2023, the list contained 866 cases (HHS, 2023). In their annual data breach report IBM has estimated that the highest costs of a data breach by industry are experienced in the healthcare sector with an average of over 10 million USD per data breach. According to the report, healthcare has been the highest cost industry for twelve years running (IBM, 2022). In cyberattacks against healthcare, cybercriminals have used tactics such as ransomware to encrypt files, making the devices and systems that rely on them unusable unless a ransom is paid (CISA, 2022). Some criminal groups are known for using ransomware and especially targeting healthcare organizations (HHS, 2022).

In 2017 the National Health Service (NHS) in the United Kingdom suffered a cyberattack that crippled 200 000 computers in total of 81 hospitals leading to cancellation of 19 000 hospital appointments. It took months to recover from the attack and the estimated costs were at least 92 million pounds. (National health executive, 2018; National Audit Office, 2017).

In 2020, it was revealed that the Finnish psychotherapy Centre Vastaamo had suffered a cyberattack against its services. Serious flaws in the company's security controls enabled the hacker to copy the entire patient record database. First, the hacker demanded ransom which the company did not pay. Later the hacker contacted the patients directly and demanded a ransom or their personal patient records would be published. The hacked database was eventually leaked to the public containing sensitive information of up to 40 000 patients including information the patients shared with their therapists. The cyberattack led to the bankruptcy of the company in 2021. (Wired, 2021; European Data Protection Board, 2022).

These examples show how dependent modern healthcare organizations are on cybersecurity and how devastating consequences can be when cybersecurity is lacking. In both cases, the lack of cybersecurity enabled the successful cyberattack (European Data Protection Board, 2022; National Audit Office, 2017). Furthermore, even though the estimated costs caused by a cyberattack can be high, the total costs that would cover the harm caused to victims can be difficult to calculate and remain unknown. Healthcare organizations should take care of their cybersecurity to increase trust and reduce privacy concerns to ensure patient safety (Kisekka & Giboney, 2018). Investments in cybersecurity should not only be symbolic but institutional factors in the healthcare organizations should be considered to make cybersecurity investments effective (Angst et al., 2017).

The importance of the healthcare sector is known, and it is known that the healthcare sector is more dependent on cybersecurity than ever before. The lack of cybersecurity in the sector has been noted and this has had a serious impact on the operation of healthcare organizations. This led to the following statement: Cybersecurity in healthcare should be improved.

The current state of cybersecurity in the critical infrastructure sectors has been studied worldwide and healthcare along with its dependencies on cybersecurity, and to other critical infrastructure sectors, has been noted (Hemme, 2015; Dunn, 2005; Katina et al., 2014). Yet despite the importance and risks of cybersecurity in healthcare being known, a study concerning the improvement of cybersecurity in the sector has been missing. To improve the current situation, more knowledge was needed, and this dissertation aims to study how to improve cybersecurity in healthcare.

1.2 Objectives and scope

This dissertation analyzed cybersecurity management in healthcare. The subject was studied using the interpretive research approach and the main goal of this study was to develop a tentative theory that could guide cybersecurity management in healthcare. Following Gregor's (2006) primary goals of theory, the nature of this tentative theory was prescriptive that "*provides a description of the method or structure or both for the construction of an artifact (akin to a recipe)*".

The research focus included three areas: information security policies, cybersecurity awareness, and incident reporting. In this study information security policies of healthcare organizations were analyzed; the awareness of cybersecurity was investigated with surveys for healthcare employees. Incident reporting was investigated by analyzing information security incidents reported and processed in healthcare. The areas included in the scope of this study were selected by using the NIST Cybersecurity Framework for improving critical infrastructure cybersecurity (NIST, 2022d).

The hypothesis was that cybersecurity in healthcare should and could be improved with improvements in this area? As mentioned earlier, healthcare is part of the critical infrastructure that has been targeted and has suffered from adverse cyberattacks (Jalali et al., 2020), which supports that cybersecurity should be improved. Considering that complete security is impossible to achieve and that a lack of cybersecurity has enabled the successful cyberattacks against healthcare organizations (European Data Protection Board, 2022; National Audit Office, 2017) it was known that cybersecurity could also be improved.

Cybersecurity and the chosen framework included several other areas that were left out of the scope of this work. The areas included in the scope of this study can be viewed without prior knowledge of cybersecurity or frameworks related to it. Additionally, cybersecurity includes several technical areas that were not included or discussed in this work. Therefore, this work is also for readers who are not technically experienced or do not have prior experience in cybersecurity.

1.3 Research process, questions and dissertation structure

The research process started with systematic literature review on the subject. The literature review revealed how cybersecurity management in healthcare has been studied by the previous literature. From the literature review a research gap of missing interpretive research studying cybersecurity management via ISPs,

cybersecurity awareness and incident reporting was identified. Based on these findings an initial state of the model describing the relationship between cybersecurity awareness, information security policy and incident reporting was created. Figure 1 describes the research process of this dissertation.

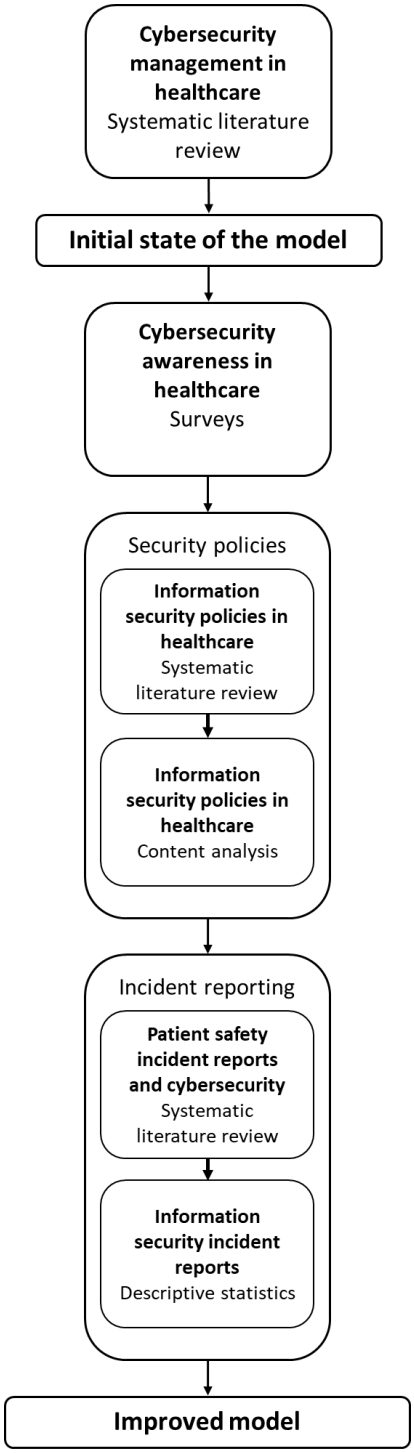

Figure 1. Research process

Next, the three areas included in the scope of this work, namely cybersecurity awareness, ISPs, and incident reporting were taken into closer investigation. This choice was based on the NIST framework for improving critical infrastructure cybersecurity. The idea behind the selection was to select areas that cover all core functions of the framework for improving cybersecurity. In the NIST framework, security policies are connected to the identify phase, awareness is connected to protect phase and incident reporting including the incident handling can be connected to the remaining three phases: detect, respond, and recover. The NIST framework and its core functions are presented in more detail in chapter 2.3.

Cybersecurity awareness was chosen because it was known that it is one of the easiest, fastest, and cheapest ways to improve cybersecurity in an organization (Lehto & 2017). Cybersecurity awareness was studied via surveys for employees in healthcare organizations and included both qualitative and quantitative questions related to cybersecurity. The three surveys had over 1200 respondents in total.

Even though the literature review on cybersecurity management showed that security policies and incident reporting in healthcare had been studied by the previous literature, additional systematic literature review following PRISMA was conducted on both subjects. With these literature reviews, it was shown that there are several research gaps in both subjects and future research was needed. Next, security policies and incident reporting were studied to provide new information.

Security policies were studied by analyzing ISP documents obtained from 21 healthcare organizations with content analysis and comparing the policies against ISO27002 standard guidelines. The third research area, incident reporting, was studied by analyzing information security incident reports reported in healthcare with descriptive statistics. The data sample consisted of 275 information security reports that were reported and handled in one healthcare organization.

After completing the analyzation of the selected research areas, conclusions were drawn and discussed in the discussion chapter. The main findings from the analyzed ISPs, cybersecurity awareness and incident reporting were shown with conclusions. This information was then used to create an improved model that could guide cybersecurity management in healthcare with information security policies, cybersecurity awareness and incident reporting. After theoretical and practical implications, the reliability and validity of this study was discussed. The discussion chapter ended with recommendations for further research.

The following table describes all research questions used in this dissertation.

Table 1. Research questions

Main research question	What kind of model could guide cybersecurity management in healthcare with information security policies, cybersecurity awareness and incident reporting?
1. Sub-question	What areas of cybersecurity management in healthcare have been studied by the previous literature?
2. Sub-question	How do healthcare organizations manage their cybersecurity with cybersecurity awareness?
3. Sub-question	How have information security policies in healthcare been studied by the previous literature?
4. Sub-question	How do healthcare organizations manage their cybersecurity with information security policies?
5. Sub-question	How have patient safety incident reports been used in cybersecurity related studies?
6. Sub-question	How do healthcare organizations manage their cybersecurity with information security incident reporting?

1.4 Scientific research and data protection

In healthcare, personal data is often processed and, for example, patient information systems contain a large amount of personal data. Legislation such as GDPR sets strict requirements for the use of personal data that must be considered in the operation of healthcare organizations (GDPR, 2021). When studying healthcare related information, data protection should also be considered.

To ensure that the requirements and best practices for data protection are considered, this study followed the guidance for scientific research and data protection given by the Office of the Data Protection Ombudsman (2021). The research data used in this study contained information that was obtained from both public sources and directly from the healthcare organizations. For example, ISPs were found on the internet and information security incident reports were obtained directly from a healthcare organization.

As the aims of this study did not require handling any personal data, the use and processing of personal data was minimized thorough the work and considered in the research permit application for information security incident reports. All personal details in the research data were anonymized immediately and were not included in this dissertation. Research data was stored and processed only via the researcher's personal computer. Research data was not transferred, given or stored in other media such as thumb drives or cloud services. In addition, the HaiPro data was not combined with other data such as patient data. The HaiPro data used in this study was removed after analyzation.

2 THEORETICAL FOUNDATION AND RESEARCH APPROACH

2.1 Cybersecurity

We can see the term cyber used broadly today. What is more, there are several other terms that are used with the term cyber. We may have heard of cyberattacks, cyberspace or cyber warfare, for example. English Wikipedia lists hundreds of pages starting with the prefix cyber from Cyber ninjas to Cyber diplomacy (Wikipedia, 2023a). So, what is cyber? The use of the term cyber can be traced at least to the late 1940's and to Norbert Wiener's (1948) book Cybernetics where he defined cybernetics as "control and communication in the animal and the machine". The term cybernetics derives from the Ancient Greek term κυβερνητικης (kubernētikēs, '(good at) steering') that appeared in works of the philosopher Plato over 300 years anno Domini (Wikipedia, 2023b). Today, the Merriam-Webster dictionary defines the term cyber as an "adjective or prefix that means relating to or involving computers or computer networks" (Merriam-webster, 2023a). This definition gives a hint why there are so many cyber related words in today's digitalized and networked world.

One of the cyber related words seen in the headlines is cybersecurity, which is often joined up or sometimes written separately as cyber security. In this work the joined-up form cybersecurity is used. This form is preferred, for example by Merriam-Webster (2023b), Gartner (2023) and CISA (2023). In their article Defining Cybersecurity, Craigen et al. (2014) analyzed the previous literature and the use of the term cybersecurity. They found several different definitions for cybersecurity, analyzed them, and concluded that a broadly accepted definition is missing and that the term cybersecurity has been used broadly, subjectively, and even uninformatively. As an improvement Craigen et al. (2014) proposed the following as a new definition for cybersecurity: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.".

In this dissertation the term cybersecurity is defined in accordance with the Vocabulary of Cybersecurity by The Security Committee of Finland (TSK). The TSK defines that "Cybersecurity means the security of a digital and networked society or organization and its impact on their operations" (TSK, 2018). The main reason for using this definition is that it links cybersecurity to both societal and

organizational levels. This definition was seen to be useful in the context of critical infrastructure and healthcare organizations.

The following Figure 2 illustrates the main cybersecurity related terms and their definitions used in this work. Additionally, Figure 2 shows the connection between these terms and targets to be protected. These definitions are based on TSK's two vocabularies: Vocabulary of Cybersecurity (TSK, 2018) and Vocabulary of Comprehensive Security (TSK, 2017). It should be noted that this is not a comprehensive list of security related terms and that there might be definitions that differ from the ones mentioned in Figure 2.

Target to be protected	Term used of the protection
Society	**Concept for comprehensive security** is a state where vital societal functions are handled together by authorities, businesses, NGOs and citizens.
Digital and networked society or organization	**Cybersecurity** means the security of a digital and networked society or organization and its impact on their operations.
Organization	**Organizational security** means the security of the organization's personnel, information, material, technical infrastructure and environment.
Information	**Information security** means arrangements aimed at ensuring the availability, integrity and confidentiality of information.
Personal data	**Data protection** means arrangements aimed at ensuring the appropriate processing of personal data and their privacy preservation

Figure 2. Cybersecurity related terms

As seen in Figure 2, in the background the target to be protected is a society. The term used for protecting a society is "Concept for comprehensive security" (TSK, 2017). Even though this concept is the Finnish cooperation model for preparedness and will not be discussed in detail in this work, it aims to protect vital societal functions (TSK, 2022). On the second level, the target to be protected is a digital and networked society or organization that is protected with cybersecurity (TSK, 2018). Different from the definition by Craigen et al. (2014), for example, cybersecurity is not only for protecting cyberspace but for protecting a digital and networked society or an organization (TSK, 2018).

On the third level, to protect an organization the term "organizational security" is used. As the term says, the main goal for organizational security is to protect the organization and more precisely, to protect the personnel in the organization, information, material, technical infrastructure, and environment. On the next level, information is protected with the term "information security". Information

security aims to ensure the availability, integrity and confidentiality of information. At the bottom, the target to be protected is personal data and the term used is "data protection". (TSK, 2017, TSK 2018)

Information security is often linked to the classical CIA triad that includes protection of *Confidentiality*, *Integrity* and *Availability* of data (Samonas & Coss, 2014). As stated by Samonas and Coss (2014), even though there have been many expansions suggested, the CIA triad has remained in use for several decades. In a glossary of the computer security resource center of the NIST (NIST, 2022a) and in an ISO15288 standard for systems and software engineering (ISO, 2015), the term *Usability* has been stated as the fifth attribute of security in addition to confidentiality, integrity, availability, and accountability. The term *Usability* refers also to the effectiveness and efficiency of a system that satisfies user needs (Weir et al., 2009). Furthermore, conflicts between usability and security are a known issue that must be considered with information systems (Yee, 2004).

In some cases, the terms *Availability* and *Usability* can be confused. The Finnish National Cyber Security Centre, for example, defines information security with the classical CIA triad with terms *Confidentiality*, *Integrity,* and *Availability* of data on their English language site, whereas in the Finnish version of the same site the term *Availability* has been replaced with the Finnish term for *Usability* (National Cyber Security Centre of Finland, 2022). This is also the case with the European GDPR's article 32 that contains the term *Availability* in the English version but in the Finnish version the term refers to *Usability* (GDPR, 2016). Even though the two terms can be mixed, they have different meanings. According to NIST, the term *Usability* refers to the effectiveness, efficiency, and satisfaction in a specified context of use, whereas *Availability* stands for "Ensuring timely and reliable access to and use of information" (NIST 2022b, NIST 2022c).

2.2 Digitalized healthcare needs cybersecurity

According to Wikipedia, healthcare or health care is "the improvement of health via the prevention, diagnosis, treatment, amelioration or cure of disease, illness, injury, and other physical and mental impairments in people" (Wikipedia, 2023c). In a shorter definition, the Cambridge Dictionary (2023) describes healthcare as "the activity or business of providing medical services". Healthcare services can be provided by public or private providers, where public healthcare is often provided by the government and private healthcare is provided by "for profit" providers or "not for profit" non-governmental providers (Basu et al., 2012).

Healthcare is expensive and unequal. The global spending on healthcare has been increasing for years and reached US$ 9 trillion in 2020 that represents 10,8% of global gross domestic product (Global GDP). From the total spending, US$ 5.7 trillion (63 %) was from government sources, and US$ 3.3 trillion (36 %) was from private sources. Most of the health spending accounted for high income countries, whereas in low-income countries external aid is playing a critical role in providing healthcare. In 2020, the share of the United States (15.3 % of the world's population) of global spending on health was 43.5 percent whereas the global spending of low-income countries on health (8 % of world's population) was 0.2 % combined. Overall, the WHO has estimated that 30 % of the world's population do not have access to essential health services. (WHO, 2022a, 2022b).

Still, life expectancy has increased almost in all countries over the world for the past 50 years (Ourworldindata, 2023). Behind this trend are things such as improved living environments, healthier lifestyles, and rising incomes. One of the reasons for increased life expectancy has been more accessible and higher quality healthcare that have been achieved with the help of digital health services. (OECD, 2021). With digitalization several factors such as effectiveness, responsiveness, and accessibility have been improved in healthcare (OECD, 2021). Furthermore, digitalization has been used to make healthcare more cost-effective (OECD, 2021). Nonetheless, it is estimated that the healthcare sector is far behind in using the potential of digitalization that could save both lives and money (OECD, 2019).

To get a visual overview of the rapid digitalization of healthcare and its dependencies on cybersecurity the following two photos can used.

Figure 3. Hospital bed in the 20th century (Wikimedia Commons, 2023)

Figure 4. Operating room in the 21st century (Pixabay, 2023)

The first picture (Figure 3) shows a hospital bed. According to Wikimedia Commons (2023), the photo was taken in Budabest in 1963. Another piece of information informs the photo was taken in 1930. In any case, the exact year is not important, because for this brief overview of the digitalization of healthcare, it is enough to known that the photo was taken in the 20th century.

What can be seen in the first photo is one empty hospital bed in the center and almost half of another bed on the left. Even though the photo is in black and white the room is clean, there is a sink and waterpipes, two electric lights, one above the sink and another above the bed. Additional furniture can be seen such as an empty chair, and two desks, one on the right side of each bed. There is a drinking glass on the table on the left, flowers in a vase on each table, a mirror, a toothbrush and more. At the foot of both beds there is an information board, that is probably used for patient information.

The second photo (Figure 4) was taken in an operating room in a hospital. This photo has been published in 2020 on Pixabay.com, that shares royalty-free photos (Pixabay, 2023). The exact date or year when the photo was taken is not mentioned, however, considering the equipment seen in the photo, such as flat screens, the photo was taken in the 21st century. According to the photo and its description, there is an ongoing medical operation in the room where a person is undergoing surgery and is surrounded by several health professionals such as a surgeon and surgical assistants. The patient, his or her personal details or body are not visible in the photo.

What stands out in this photo is the high amount of digital equipment. There are, for example, several monitors, racks with devices, lots of cables, tubes, and lights. It almost seems like the room is full of electric devices. What is left out of this photo is not known, but at least some of the devices are not fully shown, meaning that there is more electronic equipment in the room. Moreover, it is known that in hospitals heating ventilation and air conditioning (HVAC) can be connected to a network and controlled remotely (HIPAA journal, 2021).

These two photos show the rapid digitalization of healthcare. Even though the use of medicine is thousands of years old (Hajar, 2015), in less than hundred years the amount of electronic equipment used in healthcare has been drastically increased. Whereas, in the first photo there were no electronic equipment except lights, in the second photo there is a great amount of digital and networked devices being used.

These two photos also show the rapid growth of dependence on cybersecurity in healthcare. In the first photo, there was no digital equipment used, meaning the risk of cyberattack, for example, did not exist, because there were no networks or

devices that could have been attacked. Considering the TSK's (2018) definition for cybersecurity namely "Cybersecurity means the security of a digital and networked society or organization and its impact on their operations", cybersecurity was not needed during the time the first photo was taken because neither the society or the organization was digital and networked.

In the second photo, it can be clearly seen that there are digital and networked equipment being used. This equipment is part of the organization's attack surface that is the sum of the different ways an attacker could try to affect the digital environment (NIST, 2023). Whereas in the first photo, the risk of cyberattack did not exist, in this photo there is a risk of cyberattack. These indications show that the organization in the second photo is digital and networked and therefore needs cybersecurity.

It is known that healthcare organizations need the reliable operation of information systems that must be protected against malfunctions and cyberattacks (Jalali & Kaiser, 2018). Yet, the task is challenging because healthcare organizations such as hospitals are very complex organizations (Smet, 2002) with complex IT environments that should be considered in the organization's cybersecurity (Jalali & Kaiser, 2018).

2.3 Improving cybersecurity

One of the most known frameworks for cybersecurity management was published by the National Institute of Standards and Technology (NIST) for improving critical infrastructure cybersecurity, also known as the NIST Cybersecurity Framework or CSF (NIST, 2022d). The aim of the framework is to help organizations, regardless of their size, to better manage cybersecurity risk and it is based on existing standards, guidelines, and practice. Even though the framework is voluntary guidance, it is mandatory for US federal government agencies. (NIST, 2022e).

As seen in Figure 5, the CSF framework version 1.1 consists of five phases called *Core Functions*. These core functions are: *Identify*, *Protect*, *Detect*, *Respond* and *Recover*. Furthermore, each core function contains categories with subcategories and informative references. The whole framework with more details and hands on guidance is freely available on the NIST website. (NIST, 2022d).

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 5. CSF Core Functions and Categories framework (NIST, 2018)

At the core function level, the *Identify* function aims to develop an understanding of the organization's context and what should be protected with cybersecurity. The *Protect* function's goal is to develop and implement cybersecurity protection to the identified targets of the protection. The *Detect* function is needed to detect cybersecurity events such as anomalies and the *Respond* function considers actions that will be taken when cybersecurity incidents that have an impact on the organization are detected. The fifth function, *Recover,* stands for developing and implementing activities and plans to recover from cybersecurity incidents. (NIST, 2018).

In this work, the CSF and its core functions were utilized as guidelines to determine the scope of the study and areas to be studied on how to improve cybersecurity in healthcare. Because it would have been impossible to cover all categories in one study, the selection of areas to be studied aimed to cover all core functions of the CSF framework. The areas to be studied and their correspondence in the CSF core functions are listed in Table 2.

Table 2. CSF core functions and areas to be studied.

CSF Core Function	Area to be studied
Identify	Information security policies
Protect	Cybersecurity awareness
Detect, Respond & Recover	Incident reporting (including analyzation and handling of incidents)

2.4 Research approach

It has been argued that choice of theory is essentially subjective (Walsham, 2006). Nonetheless, the use of the interpretive research method is justified for this study as it can provide a deep insight into the phenomenon of interest and assists in deriving a theory from the gathered data. Interpretive research is a research method that uses existing observed data to derive a theory about a phenomenon in a specific context (Bhattacherjee, 2012). In this study, the context was cybersecurity management in healthcare organizations, the phenomenon of interest was the relationship between information security policies, cybersecurity awareness, and incident reporting. The observed data was gathered from healthcare organizations and employees working in the healthcare sector.

Schwandt (1994) claimed that the interpretive research approach helps to understand "the complex world of lived experience from the point of view of those who live it". Even tough interpretive research can be mixed with qualitative research, the characteristic of interpretive research contains the assumption that reality is socially constructed and subjective, and that there are multiple ways of knowing and understanding the world. In interpretive research, the researcher tries to interpret the reality though a sense-making process by exploring and describing the complexity and richness of a phenomenon, rather than testing theories or hypotheses. (Bhattacherjee, 2012).

Whereas the positivist researcher starts with a theory and tries to test it with empirical data, the interpretive researcher starts with data and tries to derive a theory from it. In this process, the interpretive researcher often uses qualitative data, but quantitative data may be used to improve the precision and understanding of the phenomenon. When performing interpretive research, collecting both qualitative and quantitative data can be seen as preferred because of its potential to provide novel insights about the phenomenon. (Bhattacherjee, 2012).

In IS studies, interpretive research design has been preferred because of its nature to explore human thought and action within social and organizational contexts. Interpretive research can help to understand both the context of the IS and the process where the IS is influenced by the context (Walsham, 1993). This makes it possible to provide a better understanding of IS related phenomenon such as the management of IS and IS development. It has been argued that IS research is interpretive when it assumes "that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools, and other artifacts". (Klein & Myers, 1999).

Walsham noted that an interpretive researcher should have access to relevant organizations to enable the fieldwork for the study. The researcher should also have good social skills and have courage to try different ways to gain and maintain the access if the first try fails. However, according to Walsham, change, luck, and serendipity are needed. (Walsham, 2006).

As mentioned, interpretive research tries to derive a theory from the gathered data and in this process, generalizability is used. The research data of interpretive research often consists of interviews, publications on the sectoral context, internal documents, observations, web-based data or surveys. (Walsham, 2006). Walsham asks whether it is possible to use generalizability in interpretive research where the research data can contain data from one organization only? By citing his earlier work (Walsham, 1995) and the work by Lee and Baskerville (2003), Walsham claims that even with a limited set of organizations, generalizability is possible with outcomes such as concepts, theories, specific implications or rich insights. (Walsham, 2006).

In conclusion, the use of the interpretive research method is justified for this study. The emphasis of the interpretive research method on subjective meanings, understanding the context and theory development is aligned with the research question and supports the main goal of this study. With the interpretive research approach, this study can provide valuable insights into healthcare cybersecurity with theoretical and practical contribution.

2.5 Research methods

Through following the interpretive research approach, this study aimed to derive a theory, a model that could guide cybersecurity management in healthcare with information security policy, cybersecurity awareness, and incident reporting from the gathered data. After the systematic literature review on cybersecurity management in healthcare, first an initial version of the model was created, and after studying the three areas of interest, the gathered data was used to create a final version of the model.

As suggested by Walsham (2006) for interpretive research both qualitative and quantitative data was gathered. The research data consisted of relevant literature, survey data, organizational documents and data gathered from a database containing reported information security incidents reports and handling in healthcare. The research methods used in this study included systematic literature reviews, surveys, content analysis and descriptive statistics. Literature reviews were conducted by following the common approaches of a literature review

(Webster & Watson, 2002) and through using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to derive the structure of the review (Moher et al., 2009). With literature reviews it was possible to provide information on the previous literature on the specific subject, and identify research gaps.

Cybersecurity awareness was studied with surveys for employees working in the healthcare sector. Two out of three surveys were conducted in paper form and one survey was conducted as an online questionnaire. All surveys contained both qualitative and quantitative questions. After gathering the data, survey results were digitalized and analyzed using content analysis that is useful to form interpretations from the content and to increase the value of the gathered information (Hsieh & Shannon, 2005).

Information security policy documents obtained from healthcare organizations were also analyzed with content analysis. The use of content analysis was chosen because it is a widely used research technique for analyzing and quantifying text and useful to make interpretations from the content (Hsieh & Shannon, 2005).

Information security incident reporting was studied with analyzing information security incidents reported and handled in healthcare. In this analyzation, descriptive statistics was used. Descriptive statistics are useful when the researcher wants to describe the characteristics of the data (Fisher & Marshal, 2009). Descriptive statistics was chosen based on the literature review on patient safety incident reports that provided information about the methods used in studies studying incident reports and because descriptive statistics was seen to support the interpretive research approach.

In conclusion, the used research methods were selected to support the interpretive research approach and to provide a deep insight into the phenomenon of interest and help to derive a theory from the gathered data.

2.6 Initial state of the model for improving cybersecurity management in healthcare

As shown in the literature review in chapter 3, research on cybersecurity management in healthcare was lacking. In addition to the identified research gap, it was known that cybersecurity management in healthcare was also lacking (Ghafur et al., 2019; Choi et al., 2019). To fill the identified research gap and to provide a better understanding on how cybersecurity management in healthcare could be improved, a new model was needed.

Based on the NIST cybersecurity framework and the three chosen areas justified in chapter 2.3 this model aimed to describe what kind of model could guide cybersecurity management in healthcare with information security policies, cybersecurity awareness and incident reporting. Table 3 describes the initial state of the model.

Table 3. Initial state of the model

Cybersecurity management	Cybersecurity awareness
	Information security policy
	Incident reporting

At the beginning of this study it was known that the three areas seen in Table 3, cybersecurity awareness, information security policy, and incident reporting, are parts of cybersecurity management and when improving cybersecurity each area should be considered (NIST, 2018). Whereas cybersecurity awareness has been stated to be one of the easiest, fastest, and cheapest way to improve cybersecurity in an organization (Lehto & Limnéll, 2017), information security policy was seen as one of the most important cybersecurity related controls for an organization (Höne et al., 2002). On the other hand, incident reporting was known to play an important role in learning from incidents and preventing incidents that in the healthcare sector can be directly related to patient safety (Kohn et al., 2002).

As seen in Table 3, the initial state of the model listed the areas of interest, but did not describe the relationship between cybersecurity awareness, information security policies, or incident reporting. With this model, understanding cybersecurity management in healthcare or improving cybersecurity in healthcare could be difficult. Therefore, there was a need to improve the initial model. To improve the model, each area was studied in the following chapters.

3 CYBERSECURITY MANAGEMENT IN HEALTHCARE - LITERATURE REVIEW

The key responsibility in cybersecurity in healthcare organizations resides with management (Blanke & McGrady, 2016). The surveys in the previous chapter showed that cybersecurity awareness is lacking among management and concluded that cybersecurity awareness should be improved in healthcare organizations starting from the management level.

The previous systematic literature reviews have focused on cybersecurity vulnerabilities in healthcare (Kruse et al., 2017), or studied the literature related to cybersecurity and healthcare revealing that the management of cybersecurity in healthcare might be understudied (Jalali et al., 2019). When considering the importance of management of cybersecurity for healthcare, there was a need to provide a holistic view of the literature related to the subject. This literature review aimed to answer the following research question: What areas of cybersecurity management in healthcare have been studied by the previous literature?

3.1 Study eligibility criteria

A systematic review was used following the common approaches of a literature review (Webster & Watson, 2002). To focus on the representative literature regarding cybersecurity management in the healthcare sector, the literature reviewed consisted of journal articles found with keywords including cybersecurity management and healthcare related terms. Because the word “cyber” might not be included in all relevant articles, terms related to securing IT infrastructure and information security such as “data”, “protection”, “computer” and “security” were included. In addition, the word “administration” was included to widen the search to managerial articles besides including results found with word “management” only. To focus on healthcare sector, terms “health” and “healthcare” were used with “hospital” and “hospitals”. In the literature search the following search string was used:

("Data" OR "Computer" OR "Cyber" OR ”Information”) AND
(("Security" OR "Protection") OR ”Cybersecurity”) AND
("Management" OR "Administration") AND
("Health" OR "Healthcare" OR “Hospital" OR ”Hospitals”)

The electronic databases and search engines used in this study were: PubMed, Cinahl Complete, Ovid Medline, Ebsco Medline and IEEE Xplore Digital Library. The literature search provided 22 516 papers in total. After the initial search, the titles and abstracts of the studies were prescreened for relevance and 64 studies

were retained to be examined in detail. Search results per database with the date range available are shown in Table 4.

Table 4. Search results per database

Database	PubMed	Ebsco Medline	Cinahl Complete	Ovid Medline	IEEE Xplore Digital Library
Date range	1974 - 2019	1935 - 2019	1980 - 2019	1946 - 2019	1968 - 2019
Search results	15947	2023	2270	1998	278
Total screened	22516				
After screening	24	15	10	11	4

3.2 Data evaluation

The following evaluation criteria for the literature were used:

- Published in English
- Scholarly journal article or peer reviewed
- Abstract available

Papers that did not meet the evaluation criteria were excluded. These papers included non-managerial and technology-focused studies such as medical device security studies and studies concentrating on cybersecurity vulnerabilities or data breaches. The total of 25 papers were found relevant in detailed examination and retained for appraisal. The evaluation process and the number of papers is described in Figure 6, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) to derive the structure of the review (Moher et al., 2009).

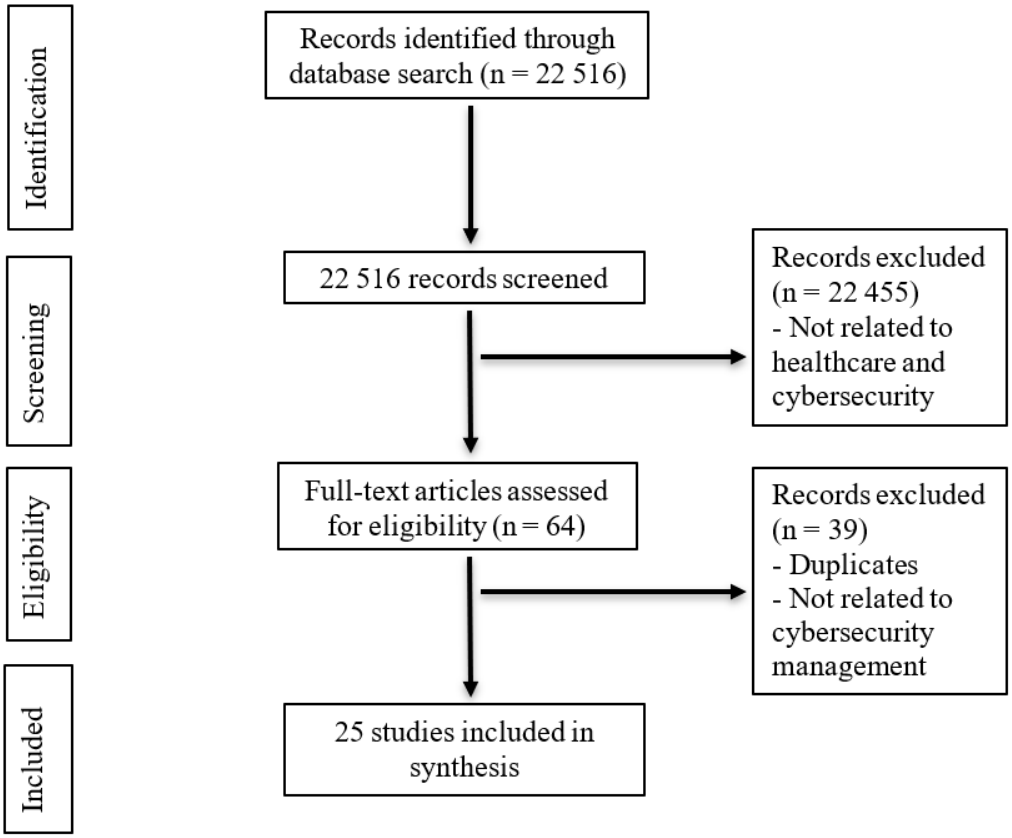

Figure 6. Cybersecurity management in healthcare PRISMA flow diagram

Two different frameworks were used in reviewing the studies included in the synthesis. The frameworks used were the Socio-technical approach and ISO / IEC 27001:2013.

3.3 ISO / IEC 27001 standard

ISO / IEC standards are jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO / IEC 27000-series concentrates on information security and the ISO / IEC 27001 standard focuses on information security management. (ISO, 2020). The use of the ISO / IEC 27001 standard was chosen because it provides clear definitions for different domains to be controlled when securing the IT infrastructure of the organization.

In this study, the ISO / IEC 27001 standard “ISO / IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements" was used. In the standard information, security management

controls have been divided into 14 different domains that can be used to manage information security (ISO, 2020).

3.4 Socio-technical approach

The socio-technical approach presented by Kayworth and Whitten (Kayworth & Whitten, 2010) is a framework for a strategically focused information security strategy. This framework was chosen because besides technology, it also considers organizational integration, and social alignment mechanisms, and includes three primary objectives for an effective information security strategy. All these objectives should be addressed by the security management despite the organizational context. These objectives are: *Ensuring compliance*, *Maintaining cultural fit* and *Balancing information security and business needs*. (Kayworth & Whitten, 2010).

Balancing information security and business needs is described as an objective where risk calculations are business driven with the business continuity and organization characteristics in mind. For example, locking down servers would effectively decrease security risks but hinder business operations. Therefore, a balance between information security and business needs is required.

Ensuring compliance considers all requirements set for the design and implementation of information security policies that come from external sources such as legislation or standards and tries to meet them. For example, a company may have to comply with federal legislation, state legislation and industry standards requirements at the same time.

Maintaining cultural fit aims to ensure that information security guidelines and policies are in alignment with the organizational values and culture. For example, if information security guidelines do not fit the organizational values or culture, employees may not follow the guidelines and employee resistance against security policies can be increased. (Kayworth & Whitten, 2010).

By combining the objectives of the socio-technical approach identified in the studies and ISO / IEC 27001 domains included, the outcome provides information about domains that have or have not been studied with the research focus. This cross comparison could reveal gaps in the literature related to cybersecurity management in healthcare. Furthermore, the cross comparison of these two frameworks can be used in studying cybersecurity management in the future and could help finding the covered and uncovered areas in other sectors as well.

3.5 Literature overview

The date range varied being the longest with the starting year of 1935 in Ebsco Medline and the shortest with the starting year of 1980 in Cinahl Complete, therefore the search covered at least a 39-year period in every database. However, the oldest study included in the synthesis was 20 years old from the 1999 from PubMed database. This signals that the topic may have been studied in different terms before, or that studies meeting the evaluation terms may have not been published prior to 1999.

According to the number of studies included in this synthesis after the evaluation process sorted by the year of the publication, there are a few studies conducted annually related to the cybersecurity management in healthcare sector meeting the evaluation criteria, with the average annual amount of 1,2 studies per year between 1999 and 2019. Because the database search was conducted during 2019, the total number of studies for the year 2019 is not valid. Although, as seen in Figure 7, the number of publications published about the subject annually has been increasing from the year 1999, which may refer that the topic is emerging and that the amount of studies related to the subject will be increasing in the future.

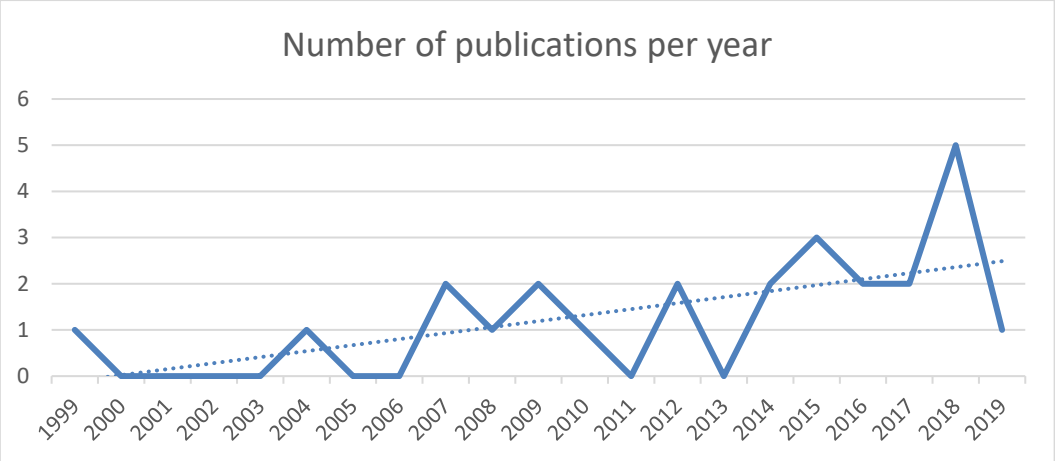

Figure 7. Number of publications included in the synthesis per year of the publication

Many of the studies were originated from the United States with eight publications and the second most common country of origination with four studies were shared between Iran and Australia. The rest of the studies included in the synthesis were from a different country each.

The most common research type used was an empirical study with empirically gathered data. In 9 out of the 20 empirical studies (45%) the data was gathered via surveys and in 7 studies (35%) the data was gathered using interviews. Three studies (15%) included both survey and interview and one study (5%) included survey and workshop with end-users. Five of the 25 studies (20%) were identified as conceptual studies with no empirically gathered data.

In 10 out of the 20 empirical studies (50%) the data was gathered from both public and private sector healthcare organizations, six studies (30%) were using data from public organizations only and one study (5%) was relying on data gathered from a private health care sector organization. In three empirical studies (15%) the sector was not defined. A study conducted by Evans et al. (2019) was the sole paper concentrating solely on the private sector. Zarei and Sadoughi (2016) had gathered data from hospitals operating in sectors such as military and charity, expanding the view and perspective from private and public sectors.

3.6 Standards and guidelines

As requirements, these studies often referred to the Health Insurance Portability and Accountability Act (HIPAA) which is a federal law set by the US congress in 1996, that includes requirements for privacy and security in healthcare (U.S. Department of Health & Human Services, 2017). Besides HIPAA, the studies often referred to other national level standards or guidelines such as HITECH or NIST. When examining the year of publication, the HIPAA was referred to almost during the whole date range from 1999 (O'Brien & Yasnoff, 1999) to 2018 (Jalali & Kaiser, 2018).

The high number of studies referring to HIPAA is explained as due to the high amount of studies originating from the US, whereas studies from other countries often referred to the local national requirements. However, HIPAA was used as a reference outside the US, especially if compared to the local national guidance or requirements or in case of their absence (Fernández-Alemán et al., 2015; Gomes & Lapão, 2008; Samadbeik et al., 2015). Most of the studies even referred to the national level requirements, the most referred international standard or guideline were ISO / IEC standards and especially the ISO 27000-series that was referred to in ten studies.

By using the socio-technical approach represented by Kayworth and Whitten (Kayworth & Whitten, 2010), the studies included in the synthesis were divided into three categories by the research topic and aspect considered in the study. This provided information on how these three primary objectives for an effective

information security management have been studied in the past literature meeting the evaluation criteria.

3.7 Ensuring compliance

From the 25 studies included in the synthesis, in 14 studies (56 %) the research focus was identified as *Ensuring compliance* where 11 studies (79%) included empirically gathered data and 3 studies (21%) were conceptual. In conceptual studies, *Ensuring compliance* was also the most used research focus, which indicates that this has been the most studied research focus of cybersecurity management in the healthcare domain, and that the researchers have found *Ensuring compliance* as important to study.

As stated by Blanke and McGrady (Blanke & McGrady, 2016), the number one sector for reported cybersecurity breaches is healthcare. Even though the cybersecurity can be complex, with many parties involved in maintaining security, the responsibility and the key role in securing the healthcare organization from cybersecurity breaches resides with the management. In their study they list the three most common reported breach types in healthcare: portable devices, insider, and physical breaches. In addition, they introduced a framework for the managers to reduce these risks in the operation of the organization via risk management. (Blanke & McGrady, 2016).

According to Kwon and Johnson (2013), the compliance requirements for healthcare have been increased and derived from the growing concern of information security in the sector. Yet, practices on how to meet certain requirements such as HIPAA or HITECH vary between the organizations. Whereas, the level of compliance can indicate how cybersecurity is managed in the organization, the highest level of compliance was found in large organizations balancing technical and non-technical practices. (Kwon & Johnson, 2013).

Although, many of the studies concentrated on *Ensuring compliance* including legal regulations and international or national standards, (He & Johnson, 2017; Kwon & Johnson, 2013; O'Brien & Yasnoff, 1999; Park et al., 2010; Samadbeik et al., 2015; Schattner et al., 2007; Zarei & Sadoughi, 2016) meeting these standards can be hard to achieve. As stated by Lederman (2004), national laws and regulations for data privacy and information systems in the healthcare domain can be demanding and difficult to comply with in practice and that such actions can require completely new information systems and procedures that need resources and support from regulating authorities.

The requirements of such standards and regulations may have insufficiencies as well, and the outcome can be something else than what was intended. As noted by Kumar et al. (2007), when examining the effects of HIPAA on the healthcare in the United States, the act was intended to improve the patient and information security in US healthcare; however, during the publication it was already outdated, confusing, and difficult to comply with resulting in negative effects on the healthcare sector.

Whereas organizations can concentrate on cybersecurity in their own organization, one characteristic that must be considered in healthcare cybersecurity are the third parties. Third-party related problems in cybersecurity management were reported in three papers, (Hegarty et al., 2014; Kwon & Johnson, 2013; Park et al., 2010). Park et al. (2010) encountered one hospital with over 500 beds that had not addressed security with customers at all.

Third parties can have lower compliance in cybersecurity or even be the source of data-breach as well. As mentioned by Kwon and Johnson (2013), the most advanced healthcare organizations in security-practice adoption took care of auditing and training the third parties, whereas the other organizations put their trust on the agreements between the healthcare organization and third parties. Third parties in this paper included the organizations directly connected to patient care only leaving other third parties such as supporting organizations, manufacturers, and remote consultants out of scope. (Kwon & Johnson, 2013).

3.8 Maintaining cultural fit

Seven of the 25 publications (28 %) were identified as studies with *Maintaining cultural fit* as the research focus and five of them were empirical studies including empirically gathered data. In four empirical studies, the data was gathered from public organizations and in one study the organization type was not identified. None of the studies reportedly gathered data from private healthcare organizations.

Based on the socio-technical approach, the cultural conflicts that security executives try to avoid by maintaining the cultural fit occurs when the information security program does not fit the organizational culture resulting in inconsistent or non-compliance behavior (Kayworth & Whitten, 2010). This kind of behavior was reported for example by Fernández-Alemán, et al. (2015) from a public hospital in Spain where the security behavior of healthcare professional did not meet the security standards, guidelines, or best practices.

Fernando and Dawson reported as a reason for cultural conflicts that the operation of hospitals does not support the regulatory environment in practice and that in some cases, the security features implemented were reported to take time from patient care and felt to interfere with the healthcare process. Such a situation was seen to bring negative feelings and attitude towards privacy and security implementations among the healthcare personnel. However, in the same study the security features that did not have an effect on the patient care process productivity were adopted without a negative outcome (Fernando & Dawson, 2009).

Eikey et al. saw that the IT staff did not have enough knowledge of clinical user needs and practices. To improve cybersecurity by implementing new security features, the communication and knowledge between the IT and the users should be considered. A gap in IT personnel understanding of users' work activities resulted into a situation where security features were implemented by the IT department but bypassed or neglected by the users. In this kind of case, implementing the security feature can be a waste of time and the security is thought to be improved when it is not implemented. Understanding the underlying reasons and reasons for one's behavior were introduced as an improvement. (Eikey et al., 2015). Yet, it can be questioned if the IT department is responsible for the behavior of users and how the management level or other persons responsible for the information share were informed about these implementations and if they shared this information in their departments?

Even traditional ways can influence the information security management, and as written by Jahanbakhsh et al. (2014), the shared administration does not mean that the systems and procedures are standardized or alike. Roles of health information management professionals in health information technology should be clearly defined including responsibilities for cybersecurity (Zeng et al., 2009). However, unclear management roles were found by Jahanbakhsh et al. (2014) and Hegarty et al. (2014) who noted that the management structure in hospitals was not updated to meet modern hospital operations, and they provided an example from a hospital where the responsible for risk management of the medical IT network was the director of the intensive care unit. Park et al. (2010) warned that these kinds of improper dual roles without exclusive charge in information security, can lead to a situation where there are no regulations for responsibilities. The lack of resources or unproper resource management can lead to a situation where one person has too many responsibilities creating person dependency that can pose challenges in an event where the person leaves his or her current role (Hegarty et al., 2014).

Improvement suggestions for *Maintaining cultural fit* included improved security education, security policy, and risk assessment (Fernández-Alemán et al., 2015), as well as creating organizational policies and guidelines that are clearly written and easy to understand (Humaidi & Balakrishnan, 2018). The communication between IT staff and clinical users should be improved (Eikey et al., 2015) and both soft and hard trust mechanisms should be used (Natsiavas et al., 2018).

Fernando and Dawson (2009) suggested that more resources in hospitals supporting privacy and security are needed, and that governments, health authorities, and hospital management should work together to improve the situation. Furthermore, if successful, management support was found to have a positive impact on the health professional's security compliance behavior and increase the trust in organizational security policies (Humaidi & Balakrishnan, 2018). Jahanbakhsh et al. proposed as an improvement a clear national IT strategy and the use of standardization such as the ISO 27000 family (Jahanbakhsh et al., 2014).

3.9 Balancing information security and business needs

In four of the 25 studies included in the synthesis (16 %), the research focus was identified as *Balancing information security and business needs*, three of which were published in 2018 and one in 2019. According to the publication years, there are less publications meeting the evaluation criteria with this research focus than there are with *Ensuring compliance* or *Maintaining cultural fit*, and that *Balancing information security and business needs* has increased attention in studies related to the healthcare domain lately. All four studies were empirical studies with empirically gathered data and therefore no conceptual studies meeting the evaluation criteria with this research focus were found. This signals that these type of studies can be understudied in the healthcare sector.

When comparing the studies with *Ensuring compliance* or *Maintaining cultural fit* as the research focus, the studies focusing on *Balancing information security and business needs* may include both, and more. Natsiavas et al. (2018), for example, used a definition of user scenarios with threat analysis of the business processes that aimed to design a secure and interoperable toolkit for cross-border health data exchange within the European Union including *Ensuring compliance* with ISO / IEC standards and *Maintaining cultural fit* by collecting feedback from key stakeholders.

Jalali and Kaiser raised limitations related to the Ensuring compliance noting that the compliance may not be enough because it does not guarantee security and that

healthcare organizations should aim higher in cybersecurity than the current regulations and policies that often tend to note data privacy but not information security. They also made notes about problems Maintaining cultural fit, such as the following quote from their interview of healthcare cybersecurity professionals "To me, what that means is that the culture of the organization has to change. Processes are a very strong way of changing the security posture of the organization. It is not just changing the technology. It is about the vendors, the workflow you use for onboarding employees, for moving data around the organization. That is all awareness and training. It's a real cultural thing that your org has to see security through.". (Jalali & Kaiser, 2018).

Yet, the study from Jalali and Kaiser (2018) reported friction in the cybersecurity management if the IT and the information security resources were separated and concluded that the most effective ways for individual hospitals to improve cybersecurity capabilities includes that chief information officers and chief information security officers should reduce the end point complexity and improve internal stakeholder alignment. In terms of a nation's critical infrastructure, they warned that only a few low resourced hospitals can threaten the whole healthcare infrastructure.

In addition to the low number of studies concentrating on *Balancing information security and business needs,* a lack of studies was noted related to the patients and their safety. From the 25 studies included in the synthesis, only in one study the research was focused on the patient's perceived security in healthcare where Peikari et al. (2018) who by studying the relationship of the organizational and human factors concluded that technical and physical protection, staff training and monitoring can have a positive impact on patient trust and the perceived security in hospital.

3.10 Cross comparison of socio-technical approach objectives and ISO / IEC 27001 domains

As mentioned, the ISO / IEC 27001 standard for information security management includes 14 different domains. By identifying the use of these domains in the studies it was possible to calculate how many times a domain has been included in the synthesis. These numbers are shown under a sector named "Total" in Table 5. Furthermore, when combining the objectives of socio-technical approaches used in the studies and the ISO / IEC 27001 domains included, the outcome of cross comparison of both frameworks produced data that could be used to analyze what domains have been or have not been studied with the research focus.

Table 5. Cross comparison of socio-technical approach objectives and ISO / IEC 27001 domains

Domain	Ensuring compliance	Maintaining cultural fit	Balancing Information Security and business needs	Total, n (%)
Information security policies	11	4	3	18 (72)
Organization of information security	7	1	2	10 (40)
Human resource security	9	6	4	19 (76)
Asset management	6	1	2	8 (32)
Access control	8	2	1	11 (44)
Cryptography	5	1	0	6 (24)
Physical and environmental security	5	0	2	7 (28)
Operations security	3	0	1	4 (16)
Communications security	7	0	1	8 (32)
System acquisition, development, and maintenance	5	0	2	7 (28)
Supplier relationships	2	1	0	3 (12)
Information security incident management	6	1	3	10 (40)
Information security aspects of business continuity management	6	2	3	11 (44)
Compliance	14	4	3	21 (84)

As seen in Table 5, the three most referred domains in the 25 studies were *Information security policies* with 18 studies (72%), *Human resource security* with 19 studies (76%). and *Compliance* with 21 studies (84%). The high number for *Compliance* is in line with the high number of studies concentrating on *Ensuring compliance* that according to this study often included *Information security policies* with 11 studies (44%) and *Human resource security* with 9 studies (36%). This result signals besides the *Ensuring compliance* has been seen valuable to study, that the *Information security policies* and *Human resource security* are often linked to the *Ensuring compliance*. These three domains were also among the most referred domains in studies categorized as *Maintaining cultural fit* or *Balancing information security and business needs,* and therefore seen as important to study in healthcare cybersecurity management.

The three least referred domains identified in the studies were *Cryptography* with six studies (24%)*, Operations security* with four studies (16%)*,* and *Suppliers relationships* with three studies (12%). There can be several reasons for not

including these domains. These domains may have not been seen as valuable to study, as they have been difficult to study or there may have not been information enough to support the use of these aspects, for example.

When considering the research focus and the included domains it was possible identify uncovered areas in the previous research literature. In studies with *Maintaining cultural fit* as the research focus, the use of the following domains was not identified: *Asset management*, *Physical and environmental security*, *Operations security*, *Communications security* or *System acquisition, development, and maintenance*. Again, in studies with *Balancing information security and business needs* as research focus domains, *Cryptography* or *Supplier relationships* were not identified. These results provide information about gaps in the knowledge concerning previous literature related to cybersecurity management in healthcare.

3.11 Research contribution

Table 6 lists the main findings on this investigation.

Table 6. Main findings on literature regarding cybersecurity management in healthcare

Number	Finding
1	The current research was concerned with *Ensuring compliance* with national and international standards and legislation rather than *Maintaining cultural fit* or *Balancing information security and business needs*
2	*Balancing information security and business needs* was the least studied research focus
3	Several gaps of knowledge were identified

This review analyzed the previous literature of cybersecurity management in healthcare. According to the results, cybersecurity management in healthcare is an emerging topic, and considering the importance of cybersecurity for modern healthcare, the number of studies published per year is likely to grow in the future as well. Yet, there are several shortcomings related to previous literature.

Overall, the current research is concerned with *Ensuring compliance* with national and international standards and legislation rather than *Maintaining cultural fit* or *Balancing information security and business needs* which is the least studied research focus in the healthcare sector and has only been studied during the past few years. In addition to using *Ensuring compliance* as the research focus, the studies often covered I*nformation security policies* and *Human resource security*

whereas domains such as *Supplier relationships*, C*ryptography* or O*perations security* were the least studied domains of cybersecurity management.

Favoring the *Ensuring compliance* as the research focus can be reasoned because it can provide an easy approach to the subject to be investigated by offering a checklist type form. This form can be then used to check if a subject meets the requirement mentioned in a standard or legislation. *Ensuring compliance* can also offer an easier way to conduct research than studying *Maintaining cultural fit* or *Balancing information security and business needs*. This can also apply to certain domains of cybersecurity management that have been used more often than others. Nevertheless, it can be questioned how comprehensive these requirements in standards and legislation are and what remains outside of their scope. By using *Ensuring compliance* as the research focus, the researcher can be locked to see only what is in the standard. If the research focus will be on the *Ensuring compliance* also in the future, the studies may continue to repeat themselves rather than going deeper into the subject and providing new information. The uncovered areas found in the previous literature may include domains that are more demanding to study; however, until these gaps are covered, there is no information about the current situation related to them at all.

Previous studies have provided different aspects to the subject, but until now, no holistic view of the existing literature related to the cybersecurity management in healthcare has existed. By systematically reviewing the existing research literature this study contributed new information about how the subject has been studied and what areas of cybersecurity management have or have not been covered by these publications.

In addition, this study introduced a cross comparison of objectives of the socio-technical approach and domains of ISO / IEC 27001 standard. This cross comparison was used to identify and to provide quantitative data about the areas covered in total and per research focus in the existing literature. This framework can be used in studying covered and uncovered areas of cybersecurity management in other sectors in the future as well.

Future research is needed, and the gaps found in the research literature should be addressed. The following avenues of future research are proposed to improve the knowledge on cybersecurity management in healthcare sector. Firstly, future research should be concerned with *Maintaining cultural fit* as a research focus and including any of the following cybersecurity management domains: *Physical and environmental security*, *Operations security*, *Communications security*, *System acquisition, development, and maintenance*. According to the results, there is no study of this kind, and it could provide new information about how the

organizational policies and guidelines are aligned with the organizational values and culture related to the domains of cybersecurity management.

Secondly, empirical data about how cultural fit is maintained in private healthcare organizations should be gathered, because no such data was available about any of the cybersecurity management domains listed in the ISO / IEC 27001:2013 standard. This data could provide useful information about the private healthcare sector and by comparing it to the data gathered from the public healthcare sector, it could show how the cultural fit is maintained between the two. Hospitals operating in other types of sectors such as charity or military could also provide interesting information to be compared.

Alternately, there is a need for future research focusing on *Balancing information security and business needs* to provide more information about the balance between the two vectors that both are important for the operation of a society, healthcare sector, organizations, employees and patients. Finally, this study suggests that future research should be concerned with the link between cybersecurity and patient safety. According to this study there is only limited information available on the connection between cybersecurity management and patient safety.

3.12 Limitations

In this review there are limitations to be noted. Firstly, the selected search engines had a limited coverage of research publications and the identification state search provided a wide number of publications to be screened from the databases, many other search engines and databases were not used. Secondly, the used search string may not have captured all relevant publications. In addition, the used evaluation criteria such as including articles written in English only, it is possible that not all relevant studies were found. The combination of the socio-technical approach and ISO / IEC 27001 domains introduced in this review offered a new and interesting view to review and analyze the existing literature. Yet, this is only one way to seek new information from literature and dependent on the chosen frameworks.

4 CYBERSECURITY AWARENESS IN HEALTHCARE

4.1 Cybersecurity awareness and Finnish health and social services reform

Health and social services reform has been a hot topic in Finland for years. An aging population and high prices of services have challenged the current system and its funding. Nonetheless, the reform that would improve the health and social services has been planned by several different governments for over ten years. The objectives and needs for the reform have aimed to narrow differences in the services and to ensure high-quality health and social services for citizens of Finland also in the future. In addition, another goal for the reform has been to improve safety. (Finnish institute for health and welfare, 2022). Cybersecurity in healthcare is known to be linked to patient safety (Kisekka & Giboney, 2018).

It has been stated that the easiest, fastest, and cheapest way to improve the cybersecurity level in an organization is to improve the basics, such as cybersecurity awareness (Lehto & Limnéll, 2017). Additionally, the only way to defend against both known and unknown cyber threats is by keeping the cybersecurity updated, improving the overall cybersecurity awareness and resilience with reactive practices (Limnéll et al., 2014), because education and awareness are equally important security measures compared to technology, policy, and practices (McCumber, 2005). Cybersecurity in healthcare is also seen as one of the key sectors for society's operation in Finland's cyber strategy for 2017 – 2020 (The Security Committee, 2018), and according to European Commission, improving cybersecurity awareness is seen as important for the operation of healthcare (European Commission, 2017).

However, even today, not all employees have attended cybersecurity lessons or training. In fact, organizations may not have even organized training or education for their employees to improve the overall cybersecurity awareness and create a cybersecurity culture (ESET, 2017). Insufficiency and lack of staff training, as well as the difficulty in getting dedicated information security staff, are mentioned in many reports and papers when talking about the biggest problems regarding the cybersecurity level and preparedness in organizations combating cyber threats (Hoffman et al., 2012; Independent security evaluators, 2017; KPMG, 2018; Trendmicro, 2017a; White et al., 2017;).

The management of risks related to personnel is called personnel security, and it can be improved and maintained with systematic education, proper management, risk analyses, defining responsibilities, and creating a safety culture, for example

(Ministry of Finance, 2008). The legislation concerning personnel security has been included in several different injunctions in Finland (Ministry of Finance, (2009).

4.2 VAHTI information security barometers

The Government Information Security Management Board of Finland (VAHTI) has conducted two information security barometers for the personnel and management in 2016 and 2017. These barometers were targeted at public administration organizations and personnel in Finland focusing on the importance and challenges in taking cybersecurity into practice.

The key observations from both barometers included positive findings such as: Cybersecurity is seen as an important and necessary enabler to the work. The cybersecurity level in the organizations is seen as high and the respondents feel safe when using digital systems. As a result, both barometers suggest that personnel should be educated and trained regularly about cybersecurity and topical threats related to it (Rousku & Kuivalainen, 2016; Rousku & Mellin, 2017).

Even if the barometers had positive results, they provided only a limited view to the healthcare sector because only few healthcare organizations participated in the barometers. The first barometer included only a few respondents from the healthcare sector (Rousku & Kuivalainen, 2016) however, the second barometer received answers from 791 respondents working in three different hospital districts in Finland (Rousku & Mellin, 2017). Yet, according to the number of hospital districts in the country (EU-healthcare, 2021), most of the healthcare hospital districts did not participate in the survey.

Based on the needs of the national health and social services reform and the limitations of the previous VAHTI information security barometers, a more detailed view of the current cybersecurity awareness level in healthcare organizations was needed. To answer these needs and to study how to improve cybersecurity awareness in healthcare organizations, the following research question was used: How to improve cybersecurity in healthcare with developing cybersecurity awareness?

4.3 Conducting cybersecurity awareness surveys

The data was gathered via three different surveys that included both qualitative and quantitative questions related to cybersecurity. The first two surveys were

conducted via paper forms to the employees of a Hospital District participating in cybersecurity lectures, and the last survey was an online survey to organizations operating in the health and social sector in the region.

The first survey form included questions concentrating on finding answers to questions about how the respondent felt about the importance of the cybersecurity and the attractiveness, instructiveness, and usefulness of the lecture. In addition, the lecturer's expertise and presentation material was asked to be rated and open feedback to be written.

In the second survey form, the respondent was first told to give open feedback about the lecture and then to rate their personal and the cybersecurity level of the organization on a scale from four to ten. Lastly, the respondents were asked to answer to open question about the kind of cybersecurity risks they have seen in their work and how they would improve the cybersecurity level in the organization.

The online survey had seven demographic questions and twenty-four questions related to cybersecurity such as use cases from everyday information security practices to questions characterizing the respondent's knowledge and feelings about the topic using the Likert scaling. Before sending the answers, the respondents were asked to give open feedback about the online survey.

Before the third survey was published, a test group of ten persons tested the survey to gather feedback. This feedback was essential to ensure the proper operation of the online survey and was used to improve the survey's functions, instructions, questions, and to find out the average duration the survey will take.

These three surveys were answered by 1,229 respondents in total. The first survey was answered by 153 respondents, the second by 195 respondents and the third survey by 881 respondents. The population targeted with the surveys varied. Whereas in the first two surveys the population covered employees in one organization, the population in the third survey covered several organizations and their employees. The total response rate in the first two surveys was 10,2 % and 8,5 % in survey number three. The response rates were higher than expected when considering the subject can be new to many but support the results that showed how employees working in healthcare can be interested in cybersecurity. Table 7 describes the response rate on these three surveys.

Table 7. Cybersecurity awareness survey response rates

Survey	Population	Respondents	Response rate
1 & 2	3418	348	10,2 %
3	10400	881	8,5 %

After gathering the data from all three surveys, the results were analyzed using data-driven content analysis. The answers from the first two surveys were digitalized for an analysis with the online survey answers. Data-driven content analysis was chosen because it can be used especially to form interpretations from the content and to increase the value of the gathered information (Hsieh & Shannon, 2005). In practice, the data from the surveys was coded into code categories and then quantified and analyzed to produce information on themes aroused from the first two surveys and relationships such as rates between two groups; respondents who had participated on cybersecurity training or lecture, and respondents who had not participated in these kind of events. Lastly, the results from these surveys were compared to the results from the VAHTI-barometers.

4.4 Results from the first two surveys

Themes arising from the written feedback included importance of the topic and education of the users. The participants felt the lecture was interesting and necessary as well, even if the subject or parts of it were mentioned to be familiar to the participant. Especially reminders about and discussions on cybersecurity were answered to be thought-provoking and necessary. When asked if the participants had learned something about the subject during the lecture, the average instructiveness was graded nearly excellent. Even though the participant rated the instructiveness as low, the average results showed that the participants did not feel the lecture was a waste of their working time and that there is an actual need, as well as a benefit from educating users with these type of lectures.

Both the level of knowledge of participants and organization were rated to be high; in fact, higher than the feedback from the lectures could reveal. If the participants had had a good knowledge about the subject, the basics should have been familiar to them and not rated as educative. Nevertheless, participating in a cybersecurity lecture for the first time can have an effect where the participant realizes that he or she in fact has knowledge about the subject but has not used it. A similar analysis can be conducted from the written feedback that bringing up the subject among the participants was seen as important.

According to the average grade, the participants' own cybersecurity knowledge was graded somewhat lower than the organization's level. Whether this is the reality or not, the organization's higher level can be due to the lecture and the information the lecturer had shared recently. Yet, rating the organization's cybersecurity level

higher than one's own personal level indicates that the participants value and trust the actions taken towards cybersecurity.

A particular individual written comment from a person working at management level caught the writer's attention with "Those who needed the lecture most did not come and participate in it". As mentioned, attendance at these lectures was voluntary; the participants were invited, and the lectures were not compulsory. Nevertheless, the head of the department may have asked all employees available to take part in the lecture to ensure that as many as possible would participate; however, many departments remained non-visited. The comment: however, refers to that there are employees whose cybersecurity awareness should be improved more than that of some others. This can signify that their level of awareness is known to be low or that their behavior is known to be against best practices discussed during the lecture or it could even be wrong.

When asked what kind of security risks one confronts in one's work regarding cybersecurity, the answers included receiving spam emails and leaving computers unlocked. Some of the users were concerned about physical issues such as unlocked doors, USB drives and too easy physical access to the organization's digital equipment. When finding similarities among the answers, they were often related to user irresponsibility. Even indifference was mentioned as a faced security risk in the workplace; however, the majority of the answers pointed more to things being unintentional rather than intentional.

The last question in survey two was "How would you improve cybersecurity in the organization". Many improvement proposals received included topics discussed during the lecture such as using privacy filters that can be installed on the screens restricting the viewing angle, so only the user sitting directly behind the screen can see the screen's content. Physical safety issues and improvement to the physical environment were proposed. Other proposals mentioned varied from proper use of confidential papers to secure use of digital credentials and identity cards. Yet, the most common improvement proposals were related to training and educating, and that users should be educated with similar lectures.

The notes and proposals from survey one and two show that users have made observations about their physical and digital environment related to cybersecurity. According to the answers, there are employees who are able to scrutinize the behavior of their own and colleagues, as well as the physical and digital infrastructure. Therefore, it can be said they are at least somewhat aware of cybersecurity and issues related to it. Next, the results from the online survey are examined to obtain better confirmation for this analyzation.

4.5 Results from the third survey

According to the results of the online survey, most of the respondents have not participated in any training or lectures related to the subject, with the average percentage of those that have not participated being 56 per cent as seen in Figure 8. Additionally, a total of 38 % of the respondents informed they have not read the organization's information security instructions.

When the results are compared between organizations with over twenty respondents, there were two organizations where clearly over a half of the respondents had participated in cybersecurity training or lecture. In other organizations, the percentages were half or below.

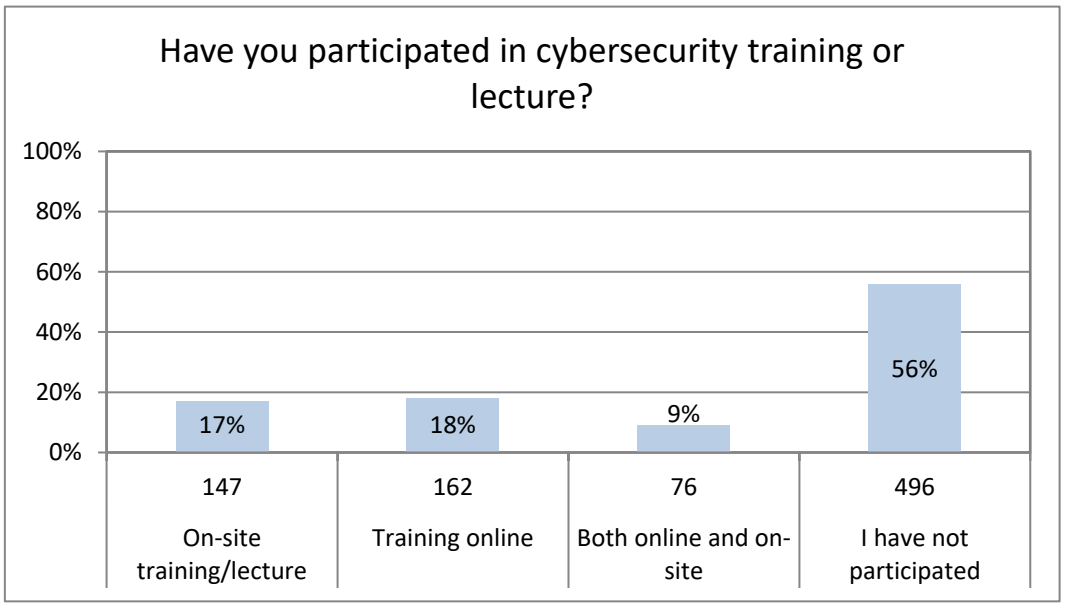

Figure 8. Percentage of participation in cybersecurity training or lecture

The amount of people that have participated in training or lecture on-site versus the number of those that have participated online was alike. These numbers indicate that cybersecurity awareness is not trained in the organizations, or the training is not compulsory. When analyzing people who have not participated in any cybersecurity training, the answers to the demographic questions are similar to all respondents, which can mean that the participation is not directly dependent on the demographic factors.

When compared to the results of the two information security barometers conducted by The Government Information Security Management Board of Finland (VAHTI), the respondents of survey three have had less cybersecurity training and education. There can be regional differences; however, the difference

is highest when comparing the results to the VAHTI barometer's governmental sector, and it is notable compared to the municipal sector as well. These differences include a signal from a lower cybersecurity culture in the target organizations. The Cybersecurity awareness may not have been included in the organization's risk management at all, or it has been measured as a low-level risk. One reason for this can be the stronger usage of VAHTI instructions especially targeted at and used by the governmental sector.

Even though most of the respondents had not participated in any education regarding cybersecurity, only a few respondents answered that they do not need more information about the topic. This supports the results from previous surveys showing that the respondents have acknowledged they need more information about cybersecurity. According to the answers, the best way to get more information about cybersecurity was by participating onsite in a lecture or training, the least desired option was participating online.

The popularity of onsite training was higher than expected. It would have been less surprising to find that people want to participate in online education about things related to the internet and digital ecosystems; however, it is understandable when considering the excellent feedback received from the lectures.

The respondents who did not want more information about the subject were a clear minority. If compared to the majority who wanted more information about cybersecurity, they were often younger with a lower education and working elsewhere than at an IT department nor management sector. Similarly, to the others, most of these participants had not participated in any cybersecurity lectures or training. In fact, the participation percentage was even lower than with those who wanted more information. Yet, the respondents not wanting more information, rated their cybersecurity awareness at the same or higher level, when compared to the other respondents, and they estimated that they have more knowledge about cybersecurity for their jobs than others. The respondents who did not want more information about cybersecurity felt the subject less important and the need for education on it less valuable. Alarmingly, they had not read the organization's information security instructions more than other respondents.

The motives for not wanting more information about cybersecurity can be the same as mentioned earlier when discussing why people might not want to participate in a cybersecurity lecture or training. The online survey results support mostly the motive to be a feeling that a respondent thinks he or she has enough knowledge about the subject already. This could be a good thing if the knowledge were good also in reality.

When comparing answers from respondents who did not want more information about cybersecurity to respondents who had participated in cybersecurity lessons or training, the results are indicating that the first group can be thinking that they have enough knowledge about the subject but in reality they do not. What should be noted is that these respondents should be more familiar with their organization's security instructions, now only half of the respondents not wanting more information about cybersecurity had actually read the instructions. Another supported motive is that they have not found the subject as important and that there is no reason to know more about it.

When considering the young age and lower education of these respondents, their knowledge could still be improved in the future. They may have a better overall knowledge about the subject but there are no signs that they do not need participation in cybersecurity lessons or training like other employees. Cybersecurity awareness could especially be improved in the organization and among personnel, relating to their job, if employees participated and the meaning and importance of the subject could be increased.

As seen in Figure 9 the overall knowledge was better among employees who had participated in cybersecurity training, or a lecture compared to employees who had not participated. The difference is not significant; however, it is visible and repeated in every question throughout the survey, and it can be seen as well in the answers from the management.

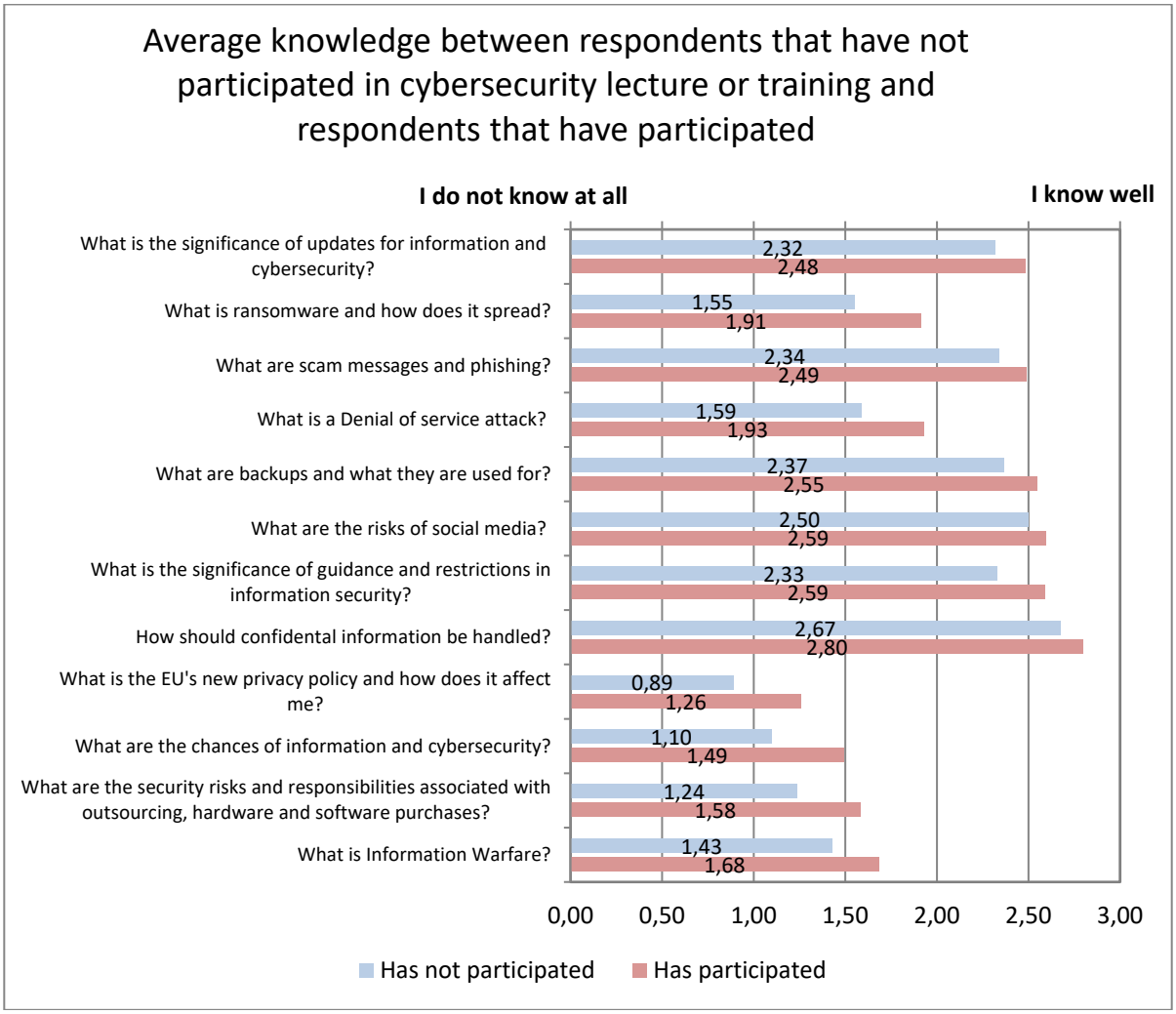

Figure 9. Level of knowledge about cybersecurity related topics estimated by all participants

The difference could be due to the better overall knowledge about the topic among respondents who have participated and who would be more likely to answer the survey about a topic they are interested in already. Still, because the difference is repeated through the survey with a high number of respondents, it is assumable that the respondents could learn and improve their cybersecurity awareness by participating as well, even if they are not keen on the topic. The presentation approach of the lecturer that raises the interest level of the topic making it easy to understand, can have affected the positive results.

One of the most alarming findings from the results was the low rate of Cyber Resilience, "the ability to continuously deliver the intended outcome despite adverse cyber events" as defined by Björck et al. (2015). According to the answers seen in Figure 10, it is not clear for the respondents what to do if something

unexpected happens in the cyber environment. Most of the respondents have not been instructed on what to do with cybersecurity incidents, for example, if their computer has been infected with malicious software, or a critical system for their work is not available. This does not only concern workstations but medical devices as well, that can be insecure and include serious risks for the operation and patient safety (Alemzadeh et al., 2013).

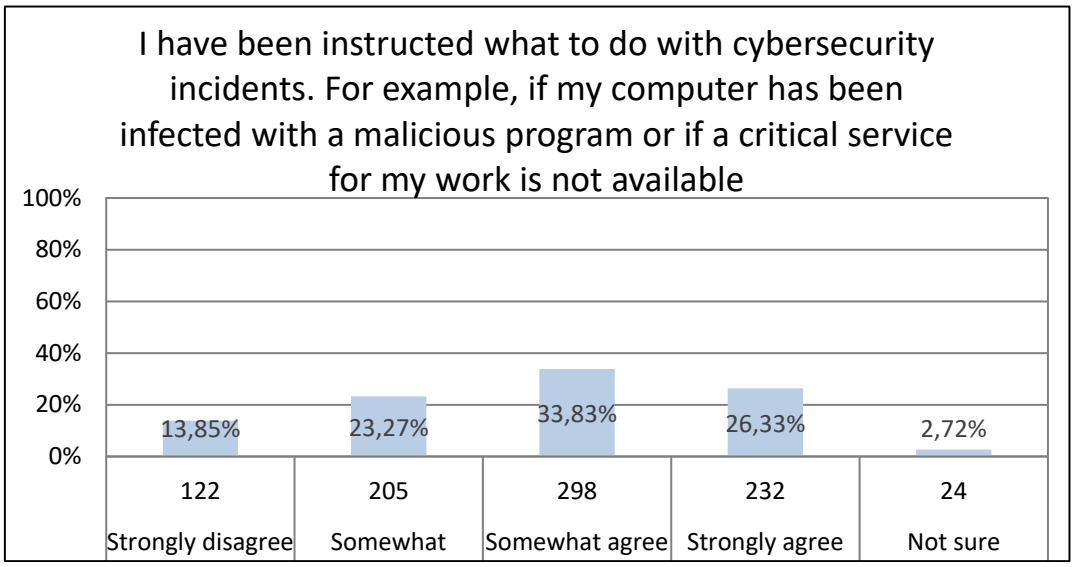

Figure 10. Work related cyber resilience

In such a case, most of the respondents know where to ask or get more information about cybersecurity. Although, management might not help because most of them have answered that they do not have enough knowledge to give guidance to their subordinates in information and cybersecurity issues related to their jobs. Furthermore, persons with subordinates have answered that they do not think their subordinates have enough knowledge about information and cybersecurity for their jobs.

If the employee does not know what to do in a case of an adverse cyber event that can be intentional or unintentional, and happen at any time, the operational risks can be high. In the case of an adverse cybersecurity event, an uninstructed person may stagnate or cause more trouble by wrong actions. Especially in critical infrastructure, the consequences from this kind of risk can be serious and should be therefore carefully analyzed by risk management to ensure the continuity and vital operations such as patient safety. Additionally, uninstructed personnel may not know how to report these kinds of incidents properly and report them with insufficient details or, in the worst case, he or she may not report them at all.

However, these answers included the largest difference when comparing the participated and non-participated respondents. This means that by participating in cybersecurity lecture or training, the knowledge and confidence are improved. This analysis is supported by the answers to the question "I have sufficient knowledge about information and cybersecurity for my job" where respondents who had participated also had better felt knowledge. Yet, as shown in the Figure 11, many felt that they do not have sufficient knowledge about cybersecurity for their job.

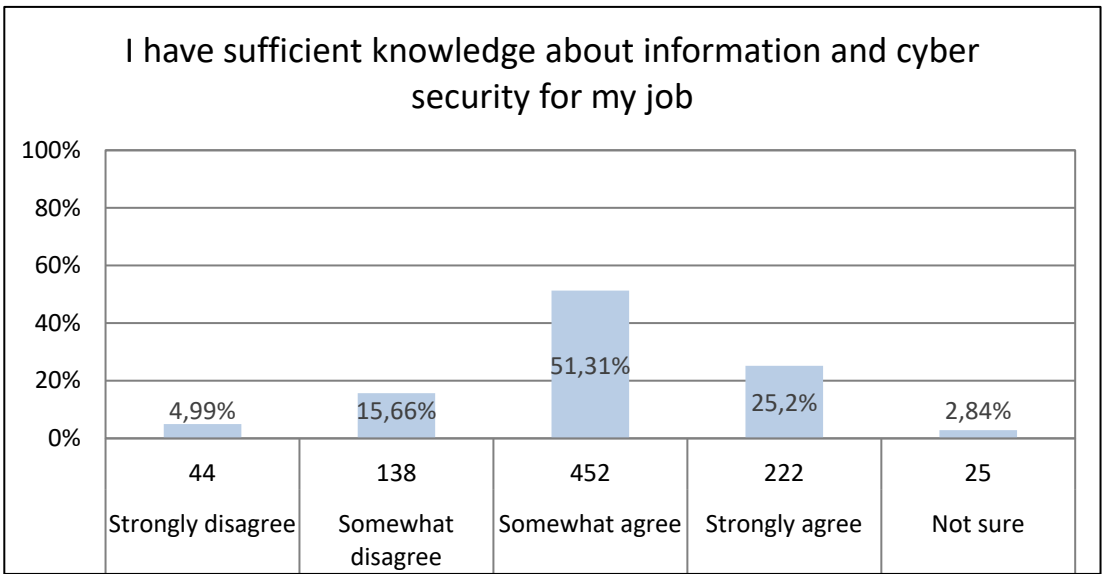

Figure 11. Sufficient knowledge for one's job

Overall, the knowledge about topical threats and issues regarding cybersecurity varied depending on the subject. The significance of updates, guidance and restrictions for information and cybersecurity was well known to the respondents, as well as fraud messages, phishing, risks of social media and backups.

Explicitly the highest rated knowledge level, according to the answers, was about how confidential information should be handled. Confidentiality and data protection are subjects that have been taken care of for years in the healthcare sector before modern digital systems have formed a point of reference for a somewhat newer cybersecurity awareness. If similar resources and attention were spent on cybersecurity awareness, an improved level of awareness would be presumably achieved.

Less-known topics included ransomware, denial-of-service attack, GDPR and its effect on the personal level, security risks and responsibilities associated with outsourcing, purchases and information warfare. In addition, most of the

respondents were not familiar with the changes relating to information security and cybersecurity.

Some of the less-known topics can be hard to understand or totally unknown for persons not interested in technology or cybersecurity. However, respondents who had participated in a cybersecurity lecture or training had a better than average knowledge and awareness about these subjects. The respondents who had participated in a cybersecurity lecture or training can be more technically oriented or interested in cybersecurity related subjects, and therefore be more likely to participate or have better existing knowledge.

Even the average respondent could be less oriented in technology than others. According to the results, most of the respondents are willing to participate in cybersecurity lectures and training to get more information and to improve their cybersecurity awareness. If a person is willing to participate in this kind of event, it is likely that he or she is able to learn as well.

4.6 Research contribution

Table 8 lists the main findings in this investigation.

Table 8. Main findings on cybersecurity awareness

Number	Finding
1	Employees had not participated in cybersecurity education or training
2	Employees were not instructed about what to do in case of a cybersecurity incident.
3	Employees had not read the organization's cybersecurity instructions.
4	The level of cybersecurity education was low in all target organizations and among the personnel and the management
5	The level of cybersecurity education was lower compared to the VAHTI barometers

The objective of this investigation was to find an answer to the question: How to improve cybersecurity in healthcare with developing cybersecurity awareness? According to the results, the level of cybersecurity education was low in all target organizations. To improve cybersecurity, organizations should pay attention to cybersecurity awareness and ensure that they have cybersecurity education available for all employees. Because the key responsibility in cybersecurity resides with the management (Blanke & McGrady, 2016) improving cybersecurity awareness should be started from the management level.

In the long run, healthcare organizations should create a cybersecurity awareness program or implement cybersecurity education in their existing education programs. Adding a mandatory cybersecurity education such as a lecture and an online course to the organization's induction process would guarantee that all new

employees will get an opportunity to participate in cybersecurity education. It should be mandatory to participate in cybersecurity education at regular intervals or if required by the changes in legislation or environment, for example. This will make certain that all employees from new to existing will participate in the education and get updated information in case of major changes. The participation in cybersecurity education must be documented and revisable if needed. In small organizations organizing and supervising the education could be managed using paper and pen. In larger organizations an information system for orientation and or induction purposes should be used to facilitate these needs and to provide data and statistics for all relevant parties from authorities to top level management and from cybersecurity professionals to healthcare workers.

The level of cybersecurity education was low among the personnel, as well as among the management. Over half of the participants had not participated in any cybersecurity related education, even if they answered that they are willing to improve their knowledge about the subject. When comparing the results to the two barometers conducted by VAHTI, even the topic was seen as important and necessary in all surveys and the cybersecurity level felt to be high, and the level of education was lower in many of the target organizations than in the organizations participated on the VAHTI barometers.

To improve the situation, a stronger use of national instructions for cybersecurity in organizations participated in survey three as well as in the whole public health care sector in Finland should be considered because the amount of education lacks behind the level in municipal and governmental sectors. This finding and the conflict between the results from the VAHTI barometers and this study should be considered when forming a national situational picture on cybersecurity awareness.

In addition, the surveys concentrated on giving the respondents an occasion to rate their personal knowledge about subjects related to cybersecurity. The questions included topics from work and free time, which both should be seen as important for the cybersecurity of the organization. If one knows how they should act in a secure way in the digital world during his or her free time, he or she is probably able to manage it at work as well, and vice versa. Real-life examples from off-work can be easier to understand and awaken the interest in cybersecurity. Therefore, the organization as well as the whole nation could benefit from increasing overall cybersecurity awareness including off-work cybersecurity more than just concentrating on the organization's own systems and use cases.

According to the answers, the best way to get more information about cybersecurity for the respondent is via onsite training and lectures. Onsite lectures

and training can pose a better change for the participants to ask questions about cybersecurity and discuss the subject, especially about things that the participant finds difficult to understand, or is even frightened about, than during online training. An improved understanding can also relieve any negative feelings and lead to a better security level where feelings always play a big role. On the other hand, online training can be more interactive and produce data that can be used in measuring, for example the educational objectives. Nevertheless, individuals have different ways to learn, and for this reason, multiple learning methods should be used.

As a conclusion, cybersecurity awareness has not been adequately taken care of and should be improved in all target organizations. Because awareness is a vital part of cybersecurity, cybersecurity management should be revised in the organizations. It can be questioned if the current level of cybersecurity awareness and education comply with laws and regulations for personnel security. The lack of cybersecurity awareness is signaling that the organizations did not have cybersecurity resources enough for cybersecurity management and to organize and oversee cybersecurity awareness. In other words, cybersecurity management is lacking, and healthcare organizations need more resources for cybersecurity management.

4.7 Limitations

In this investigation, three surveys on cybersecurity awareness were conducted, the results were analyzed by using data-driven content analysis and compared to the results of VAHTI-barometers. The limitation regarding the first two surveys was related to the respondents who were all participating in a cybersecurity lecture. Even though employees from several different departments participated in the lectures and answered to the surveys they participated in voluntarily or by a request from the head of the department.

Especially the employees participating voluntarily could have had interest in cybersecurity and had more information about the subject beforehand, compared to the employees who did not voluntarily participate in the lecture. It is also possible that the heads of the departments may not have requested that all employees from their department participate in the lectures or that those who are interested in the subject should participate. As mentioned, one management level respondent wrote: “Those who needed the lecture most did not come and participate in it”. Therefore, the surveys may have had more respondents who were already interested in cybersecurity whereas employees not interested about the

subject or improving their own cybersecurity knowledge did not participate in the lecture nor the surveys. Before answering the first two surveys, the previous lecture on cybersecurity may have also affected the answers, for example giving an increased confidence in cybersecurity because the respondent participated in the lecture and learned more about the subject.

Comparing the results from this study to the results of VAHTI-barometers had limitations to be considered. The questions used in this study differed from the questions used in VAHTI barometers. Whereas VAHTI barometers were conducted as online surveys, this study contained two surveys conducted onsite and one conducted online. The number of participants from the healthcare sector in VAHTI barometers could have been higher to provide more reliable data to be compared with. In fact, there were more participants on the surveys conducted in this study than in the two national VAHTI barometers combined. However, the results from both VAHTI barometers and this study can be seen to supplement each other.

Another limitation regarding this investigation was related to the way how the information on cybersecurity awareness was gathered and estimated. The surveys did not concentrate on testing the cybersecurity abilities of respondents or knowhow in practice. In all surveys conducted, the respondents had an opportunity to give the answers based on his or her own opinion instead. Testing cybersecurity awareness in practice could have provided different results compared to the surveys.

This kind of cybersecurity testing was in fact suggested in the feedback of the surveys and could be a good next step to improve the overall level of cybersecurity awareness. With digital interactive tests, the employees could take the test when available by using computers or mobile devices. Gamification, for example, could make the tests more attractive and profitable as well. Test results from digital tests could provide interesting data that can be analyzed and used to improve cybersecurity in healthcare organizations. In addition, this data could be used for future research purposes.

5 MANAGEMENT OF INFORMATION SECURITY POLICIES IN HEALTHCARE - LITERATURE REVIEW

Information security policy (ISP) is one of the most important information security controls for an organization (Höne et al., 2002). The need for the ISP has been noted by researchers (Doherty & Fulford, 2006; Höne et al., 2002), CSF (NIST 2018), and globally recognized standards such as ISO 27001, that requires the top management establish an ISP for the organization (ISO, 2020). As defined by Whitman et al. (2001) organizations should create ISPs to provide guidelines for their employees concerning information security that support the organizational goals.

There have been numerous studies related to the ISPs during past decades. These studies have been highlighting, for example the importance of information security policies, studying information security compliance, and compliance behavior (Bulgurcu et al., 2010), or studying how to design an effective information security policy (Paananen et al., 2019). Lack of ISPs in organizations have also been noted (Paananen et al., 2019).

Still, only a few studies have been conducted analyzing ISPs in the healthcare sector. Previous studies have had limitations regarding the ISP material that has been obtained from one single organization (Hedström et al., 2013) or based on the same organizational ISP template (Stahl et al., 2013). After a systematic search it was found that a literature review on ISPs in healthcare has been missing and an overview of the topic has been lacking. Additionally, it has been unclear what phases of ISP management have been studied by the previous literature and what phases might still be understudied. Considering these gaps of knowledge and the fact that the healthcare sector is part of the critical infrastructure (CISA, 2021) and its operation is dependent on information security, a literature review on ISPs in healthcare was needed.

To fill these gaps of knowledge, a systematic literature review was conducted and covered phases of ISP management were studied. The research question used was: How information security policies in healthcare have been studied by the previous literature? How have information security policies in healthcare been studied by the previous literature?

5.1 Study eligibility criteria

A systematic literature review was conducted to synthetize the previous literature related to ISPs in healthcare. The literature review followed the Preferred

Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach (Moher et al., 2009). Relevant literature was searched from three scientific databases and search engines: Pubmed, Scopus and Web of Science, with the following search string:

"security policy" AND (computer OR information OR data OR cyber) AND (health* OR hospital)

To cover as many ISP related articles in the healthcare sector as possible, the used search string included words such as *computer*, *data* and *cyber* that all may have been used when referring to a security policy concerning information security. In addition, the search terms *health** and *hospital* were used to focus on the healthcare sector and to include also articles related to hospital policies.

5.2 Data evaluation

Studies from the original searches were included if they met all the following inclusion criteria:

- Journal article.
- Published between 2010 – 2020.
- Published in English.
- Abstract available.

Papers that did not meet the evaluation criteria were excluded. The literature search provided 219 papers total. After screening all studies, 152 papers were excluded because of duplicates, inappropriate topic or because there were no abstract available. Inappropriate topics included articles that focused for example on food security policies or ISPs outside the healthcare sector.

Next, the remaining 67 articles were retained to be examined in detail. From these articles 25 studies were found relevant and included in the synthesis. The excluded papers included articles that were too technical and narrow such as security policies for a certain device, system or application, focused on access control policies or where the healthcare sector was only a part of the research focus. The selection process is presented in Figure 12.

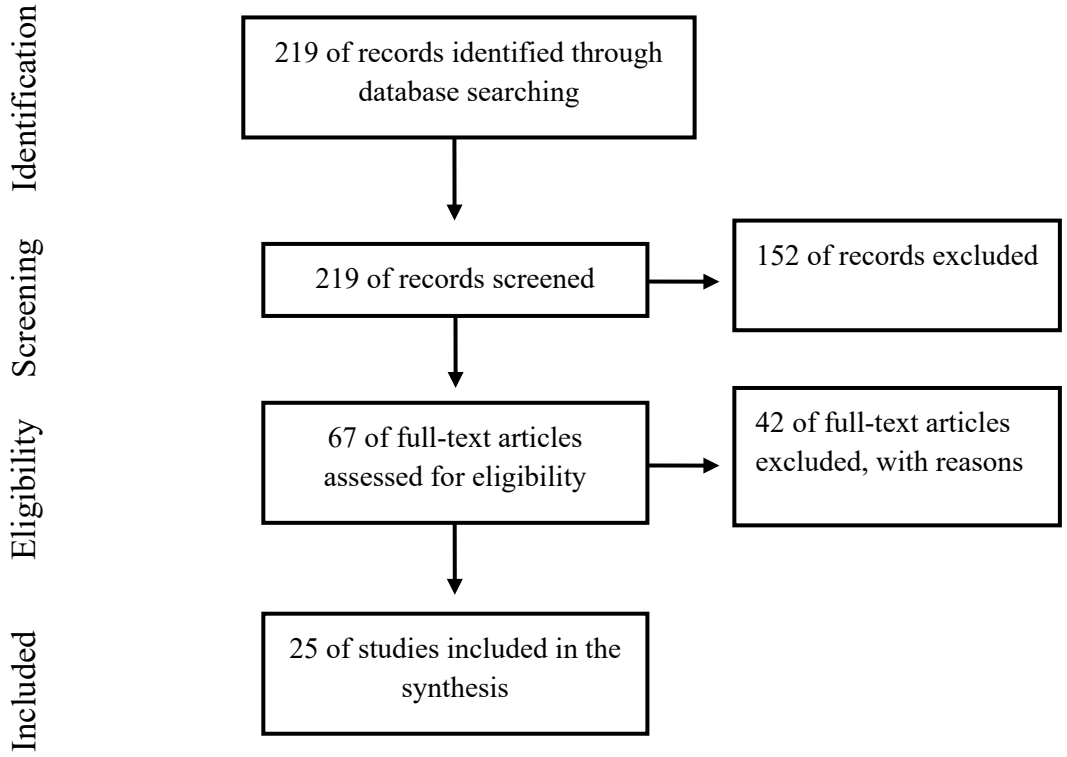

Figure 12. Management of ISPs in healthcare PRISMA flow diagram

5.3 Organizational-level process model for ISP management

Knapp et al. (2012) have developed an organizational-level process model for ISP management by dividing the ISP management process into nine phases. Together these phases form a continuous cycle starting from *Risk Assessment* and *Policy Development* and ending to *Policy Review* and *Policy Retirement*. If followed on a frequent basis, the model offers a repeatable process with cyclical nature for ISP management in organizations. The model includes the following phases:

1. Risk Assessment
2. Policy Development
3. Policy Approval
4. Policy Awareness & Training
5. Policy Implementation
6. Monitoring (Audits & Automated Tools)
7. Policy Enforcement
8. Policy Review
9. Policy Retirement

In this study the organizational-level process model for ISP management was used to identify the phases of ISP management that were included in the research focus of the eligible studies. This information was then used to provide information about the studied and not studied areas of ISP management. Even though there are several different process models available for ISP management, the model developed by Knapp et al. is one of the most advanced and takes into account the whole life cycle of the ISP development (Paananen et al., 2019). Therefore, using the organizational-level process model was seen to ensure that all phases of ISP management will be identified from the eligible studies.

5.4 Literature overview

According to the results, the topic is not emerging and only a few papers related to the topic were published annually between 2010 and 2020. This is an interesting result when considering the increasing dependency that healthcare has on information security and that cyberattacks are known targeting the healthcare sector (Ghafur et al., 2019; Jalali & Kaiser, 2018; Jalali et al., 2020).

The 25 articles included in the synthesis were published in 24 different journals and the only journal with more than one article in the synthesis was *Information Management & Computer Security* (Hedström et al., 2013; Renaud & Goucher, 2012). Two different scientific disciplines were identified from the journal themes that have been interested in publishing articles related to the topic. The first discipline included Natural Sciences and Computer sciences and IS security themed journals such as *Journal of Information Systems* and *Computers & Security* (Hedström et al., 2013; Karlsson et al., 2017; Renaud & Goucher, 2012). The second discipline included Medical and Health Science themed publications such as *Medical Care, Health Information Management Journal* and *International Journal of Healthcare Management* (Humaidi & Balakrishnan, 2018; Kim et al., 2013; Samhan, 2020). These two themes show that the topic is between the two scientific disciplines and also considered by both disciplines.

The studies were conducted in several different countries. Three papers originated from the USA, three papers from the UK, three papers from Sweden and two from Malaysia, whereas the rest of the papers were conducted in a different country each. All the papers were conducted in a single country, meaning that there might be a lack of cross-country comparisons.

A total of 18 of the papers (90 %) were empirical studies with empirically gathered data and two (10 %) studies were identified as conceptual. Ten (56 %) of the empirical studies were using surveys when gathering the research data and three

(17 %) papers reportedly used interviews, observations, and organizational documents. The rest of the studies used different combinations of the previously mentioned data collection methods.

Contrary to expectations, only two papers (10 %) used existing organizational ISP documents as research data (Hedström et al., 2013; Stahl et al., 2012). When taking into account the literature search that aimed to find ISP related studies in healthcare, this result was unexpected and suggests that even ISP related studies have been conducted in the healthcare sector the articles have not focused on the existing ISP documents implemented by healthcare organizations.

In 15 of the empirical studies (83 %) of the data was obtained from public healthcare organizations and in three studies (17 %) the data originated from both public and private organizations. In two studies (11 %) the type of healthcare organization was not clearly stated. None of the studies had reportedly gathered research data from private healthcare organizations only. Future studies should use private healthcare organizations as a source of empirical data to provide new information about these types of healthcare organizations. This information could be then used to compare private and public healthcare organizations, as well. There is also a lack of ISP related studies that have included other types of healthcare organizations such as military or charity healthcare.

When referring to standards and guidelines, eight of the studies (40 %) mentioned national policies and laws. The most referred to national policy was Health Insurance Portability and Accountability Act (HIPAA) which is a federal law set by the US congress in 1996, that includes requirements for privacy and security in healthcare (U.S. Department of Health & Human Services, 2017). HIPAA was mentioned in five studies (25 %), and it was the only national policy that was referred by studies conducted in foreign countries.

Other national policies or guidelines referred were local. International standards referred to were ISO / IEC standards such as the ISO 27000 series and ISO 17799. In total, ISO standards were referred to in six studies (30 %) and organizational guidelines in three studies (15 %).

5.5 ISP management phases included in the research focus

By using the framework developed by Knapp et al. (2021) the studies were analyzed to identify what phases of ISP management have been included in the research focus. In most of the studies, one phase was identified, meaning that this phase

was the only one included in the research focus. In two studies two different phases *Policy Development* and *Monitoring* were identified (Alexandrou & Chen, 2019; Said et al., 2017) and in one study three phases were identified (Hedström et al., 2013). The studies with more than one phase included had wider research focus than studies that concentrated only on one phase such as *Monitoring* user behavior regarding the ISP. Yet, it is arguable if the research focus was too broad with studies including several phases and should have been narrowed to include only one phase of ISP management.

The only study that included three phases of ISP management was the paper written by Hedström et al. (2013) who first analyzed the *Policy Development*, then conducted a *Monitoring* of the ISP and finally performed a *Policy Review*. For example, this study might have benefited from narrowing the topic or splitting the study into multiple articles.

The phases of ISP management and the number of studies including the phase are shown in Table 9. As can be seen from Table 9, the majority of the studies (60 %) focused on the *Monitoring* phase. These studies, for example, were *Monitoring* the ISP compliance by collecting empirical data from healthcare employees and then analyzing the employee compliance level and behavior (Alanazi et al., 2020; Alexandrou & Chen, 2019; Hedström et al., 2013; Humaidi & Balakrishnan, 2018; Kim et al., 2013; Renaud, 2012; Renaud & Goucher, 2012; Stahl et al., 2012; Samhan, 2020). The high number of studies focusing on this phase shows that previous literature has been interested on *Monitoring* ISPs.

Table 9. ISP management phases included in the studies

ISP Management Phase	Number of studies	Percentage of studies
1. Risk Assessment	0	0 %
2. Policy Development	7	35 %
3. Policy Approval	1	5 %
4. Policy Awareness & Training	2	10 %
5. Policy Implementation	0	0 %
6. Monitoring	12	60 %
7. Policy Enforcement	0	0 %
8. Policy Review	2	10 %
9. Policy Retirement	0	0 %

The second most common phase of ISP management was *Policy Development* that was included in seven studies (35 %). Two conceptual studies included in the synthesis focused on the *Policy Development* phase meaning that there were no conceptual studies found focusing on other ISP management phases (Jalali et al., 2019; Takai-Igarashi et al., 2017). All empirical studies focusing on *Policy Development* used the research data to discuss the ISP development in healthcare such as in a study by Kim et al. (2013) where privacy and security related laws and guidelines were analyzed, and with a help of policy and technical experts from the healthcare sector an ISP framework was developed.

The *Policy Awareness & Training* phase was included in two studies (10 %). The first study by DeSouza and Valverde (2016) stated that by improving information security awareness and training, employee ISP compliance could be increased. Increasing awareness and training was also suggested by Vrhovec and Markelj (2018), who concluded that healthcare workers do not see personal benefits in ISP compliance although they consider possible risks for the hospital and its patients in their behavior and that the healthcare personnel are not aware of cyber risks related to the use of personal mobile devices.

Two studies (10 %) focused on *the Policy Review* phase reviewing the existing ISP documents. In an article written by Stahl et al. (2012) a critical discourse analyzation of 25 publicly available ISP documents of the United Kingdom National Health Service Trusts was conducted. The study concluded with several findings such as that the ISPs can serve ideological aims where management legitimacy is highlighted even this can be questioned in healthcare settings where doctors or nurses may think that their opinions should be considered. Stahl et al. (2012) also raised questions about the sincerity of policies and whether the ISPs are aiming to increase ISP compliance or coerce and threaten the staff, and noted that the ISPs should be written and targeted to the users. Interestingly, the article published in 2012 noted that information security had been very actively promoted by the senior management team in the NHS in recent years, but according to a report conducted after a WannaCry cyber-attack that had serious impact on the operation of the NHS in 2017, the main reason for the infection was failing to *"maintain good cyber-security practices"* (National Audit Office, 2017).

The other article reviewing existing ISP documents was written by Karlsson et al. who also used the discourse analysis on analyzing the documents that included one high-level information security policy document and two low-lever policy documents that were obtained from a healthcare organization in Sweden. According to Karlsson et al., conflicts between policies and employees' needs were noted and they highlighted lengthy policies that may signal about text that is not

constitutively clear or missing a direct target group. As improvement suggestions the paper suggested that ISPs should be process-oriented and that both practice-based perspective and management perspective should be considered in ISP development. (Karlsson et al., 2017).

Both studies reviewing ISP documents in the healthcare sector had limitations regarding the used research data. The ISP documents reviewed by Hedström et al. (2013) were all from one single organization and the content and scope of the documents were not clearly defined. Stahl et al. (2012) reviewed 25 ISP documents, but they were all obtained from actors operating under one single organization and based on the same organizational ISP template.

Overall, as Table 9 showed, most of the studies focused on a few ISP management phases, whereas phases such as *Risk Assessment, Policy Implementation, Policy Enforcement* or *Policy Retirement* were not covered. When considering the phase *Risk Assessment* for example, and its importance for ISP development and continuous cycle of ISP management in the organizational-level process model for ISP management (Knapp et al., 2009), it is surprising that no studies were found focusing on this topic. According to these results, there are several phases of ISP management in healthcare that have not been studied by the previous literature.

5.6 Research contribution

Table 10 lists the main findings in this investigation.

Table 10. Main findings on literature regarding information security policies in healthcare

Number	Finding
1	The previous literature has focused on *Monitoring* and *Policy Development* phases
2	Studies focusing on *Risk Assessment, Policy Implementation, Policy Enforcement* or *Policy Retirement* phases were not found.
3	Studies have been often referring to national policies or international standards rather than on the existing organizational policies
4	Future studies should analyze existing organizational policies

The goal of this systematic literature review was to synthesize the previous literature on ISPs in the healthcare sector and to study how information security policies in healthcare have been studied by the previous literature? When analyzing the literature, an organizational-level process model for ISP management was used to obtain a holistic view of all phases of ISP management included in the previous studies.

Taken together, the results of this study indicated that even the healthcare sector is known to be more dependent on information security than ever before and that one of the most important information security controls for an organization is the ISP, where the literature related to the topic is limited and more research on this area of study is needed. This is also one of the first studies to address this topic and to provide a holistic view to the literature related to ISP management in healthcare.

According to the results, previous literature has focused on the *Monitoring* and *Policy Development* phases. Studies focusing on *Risk Assessment, Policy Implementation, Policy Enforcement* or *Policy Retirement* phases were not found. Reasons for not finding any studies focusing on the phases mentioned can be related to a phase that might have not been interesting or considered as less valuable to study. It is also possible that researchers have not been able find an organization that is currently at this precise phase of ISP management or that the phase has not been recognized as a focus of research. Yet, future studies should address also these under-examined phases when studying ISP management in healthcare as they can offer a clear research focus and provide valuable information and scientific contribution.

It was found that ISP related studies in healthcare have been more often referring to national policies or international standards rather than to the existing organizational policies. In other words, the studies have been more interested in what standards and policies say about ISPs and the ISP development than analyzing ISP documents that were already in use. This finding is also supported by the fact that only two papers were found studying organizational ISP documents.

There could be several reasons for not studying organizational ISP documents. Healthcare ISP documents might have been difficult to find, and healthcare organizations may not have been willing to give permission to use their ISPs for research purposes, or that getting the permission was thought to be too laborious, for example. In addition, the organizational ISPs could have been simply out of the research scope or the researchers have not noticed the potential of using ISP documents as research data.

After analyzing the two papers reviewing existing ISP documents in the healthcare sector, it became evident that more research on this area is needed. Future studies should analyze ISP documents that have been obtained from several different healthcare organizations. As the two papers mentioned used the same method in reviewing the documents, future studies should also consider different methods and utilize standards and frameworks when analyzing the documents. Currently, the previous literature has provided only a limited view to the existing ISP

documents in healthcare and there are many areas of ISP management in healthcare that have not been studied. However, as the ISP is one of the most important information security controls for an organization, the existing ISP documents have a potential to be used in future studies and they can provide valuable information about the information security management in healthcare organizations.

5.7 Limitations

There were several limitations regarding the literature review. The first limitation was related to the used search string, that may not have covered all relevant publications. The number of publications found for analysis was low. As seen in the literature, there are different names for ISPs and some of them may not have been found with the used string. Additionally, the healthcare related terms may not have captured all relevant publications.

Another limitation lies with the search databases used. There are a vast number of databases and search engines that were not used, and these could have contained relevant articles. The data evaluation was based on journal articles with abstract available, written in English and published between 2010 – 2020. It is possible that more relevant articles could have been found with a different criterion. Furthermore, the organizational-level process model for ISP management may have limited the analysis of the literature. Therefore, these limitations should be considered in future studies.

6 INFORMATION SECURITY POLICIES IN HEALTHCARE

6.1 Previous information security policy related studies in healthcare

As described in the literature review of ISPs in healthcare, the value of ISP is known, and its importance has been highlighted in several studies. Although, only a few ISP related studies have been concentrated on the healthcare sector. One reason for the low number of studies analyzing ISPs in the healthcare sector can be found from the subject itself. According to Kotulic & Clark (2004) it can be difficult to gather management of information security related data for research purposes because of its sensitive and confidential nature. Organizations might not simply want to give data related to the security practices of the organization to outsiders (Kotulic & Clark, 2004). This is of course understandable when taking into account the subject and that this kind of data could reveal security weaknesses that could for example risk the organizations reputation if published or used against the organization if found and utilized by adverse cyber actors.

Besides the low number of studies related to ISPs in the healthcare sector, a study analyzing the content of ISPs against well-known information security standards has been missing. Considering the value of ISP and the limitations related to previous literature, this study aimed to answer to following research question: How to improve cybersecurity in healthcare with developing information security policies?

6.2 ISO / IEC 27002 standard

It has been argued that the most recognized form of ISP content can be found from security standards such as ISO / IEC 27002 (Paananen et al., 2019). Similar to the ISO / IEC 27001 standard described in the chapter 3.3, the ISO / IEC 27002 has been jointly published by the ISO and IEC organizations and belongs to the 27000-standard family that concentrates on information security. The full name of the ISO / IEC 27002 standard used in this study was “ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls”. (ISO, 2013).

In practice, the ISO / IEC 27002 standard gives guidelines on how to implement and manage information security in organizations following the ISO / IEC 27001 standard. Considering an ISP, the ISO / IEC 27001 defines that an organization

should have such a policy and the ISO /IEC 27002 gives guidelines for the policy content.

6.3 Gathering healthcare ISPs from the public internet

In this study, ISPs obtained from 21 different healthcare organizations were analyzed. The target organizations included both private and public organizations and the ISPs were compared to ISO27002 guidelines.

Even though scholars such as Kotulic & Clark (2004) have experienced difficulties when trying to get information security related data from organizations for research purposes, all ISP documents analyzed in this study were obtained from public internet sites that required no authentication or additional access to the organization's internal network. Before the actual search, a test search was conducted to see if any healthcare ISPs could be found from the public internet. The test results included several ISPs from healthcare organizations and showed that ISPs for this analyzation could be gathered from the public internet. After the test search the following search was conducted.

Relevant ISP documents were searched with the google search engine. Search strings included ISP related terms such as "information OR digital OR cyber security policy" and "data protection OR data privacy policy" translated into Finnish with names of common public and private organizations operating in the healthcare sector in the country. Because many public healthcare services in Finland were provided by the Federation of Municipalities, a list from Wikipedia containing the names of the Federation of Municipalities was used in the search (Wikipedia, 2021a).

After the ISPs were gathered, they were screened and arranged into a spreadsheet sorted by the year of the publication with the name of the organization. Next, additional information from every organization was gathered from public internet sites and included into the spreadsheet. This information enabled the ISPs with the organization details, such as size of the organization, to be compared to other organizations and their ISPs.

The gathered organization details included the number of employees that provides a hint of the size of the organization. This information was found from the organization's website or from the annual staff report of the organization found with google search. Another similar number gathered was the number of customers per year and the population in the area where the Federation of Municipalities was operating. In addition, information whether the organization

was private or public, the word count of the ISP and the title of the ISP were included for every ISP.

The analyzation of the content of the ISPs compared to the ISO27002 standard guidelines was conducted by using content analysis. Content analysis was chosen because it is a widely used research technique that can be used to quantify and analyze the content of a text (Hsieh & Shannon, 2005). Content analysis can be conducted depending on the case and chosen coding, however, in this study the ISO27002 ISP guidelines directed the coding and the analysis.

In the analyzation, every ISP document was carefully read to determine whether the ISP fulfills the guidelines from the ISO27002. This analyzation process provided quantitative information from all ISP documents that could be compared with each other and against the chosen standard.

6.4 ISP characteristics

In the search of the ISPs of the healthcare organization from the public internet, a total of 21 organizational ISPs were found. The oldest ISP was dated in 2012, whereas three were dated the year 2020 when the search was conducted. Most of the ISP documents (86%) were published during the past four years and only three ISPs (15 %) were published earlier.

As written in ISO27002, to keep the policies updated the ISPs should be reviewed regularly or if changes happen in the environment (ISO, 2013). Even if only three ISPs (14%) included information about the review cycle of their ISP or the next review date, the results hint that most of the ISPs have been updated during the past few years. Yet, two ISPs were still found that were written in 2012 and 2013, years before the European union's GDPR was published in 2016 (GDPR, 2021). The GDPR includes a vast number of requirements for organizations that target or collect data related to people in the EU (GDPR, 2021).

Paananen et al. (2019) have noted that there is variation in the literature in the use of the term ISP. According to the results, there is also variation in the name of the ISP documents in healthcare. The most common name of the ISP document found was "Information security policy" that was used in 12 (57 %) documents. The name "Information security and data protection policy" was used in four organizations (19 %) and "Data protection and information security policy" in three organizations (14 %). One of the ISP documents found was named as "Digital security policy" and one as "Data protection and information security policy and principles".

Only one ISP document was found from a private healthcare organization. The rest 21 (95%) documents found were from organizations operating in the public healthcare sector. When gathering the information about the size of the organizations, at first the population of the area where the organization was operating seemed to be of good value and to be used when comparing the organizations. However, this value turned out to be unusable as some of the organizations were operating partly in the same areas and because the private organizations were operating in several different areas. Nonetheless, the gathered information tells that the public organizations had varying amounts of population to be served. The smallest population base for a public healthcare organization found was 12 400 people, whereas the largest was 470 000 people, with the average being 97 000 people.

A more usable variable to be used when comparing the size of the organizations found was the number of the employees. These numbers varied significantly as the smallest organization had 111 employees and the largest organization had 8274 employees. Besides the size of the organizations, the length of the ISP documents varied as well. The shortest ISP document had only 518 words whereas the longest document contained 6969 words, over ten times more. On average the ISP contained 2616 words. When using together the number of employees in the organizations and the number of words in the organization's ISP document, the following comparison chart was created to show how these two variables varied between the organizations. This data can be seen in Figure 13.

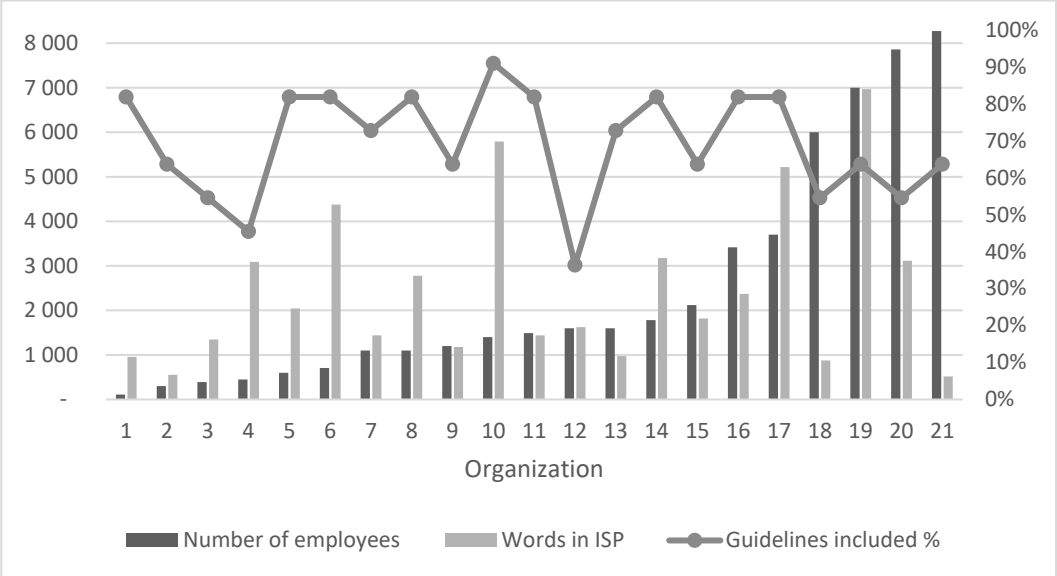

Figure 13. Number of employees and ISP length in words

In Figure 13, the organizations have been marked by numbers between 1 – 21 and sorted from the smallest to the largest organization by the number of employees. This chart shows that when the size of the organization increases from 111 employees to 8274 employees, the average length of the ISP document also increases. Although, the shortest ISP was not found from the smallest organization nor the longest ISP from the largest organization. Smaller organizations often had shorter ISP documents, but surprisingly the shortest ISP was found from the largest organization that can be seen clearly with the organization number 21 in Figure 13. Interestingly it is also seen from Figure 13, that with seven (33%) organizations, the number of employees in the organization and number of words in the ISP are very close to each other. Although, in smaller organizations the ISP had often more words than the organization had employees, whereas in larger organizations the situation was vice versa.

6.5 Example of information security policy

To provide information from the analyzed ISPs one policy document was described in more detail. From the chosen ISP three chapters were translated into English and discussed. The example ISP was chosen based on the word count of the policy and the percentage of ISO27002 guidelines identified from the document that were both close to the average of the analyzed ISPs. The name of the organization was anonymized and changed to "Organization". Because the analyzed ISPs and their content varied significantly the following description is valid with one ISP document only.

One of the chapters was entitled "*Information security knowledge and maintenance of that knowledge*", the translation of chapter nine was the following: *"Every employee of the Organization whose duties require knowledge of information security instructions, receives guidance on the location of the information security instructions and the organization of information security in the Organization. The information security instructions are available in the intranet to each staff member of the Organization. Those responsible for the maintenance, development and management of information security must be offered the opportunity to acquire sufficient basic and further education."*

In accordance with the chapter of the ISP, the organization offered information security instructions and guidance to their employees. Even so, the target personnel were limited to employees whose work duties require that knowledge. These personnel were to be informed where to find security instructions if needed. Yet, cybersecurity related education or training was not mandatory in the

organization to all employees and even personnel who needed the information in their work will be guided where to find the instructions, and not to participate in education or training.

Opportunity to acquire sufficient education on information security was offered to personnel responsible for information security. Considering the main responsibilities on information security defined in the ISP was mentioned to be for the CEO and the board of members, it would be interesting to know how many of these persons have been educated sufficiently. According to the surveys on cybersecurity awareness, the management personnel did not have sufficient knowledge on this subject. Even though the information security instructions were told to be available to each employee in the organization, it was unclear whether all employees were instructed where to find them or required to read and follow these instructions. Overall, the chapter gave the impression that instructions and education in the organization was limited.

Another chapter was entitled "*Information security monitoring and handling of problem situations*" with the following content: "*The IT director has the authorization given by the top management and the obligation to carry out monitoring of information systems to take measures to improve the identified information security weaknesses. Every employee of the Organization, data processor, administrator and user of information systems or information networks is responsible for the implementation of information security and is obliged to comply with the operating procedures, rules and information security instructions approved by the management of the Organization. The employee of the Organization has supervisory responsibility related to data protection and information security issues. Users and administrators must report their findings on information security deficiencies, information security-related abuses or suspected information security violations using the HaiPro information security reporting feature or by contacting (name of the service provider) service desk. Each operational department is responsible for implementing the given instructions on information security. The administrator users and responsible users in the department are responsible for ensuring that the department has sufficient knowledge on the instructions and how to use the information systems.*"

In the beginning of the chapter, it was mentioned that the IT director is responsible for monitoring the information systems and taking actions to fix the identified information security weaknesses. In practice, this hardly would not be the case as it would be impossible for one person to monitor a large and complex IT-environment and find and fix security weaknesses. Therefore, this more likely refers to the responsibility to oversee such actions than conducting them by

himself or herself. Next, the ISP described that all information system users were responsible for following the instructions and rules and have "*supervisory responsibility related to data protection and information security issues"*. Such responsibilities should come with proper training and education, although the instructions and education were offered to limited personnel only.

All users were required to report "*their findings on information security deficiencies, information security-related abuses or suspected information security violations"* via the HaiPro information security reporting feature or by contacting a service provider. According to this guidance, all findings could be reported via two channels. This was an interesting finding, as these channels may have different service level agreements and response times which can be vital when taking actions against possible cyberattacks or ransomware infections. Without further training or education, it can be confusing for employees to choose which reporting channel to use as well.

At the end of the chapter, the responsibility to implement given information on security instructions were sent to every department and administrator users and "responsible users" in the department. As different departments may have different cultures and needs, this can be justified. However, it should be ensured that the administrator users and the "responsible users" in the department are skilled enough to implement these rules and instructions in the department properly, and that there is enough communication, if any, between the department and personnel responsible for managing cybersecurity. Otherwise, the rules implemented may differ too much from the original.

The last chapter discussed in more detail was entitled "*Data classification*" with the following content: "*Information owned by the Organization is classified by the person who owns the information. Information on the classification is based on the law on public authorities' activities (Publicity Act, 621/1999) and the more detailed instructions given by the Organization regarding the application of the law. The categories according to the Publicity Act are public, non-public and confidential. When using cloud services, it should be noted that information that has not been classified may not be exported to the cloud services"*.

According to the policy, the classification used in the organization was based on the applicable national legislation. The classification system described included three levels: public, non-public and confidential. Surprisingly, the term "non-public" was not found in the referred act, but the term "given at discretion" instead was found. It remained unclear what was the justification for the use of term non-public as the publicity act is based on the principle that "the documents of the

authorities are public, unless this or another law separately provides otherwise." (Finlex, 1999).

The last sentence in the chapter stated that information that has not been classified, is not allowed to be transferred into cloud services. This sentence should have been explained in more detail to avoid confusion or misunderstanding. If the meaning was to prevent transferring confidential information to cloud services, the reader can now understand that information that has been classified as public, non-public, or confidential can be transferred if there is a classification mark. It is also possible to understand the sentence in a way that only information that has been classified as non-public or confidential can be transferred to cloud services as public information usually is not marked (Finlex, 1999). All in all, the whole chapter on data classification should be revised and clarified.

6.6 ISPs compared to ISO27002 guidelines

Following the guidelines set for ISP in the ISO27002 standard, the included guidelines were identified from each ISP document. The list of coding used in the analyzation is presented in Table 21 in the appendix. The percentage of included guidelines per ISP is shown with the line with markers in Figure 13.

The first ISO27002 guideline identified from the ISPs suggests that the ISP should be approved by management. From the 21 ISPs, 18 (86%) included statement that the ISP has been approved by management. In many cases this statement was found on the cover page of the document with a date of the acceptance. In public organizations the ISP was approved by the executive board and in the private organization by the chief executive officer. In three ISPs this statement was not found, and it remained unclear whether the policy document was approved by management.

The second analyzed guideline suggests that the ISP should be published and communicated to employees and to relevant external parties. This guideline was considered in 13 ISPs (62%). In these policy documents it was defined that the ISP will be published and communicated to all employees and to relevant external parties. Five of the ISPs also included information on where the document will be published and where it can be found, for example, "This document can be found from the organization's intranet and public website". However, two ISPs stated that the ISP can be found from the organization's restricted intranet only. This is an unexpected result, as all ISP documents analyzed were found from the public internet. What is more, one ISP document was marked as confidential with a reference to national regulation. In a typical four-level information classification

system, confidential is the highest level of information with the highest level of protection (ITGovernance, 2022). In other words, this classification means that the document includes sensitive information with restricted access and that the document should not be available publicly. Eight ISPs (38%) included no information about to whom the document will be communicated. Each ISP found, however, required all users to follow the policy.

Addressing requirements created by a business strategy was found from six ISPs (29%). These ISPs referred directly to the strategy of the organization. The only guideline that was fulfilled by every ISP analyzed was addressing requirements created by regulations, legislation, and contracts. This guideline was taken into account often by simply stating that the ISP is based on regulation and legislation. Although, one ISP listed 23 acts and degrees for the information security by starting from the constitution.

The most striking result to emerge from the data is that none of the ISPs included any consideration for current or projected information security threat environment. Addressing requirements created by the information security threat environment was the only guideline that was not followed by any of the ISPs analyzed. As a matter of fact, neither information security or cybersecurity threats were mentioned in these ISPs at all.

From the gathered ISPs, 19 from 21 (90%) contained the definition of information security. Unexpectedly, the ISPs had several different definitions for information security. Some of the ISPs included a detailed explanation of what is information security and how it is affecting the operation of the specific organization, while others simply defined the information security with the classical CIA triad (Samonas & Coss, 2014) that includes protection of confidentiality, integrity and availability of data. One ISP defined information security as: “securing the processing of data”.

Most of the ISPs defined responsibilities and roles for information security management in the organization. Even so, 19 (90%) of the ISPs included definitions at a general level only such as the following example taken from one ISP: “the responsibility of information security belongs to every employee in the organization. The ultimate responsibility for information security belongs to the director of the organization and the board of directors are supervising the director’s work”. More specific definitions were found from 15 ISPs (71%). The most specific ISP regarding this guideline included twelve separately named roles defined for the information security management.

Processes for handling deviations and exceptions were included in 17 ISPs (81%). The processes described in the analyzed ISPs concentrated on controls and reporting deviations and exceptions related to user behavior rather than handling or reporting security incidents. Another area of focus in these processes describes different types of deviations and sanctions.

On average, an ISP included nine (69 %) of the 13 guidelines. Nine guidelines were included in eight (36%) of the ISPs. The highest number of guidelines were found from ISP number ten, published in 2018, that included 12 (91 %) of the guidelines with the only missing guideline being the addressing of the information security threat environment. The lowest number of guidelines identified was found from an ISP published in 2018 that included four (36 %) guidelines.

As seen from Figure 13, the number of guidelines included in the ISP does not seem to be related to the size of the organization or to the length of the ISP. Whereas, the smallest organization with just over 100 employees and less than 1000 words in the ISP had 82 % of the guidelines included, and an organization with over 7600 employees and 3000 words in the ISP contained only 55 % of the guidelines. Furthermore, when comparing the first four organizations in Figure 13, it can be seen that even though the number of employees in the organization and the number of words in the ISP are growing, the number of guidelines included is decreasing.

The four biggest organizations that had more employees together than the rest of the organizations combined, had less guidelines included in their ISPs, compared to several smaller organizations that had less than the average. Nevertheless, the highest number of guidelines was found from a relatively long ISP (organization number 10 in Figure 13) that was also long compared to the number of employees in the organization.

6.7 Research contribution and implications for practice

Table 11 lists the main findings on this investigation.

Table 11. Main findings on information security policies in healthcare

Number	Finding
1	ISPs did not consider the current or projected information security threat environment.
2	The ISPs were focused on ensuring regulatory compliance rather than linking the ISP to the organizational strategy
3	ISPs did not consider reporting security incidents
4	The length and content of the ISPs varied significantly
5	None of the ISPs covered all ISO27002 guidelines

The aim of this study was to investigate how to improve cybersecurity in healthcare through developing information security policies. This study was one of the first studies to investigate ISPs used in healthcare organizations and to analyze them against an internationally recognized information security standard. The investigation provided new knowledge about ISPs used in healthcare organizations and how cybersecurity in healthcare can be improved with ISPs.

Prior studies have shown that ISP is one of the most important information security controls for an organization (Doherty & Fulford, 2006; Höne et al., 2002). Establishing an ISP has been seen to also improve cybersecurity (NIST 2022a). Previous studies evaluating ISPs in healthcare have been limited for two reasons. The first issue was related to the analyzed ISP material that has been obtained from one single organization (Hedström et al., 2013) or based on the same organizational ISP template (Stahl et al., 2012). Secondly, a study analyzing ISPs against well-known information security standards had been missing. To fill these gaps of knowledge, this study analyzed a total of 21 ISP documents against one of the most recognized forms of ISP content found from the ISO27002 standard. Each ISP document was obtained from different organizations operating in the private or public healthcare sector and analyzed with directed content analysis.

The most interesting finding was that none of the ISPs included any consideration for a current or projected information security threat environment. This finding suggests that the healthcare organizations have not considered the information security threats to their operation or how to protect from them. Moreover, the organizations may have not implemented proper risk assessment processes to cover information security related risks such as cyberattacks, and that the link and cooperation between the organization's risk management and information security management might be missing. Future studies should consider focusing on this matter. Considering that this lack can be found from ISPs that are publicly available, this can have an impact how different parties from citizens to malicious actors see the level of cybersecurity in a particular healthcare organization and in the whole healthcare sector.

Another striking result was that only a few ISPs addressed requirements created by the organizational strategy. However, all analyzed ISPs considered the requirements created by laws, regulation and contracts. According to these results, organizations are focusing on ensuring regulatory compliance rather than the information security management that considers the threat environment of the organization and supports the business strategy of the organization. Focusing on regulatory compliance may help the organizations to cover compliance

requirements, but it does not protect the organization's business strategy from information security threats, especially if they have not been considered.

A strong emphasis on regulatory compliance in ISPs, with a lack of connection to the business strategy and information security threats, gives the impression that the authors of these ISPs have recognized the regulatory requirements linked to information security but not to the information security threats or to the strategy and business needs of the organizations. In other words, it seemed that the authors did not have knowledge enough or were not able to identify the information security threat environment of the organizations and link the threats to the regulatory requirements and business strategy. With these two critical factors missing, organizations may lack proper information security management. One reason for this can be that these organizations have personnel responsible for regulatory requirements but a lack of information security and cybersecurity management personnel.

Healthcare organizations and their top management should ensure that they have someone in the organization with the defined role for cybersecurity management. The top management must also ensure that the person has knowledge of cybersecurity management so he or she is able to consider these deficiencies and manage the cybersecurity in the organization in a way that supports the strategy and business needs of the organization. If the organization cannot find or hire such a person, consulting services should be used.

When communicating security related policies such as ISP, organizations should ensure that no confidential information will be leaked. However, according to the ISPs found, some of the documents were marked as confidential but were available on the public internet. Healthcare organizations should take actions to ensure that they have a proper information and or data classification policy defined and implemented, and monitor that the policy is complied with. The objective of information classification is to ensure that the information is properly secured (ITGovernance, 2022). The investigation showed that there is a conflict between the used classification and selected security measures. Requirements for information classification can be found from standards such as ISO27001 and NIST CSF (ISO, 2013; NIST, 2018). One practical example of information classification can be found from Harvard University guide *Data Classification - Administrative Examples* (Harvard University, 2022).

On the other hand, communicating the ISP should be ensured to all relevant users, now several ISPs lacked in determining to whom the ISP will be communicated. Nevertheless, all users were often required to follow the organization's ISP. It can be questioned; how could all users, especially third parties such as consultants

working remotely, follow the organization's ISP if it has not been communicated to them? Organizations should pay attention when determining the target group of their ISP and make sure it covers all relevant parties.

6.8 Limitations

Even though this was one of the first studies to study healthcare ISPs, the following limitations of this study should be considered. The ISPs analyzed were obtained from organizations operating in one country. Organizations operating in one country and under the same national legislation may have similarities in their ISPs compared to organizations operating abroad. In addition, all ISPs analyzed were obtained from the internet. There were several healthcare organizations in the country whose ISP were not found, probably because they have not made these documents publicly available. The research material contained only one ISP from a non-public healthcare organization.

The use of the ISO27002 standard was only one way to analyze the ISPs. Comparing ISPs to other standards or guidelines would have provided different results even with the same research data. Therefore, this analyzation was limited to the chosen standard.

7 PATIENT SAFETY INCIDENT REPORTING AND CYBERSECURITY - LITERATURE REVIEW

7.1 Incident reporting and patient safety

As determined by the WHO (2020): “Patient safety is the absence of preventable harm to a patient during the process of health care and reduction of risk of unnecessary harm associated with health care to an acceptable minimum”. Yet, patient safety incidents where patients are harmed are common and the costs from these incidents are high. It is estimated that in high-income countries 10 % of the patients are harmed while in hospital care and 40 % of the patients are harmed globally while receiving healthcare with a total of 134 million adverse events and 2.6 million deaths annually (National Academies of Sciences, 2018; Slawomirski et al., 2017; WHO, 2002; WHO 2009, WHO, 2019). It is also estimated that unsafe care is one of the 10 leading causes of death and disability worldwide (WHO, 2019). Costs from patient safety related incidents in OECD countries alone are estimated to be trillions of US dollars annually (Slawomirski et al., 2017).

Nearly half of the cases in high-income countries (WHO, 2019) and over 80 % in low- and middle-income countries (National Academies of Sciences, 2018) have been considered as preventable. Investments in improving patient safety have the potential not only to save millions of dollars per year but to save many lives as well (Agency for Healthcare Research and Quality, 2015). Furthermore, preventing adverse patient safety incidents is likely to have lower costs than treating the harms caused (Slawomirski et al., 2017).

One important factor in preventing adverse patient safety incidents and increasing patient safety is the systematic reporting of incidents. Many national reporting systems were taken into action after a publication of a report *To err is* human: Building a Safer Health System published by Kohn et al. in 2002, who stated that “the problem is not bad people in health care--it is that good people are working in bad systems that need to be made safer.” (Kohn et al., 2002).

In 2007, pilot organizations in Finland started using a Finnish patient safety incident reporting system called HaiPro (Reporting System for Safety Incidents in Health Care Organizations) that was developed by VTT in cooperation with healthcare units (Ministry of Social Affairs and Health, 2008). The HaiPro system is a web-based tool that is based on anonymous and voluntary input, and it is currently used in over 200 different social service and healthcare organizations to report patient safety incidents (Awanic, 2020). HaiPro is used to report incidents

that caused harm to a patient such as medication errors, also near misses, and these reports are collected into one national database (SPTY, 2020).

The national HaiPro database includes quantitative and structured data such as the profession of the reporter, place of the incident, and qualitative data such as a free text description of the incident. The data in the national HaiPro database can be used as research data to study what kind of patient safety incident reports have been reported, analyzing reporting trends or to study the factors related to the reports, for example. The research using the national HaiPro database is controlled by SPTY. (SPTY, 2020).

The previous literature reviews related to patient safety incident reports have concentrated on studying the patient safety incident reporting systems in general (Brunsveld-Reinders et al., 2016) or determining if the use of reporting systems has improved patient safety in practice (Stavropoulou et al., 2015). Even though it was known that healthcare has suffered from cyberattacks (Ghafur et al., 2019; Choi et al., 2019) and that the sector is targeted by adverse cyber actors (Jalali et al., 2020) there have been only a few studies on cybersecurity and patient safety incident reports. For example, we know that there have been cybersecurity incidents in hospitals (Ghafur et al., 2019; Choi et al., 2019), but we do not know how they have affected patient safety incident reports. This information could be used to improve both cybersecurity and patient safety.

When considering the importance of cybersecurity on the operation of the healthcare sector, for patient safety, and that patient safety incident reports can be used to improve patient safety, there was a need to study how patient safety incident reports have been used in cybersecurity related studies. To fulfil these needs, this investigation used the following research question: How have patient safety incident reports been used in cybersecurity related studies?

The hypothesis was that there will be studies found focusing on cybersecurity and patient safety incident reporting, but less articles related to HaiPro and only a few related to HaiPro and cybersecurity. This expectation was based on the SPTY's answer to a research permit application for studying HaiPro reports and cybersecurity which stated that the idea of linking HaiPro reports, and cybersecurity was new. It was expected that the results will show how HaiPro reports have been studied related to IS and to increase the knowledge about how they could be studied regarding cybersecurity. In addition, this investigation aimed to find out how possible previous studies related to cybersecurity and patient safety incident reporting have been conducted, what frameworks have been used and what have been the results.

7.2 Study eligibility criteria

A systematic literature review was conducted to synthetize the previous literature related to cybersecurity and patient safety incident reports. The literature review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach (Moher et al., 2009).

Relevant articles were searched from the following databases and search engines: Google Scholar, IEEE Xplorer, PubMed, Sage Journals and ScienceDirect. The keywords used contained patient safety incident reporting, IS and cybersecurity related terms. The used keywords in the literature search were: “haipro”, “patient”, “safety”, “incident”, “report”, “health”, “cyber”, “data”, “security”, “computer”, “information”, “system”.

7.3 Data evaluation

The following evaluation criteria for the literature were used:

- Published in English
- Scholarly journal article or peer reviewed
- Abstract available

Papers that did not meet the evaluation criteria were excluded. Below is the list of the initial search and the search results per database:

- IEEE Xplore; the result was zero papers. After using all keywords, the search terms were narrowed to include “incident”, “report” and “healthcare” which resulted in three journal articles.
- PubMed; is focused on healthcare articles, and therefore the keywords “health” or “patient” were not used. PubMed resulted in 135 journal articles.
- Sage Journals; 225 journal articles.
- ScienceDirect; provided 240 journal articles.
- Google Scholar; provided 30200 results. Because of the high number of results, the search was narrowed with the following criteria: Results between 2000-2020, English sites only, must include “incident report”. With this criteria, Google Scholar provided 305 results.
- With the criteria described above, a total amount of 908 articles were found. After screening, 857 articles were removed because of duplicates or because there were no abstracts available. Yet, most of the removed articles focused on different topics than patient safety incident reporting, such as cybersecurity incidents or physical security. The remaining 51 full-text articles were assessed for eligibility and examined in detail.

After a detailed examination of the remaining full-text articles, only 5 of the studies were included in the synthesis whereas 46 articles were excluded because they did not use patient safety incident reports as research data. The selection process of the articles is shown in Figure 14.

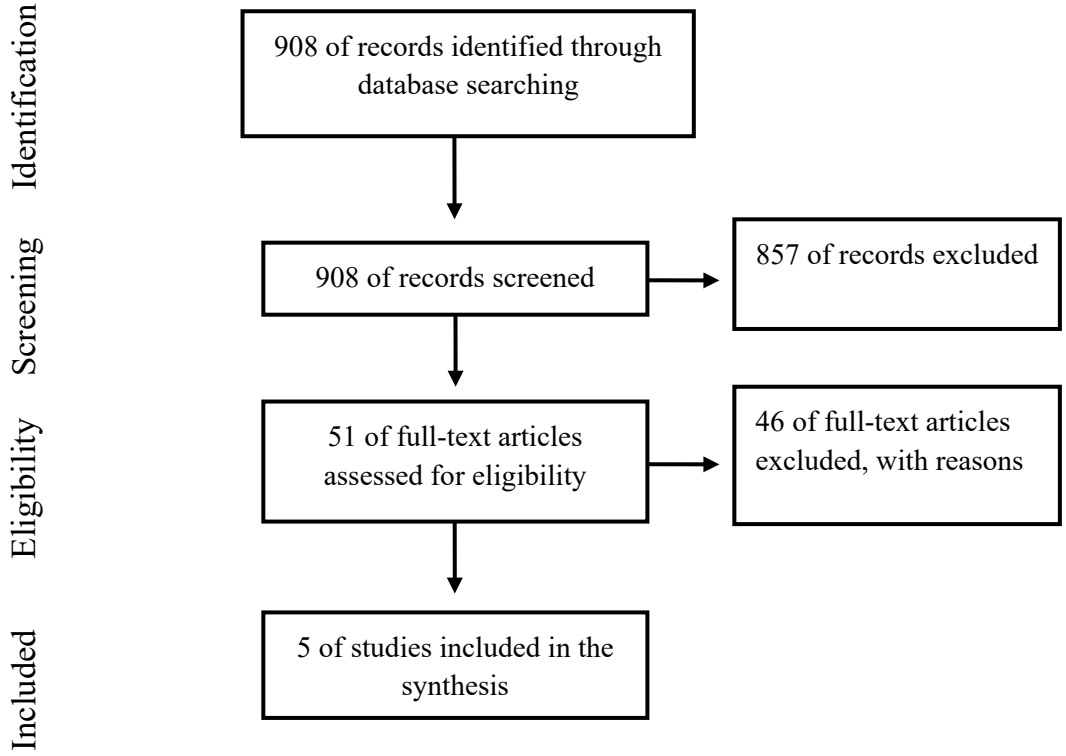

Figure 14. Patient safety incident reports and cybersecurity literature review PRISMA flow diagram

The five articles included in the synthesis in chronological order from the oldest to newest were:

- Jylhä et al. 2016. *"Adverse events and near misses relating to information management in a hospital"*
- *Palojoki et al. 2017. "An analysis of electronic health record–related patient safety incidents"*
- Hautamäki et al. 2017. *"Health information systems´ usability-related use errors in patient safety incidents"*
- Saranto et al. 2018. *"Lack of Patient Data Privacy Challenges Patient Safety"*

- Syyrilä et al. 2020. *"Communication issues contributing to medication incidents: Mixed-method analysis of hospitals' incident reports using indicator phrases based on literature"*

Even if the number of eligible studies from the literature search was low, it was decided to review the remaining five articles. The main reason for this decision was the fact that all of the remaining articles used HaiPro patient safety incident reports as research data and a review of these articles could provide information on how real patient safety incident reports have been studied before, and how they could be studied in the future. This information was seen valuable for future studies on the subject and inevitable for the next study conducted for this dissertation studying information security incident reports in healthcare reported via the HaiPro system.

7.4 Literature overview

According to the results from the literature search, patient safety incident reports have not been used in cybersecurity related studies. Relevant studies from the literature search were all related to the HaiPro-patient safety incident reporting system and IS and have been conducted during the past few years only. The five studies included in the detailed examination were all published between 2016 and 2019 making the topic both new and emerging. The reasons for the topic not being studied before may be related to the nature of incident reports themselves that may have been thought to contain information about patient related healthcare processes only and not to include data or information that is connected also to IS and cybersecurity, and to the many systems and services that are used in healthcare currently.

On the other hand, when thinking about the reasons that have aroused attention in this topic lately in the academic world, that can be related to the increased digitalization in the healthcare sector and the increased knowledge about the dependencies that modern healthcare has on a vast amount of digital systems and services. Furthermore, the previous literature about the incident reports may have increased the knowledge about the HaiPro system and the possibilities that the incident reports offer to studies related to IS. For example, a researcher may have noticed that the HaiPro incident reports include information related to the IS, and that it could pose interesting data to be studied and the findings informed to the research community.

7.5 Characteristics of the studies

The studies had all a correspondent author from the same university in Finland called the University of Eastern Finland. These authors had participated in several studies included in the synthesis, and only one of the publications had an author originating from a university outside Finland (Jylhä et al., 2016). This detail gives a signal that even though the HaiPro patient safety incident reporting system and its data is not widely used in IS related studies, the studies are conducted in Finland only and lead from one university in the country.

Moreover, studies related to the topic were also studied by a few authors supporting a view that the HaiPro is not well known in the IS research community. In all five studies, the corresponding author originated, not only from the same university, but from the same social or health related department, that could have reduced the variance used in the studies. Because there were no studies found where researchers originated from different departments such as from the department of computer sciences, it is likely that studies conducted by researchers from different schools could provide new and valuable information by using and analyzing the same data but from a different point of view.

All five studies were empirical studies with empirically gathered data, meaning that no conceptual studies about the topic meeting the search criteria were found. The lack of conceptual studies and the low number of studies can be due to the search term HaiPro, which is not a universal system but made and used in one country. Therefore, it is assumable that this system is not well known outside Finland where it could be studied as well, and used as an example in conceptual studies related to patient safety incident reports and IS. Besides, because HaiPro provides empirical data it is also more likely that it is used in empirical studies than in conceptual research.

7.6 Research settings and data collection methods

Although all the studies included in the synthesis were using data that was collected via the HaiPro system, the research setting, and the data collection method used varied. Interestingly, only one study gathered the data about patient safety incident reports from the national HaiPro database where all the reports have been sent by the user organizations to be used by authorities and researchers, for example. The other four studies obtained the data directly from a healthcare organization such as hospital or hospital district.

Reasons for obtaining the patient safety incident reports from the healthcare organization itself and not from the national HaiPro database, that could provide larger and wider amounts of reports can be several. If at least one of the researchers in the research group is working in a healthcare organization such as with Syyrilä et al. (2020) or that the University is close to the University level hospital district (Jylhä et al., 2016), the researchers may have an easier access to the data in the organization versus the data located in the national database where a research permit application must have been accepted by the SPTY before access is granted.

Even though the five studies included in the synthesis were all empirical studies with empirically gathered data and published during the past few years, the data used in these studies were gathered from several years earlier. For example, in the paper by Jylhä et al. that was published in 2016, the empirical data included patient safety incident reports between 1/2008 and 12/2009, and in the study conducted by Syyrilä et al. that was written in 2019, but published in February 2020, the data was from the year 2015 (Jylhä et al., 2016; Syyrilä et al., 2020). Because the search criteria included peer reviewed articles only, it is assumed that the acceptance and publication process for the peer reviewed research articles may have affected the long period of time between the used data and the publication, or that they have had other reasons for using a data sample with a particular time frame. The researchers may have also had some reasons for selecting the data with a particular time frame that they have not clearly mentioned in the paper such as an easier access to the data with these dates. Yet, when using data from the national HaiPro-database a researcher can request incident reports with any time frame.

When comparing the studies by the number of years between the latest patient safety incident report included in the year of publication of the paper, the study that was conducted by using data from the national HaiPro-database had the shortest time between the two measurement points. The highest number of years between the two points was seven years and the shortest two, with the average being four years. This result hints that the studies related to the patient safety incident reports and IS contain at least a couple of years of old data when the paper is being published. Even though there was only one study found meeting the search criteria and using the national HaiPro-database as a source of research data, this kind of study can include newer data. Furthermore, the study using the national HaiPro-database as the source of data was the only study including data from more than one hospital district.

When comparing the amount (*n*) of patient safety incident reports included in these five studies, the *n* varied from a data sample with 500 reports (Syyrilä et al., 2020) to a sample with 12294 reports (Saranto et al., 2018), with the average

number of reports used being 3699 reports per study. An average time period in which the data sample was collected was 38 months. Nevertheless, from the five studies included in the synthesis, two studies used data from 12 months and two studies used data that was collected from 24 months. The study using the national HaiPro-database was again different, in using a time period of ten years (120 months). The national HaiPro-database seems to provide access to a wider amount of data from the year the system was put into service and it can be due to the data is easier and more practically accessible with a long time period from the national HaiPro-database than from one organization where the time period of collected data appears to be a year or two.

Interestingly, the $x = n/t$, where the n (the number of patient safety incident reports included in the data sample in the studies) divided by t (the time period the data was collected in months), varied a lot from 34 reports per month to 208 reports per month, as the average number for x was 99 reports per month, meaning that even the time period in the sample would be alike, the data sample can contain very different amounts of IS related reports. The smallest amount of reports per month was found in the study by Jylhä et al. (2016) who apparently used more criteria and more precise search terms for the data query when selecting reports that were reportedly *"near miss and adverse event incident reports"*. The highest number of reports per month in the used data sample was surprisingly not found from the study using the national HaiPro-database, that could presumably contain more patient safety incident reports per month than organizational databases, although a paper conducted by Hautamäki et al. (2017) reportedly had over 200 reports per month and 2500 reports in total with a time period of 12 months gathered from one Finnish hospital district.

In addition to the used search terms, the varying result for factor x, could be indicating that the organizations that have been in the target of the studies may have had a highly varying amount of IS related patient safety incident reports per month. At the same time, the varying result of x can be informing whether the IS related patient safety incidents are reported differently in the organizations and its departments, or that in some healthcare organizations this kind of incidents are occurring more often than in other organizations. Nevertheless, it can be assumed that patient safety incidents take place in all organizations and therefore reporting culture and personal interests to report incidents are affecting x. This is also supported by the study of Jylhä et al. where the number of reports varied depending on the situation, information type, care records, and the profession of the person writing the report (Jylhä et al., 2016).

When a person is reporting a patient safety incident via the HaiPro-system, she will have to classify the report by using 14 main categories with several subcategories (Saranto et al., 2018). These categories apparently provide an opportunity also to a researcher to use these categories when studying the data and according to the studies included in the synthesis, the IS related reports were studied by including reports from the following main categories:

- Information management
- Information flow
- Device and use of device
- Medication management

In addition to the main categories mentioned above, the following subcategories were used:

- Prescribing and transcribing
- Documentation
- Patient Information Management (documentation)
- Coordination of care
- Verbal communication

The most reported main category in these papers was *"Information management"* which is presumably the closest category related to IS along the category called "*Information flow*". One of the papers included all reports without reportedly using any category criteria and in one paper the HaiPro-categories that were included in the research were not clearly disclosed. Besides using the predefined categories in the HaiPro-Data, one study used free-text search keywords to find relevant reports from an organizational database. Reports from the category "*Device and use of device*" was included in one paper only but considering digital and networked organizations, it could include interesting reports related to IS and cybersecurity.

By using a predetermined categorization with studying the HaiPro reports, a researcher puts his or her trust in the reporter who should have categorized the report with the same category where the researcher tries to find it. Using the built-in categorization could be an easy way to find and study relevant reports. However, if the categorization is not performed properly, it is possible that not all relevant reports are found. Another way to find relevant HaiPro-reports mentioned was using a free-text search that offered a possibility to search reports with certain keywords in the same manner as searching information with search engines and could increase the possibility to find relevant reports despite the categorization. This kind of search was reportedly possible in one organizational HaiPro-database.

Probably the most laborious way to find relevant reports used in these studies was to include all reports in the data sample and manually analyze one by one whether a report is relevant or not. Even this kind of manual search can require more time and effort compared to the use of the built-in categorization or searching with keywords, it can provide a way to find all relevant reports from the sample data despite the categorization or keywords used. However, the result of the manual search depends on the researcher analyzing the reports.

Under-reporting and miscoding of the report were reported in two papers (Jylhä et al., 2016; Syyrilä et al., 2020) and because reporting patient safety incidents via the HaiPro-system is voluntary based, it is possible that not all incidents will be reported and that some incidents may have been reported several times by different reporters. This means that the frequencies of patient safety incidents, whether they are related to IS or not, cannot be determined by using the HaiPro-database (Palojoki et al., 2017).

7.7 Research methods and frameworks used in the studies

The research methods used in the studies included in the synthesis were:

- Directed content analysis
- Descriptive and inferential statistics
- Taxonomy mapping
- Inductive content analysis
- Descriptive statistics
- Mixed method

As seen from the list, research methods and frameworks used in the studies varied. These results show that even though the studies originated from the same university and all used HaiPro reports as research data, research settings, and research methods were not the same. However, a descriptive nature of the studies was noted. Next, the classifications used in the studies are discussed with their suitability to study cybersecurity related incident reports.

The studies classified or categorized the reports by using the following frameworks or classifications:

- Original HaiPro classification
- Mix of original and classifications added by the researchers
- Lowry et al.'s classification
- MIComHos framework
- Magrabi et al.'s classification

In research by Saranto et al. (2018), the original HaiPro-categorization was used to produce new information from the existing data to find out what kind of incidents are affecting patient data privacy and what kind of harm to the patient was reported. According to the authors, this kind of result was achieved by using relevant HaiPro-categories and comparing the reported consequence for the patient.

In a study by Jylhä et al. (2016), the authors used the original HaiPro-categorization but added also new main categories with subcategories to classify the reports reportedly because *"if the data could not be coded in existing categories"*. By using these new categories, the paper provided new information about how many percent of the reports were categorized in a category such as "Written information transfer and communication / Information transfer / Data were not transferred". Using a mix of original HaiPro-categories and creating new categories to improve the classification is also an option when studying cybersecurity related reports. However, when classifying the reports between the original and own categories, the researcher is making a categorization that was not possible by the original reporter and therefore this kind of mixture should be conducted carefully.

Lowry et al. (2012) introduced a conceptual classification for usability errors related to EHRs (Electronic Health Records) in their paper *"Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records"*. This classification was used in a study by Hautamäki et al. (2017) who recategorized HaiPro reports using the framework to find out what kind of usability issues have affected the patient safety incident reports. This classification would be interesting to use with usability related cybersecurity reports, but it may be too focused on the usability to create an overall picture of the connection between patient safety incident reports and cybersecurity.

In a study by Syyrilä et al., the authors had developed a new conceptual framework called MiComHos (Medication Incidents and Communication in Hospital instrument) that was used in analyzing the HaiPro reports (Syyrilä et al., 2020). As the name of the framework suggests, it is aimed to be used in analyzing communication and medication incidents and therefore might not be the best option to be used when analyzing cybersecurity related incident reports.

Palojoki et al. (2017) used Magrabi et al.'s (2010) classification in their study *An analysis of electronic health record–related patient safety incidents,* where the authors conducted taxonomy mapping with HaiPro reports between the original HaiPro-classification and the classification created by Marabi et al. As a result, the

paper revealed the frequency of problems per type in HaiPro reports in quantitative form using the Magrabi et al.'s classification.

The Magrabi et al.'s (2010) classification was introduced in their paper *An Analysis of Computer-Related Patient Safety Incidents to Inform the Development of a Classification*. The classification includes 32 types of computer use related problems with four main categories: Information input, information transfer, information output and general technical. Even the Magrabi et al.'s classification includes several categories related to IS, such as "system interface issues" or "Network down or slow", none of the main categories or subcategories consider cybersecurity related problems.

In the current version of HaiPro, depending on the organizational policy, the system can be used in reporting information security incident reports and a reporter can also add a separate information security incident report to the patient safety incident report (HaiPro.fi, 2015). According to an annual quality report from one central hospital in Finland, a total of 57 information security incident reports were reported via HaiPro during 2018 (Vaasa central hospital, 2018). This number indicates that in the national HaiPro database there are hundreds of information security related incident reports reported annually. Interestingly, none of the studies reportedly used reports from this categorization and these reports may be understudied overall.

According to these findings, information security incident reports in the national HaiPro database should be studied in the future. This data could contain valuable and even a unique source of information related to patient safety incident reports, IS and cybersecurity. These reports could reveal what are the characteristics of patient safety incident reports related to cybersecurity, for example.

7.8 Research focuses and summary of findings

As the previous chapter hinted, even though the studies included in the synthesis were related to HaiPro and IS, none of these studies concentrated on cybersecurity related areas. The study conducted by Jylhä et al. (2016) concentrated on information management related HaiPro reports and concluded that the most common information management related to HaiPro incident reports were related to information transfer and communication. Palojoki et al. (2017) concentrated on analyzing electronic health record related patient safety incidents with the Magrabi et al.'s classification and made a conclusion that electronic health record related incidents were more common than in previous studies and the most common problems related to Human-computer interaction.

In a study called *Health information systems' usability-related use errors in patient safety incidents* written by Hautamäki et al., the authors aimed to study the connection between usability issues in information systems and patient safety incident reports. The study concluded that the usability issues in IS in healthcare can endanger patient safety and that the most common usability issues were related to distribution of information into multiple views, identification of the patient and counting on the user's memory in daily tasks. (Hautamäki et al., 2017).

Saranto et al. had their research focus on the importance of data privacy and the European General Data Protection Regulation (GDPR) in healthcare when studying the patient safety incident reports obtained from the national HaiPro database. The summary of findings concluded that the identification of a patient proved to be an important factor in incident reports and should be improved to increase patient safety. In contrast to the other studies included in the synthesis, the paper from Saranto et al. referred to adverse cyber events such as cyber-attacks and data breaches and linked the cybersecurity to the patient safety. However, the focus of the study was on data privacy and not on cybersecurity. (Saranto et al., 2018).

The latest paper in the synthesis was written by Syyrilä et al. published in 2020 and it focused on communication issues in medication that were mentioned in incident reports (Syyrilä et al., 2020). The point of view was more on medication than in IS, but the paper concluded that the most common issues in communication in patient safety incident reports was related to digital communication. It is possible that at least in some cases the errors in digital communication were cybersecurity related, nevertheless the paper did not go deeper into the root causes of the cases such as what caused the errors in digital communication.

7.9 Research contribution and research agenda for future studies

Table 12 lists the main findings in this investigation.

Table 12. Main findings on patient safety incident reporting and cybersecurity literature review

Number	Finding
1	Cybersecurity related patient safety incident reports is a new area of study
2	Studies analyzing patient safety incident reports and information systems have been limited
3	Information security incident reports reported via HaiPro-system have not been studied

The aim of this review was to provide an analysis of the literature on patient safety incident reports and cybersecurity and to find the answer to the following question: How have patient safety incident reports been used in cybersecurity related studies? According to the results, there were some patient safety incident reports and IS related studies conducted but no studies were found studying cybersecurity related patient safety incident reports. This is one of the first studies to address this issue.

It was already known that patient safety incident reporting systems play a vital role in gathering information about root causes of patient safety incidents such as system weaknesses and that these reports can be used to increase patient safety (Kohn et al., 2000; Leape, 2002; Tuttle et al., 2004). When considering the importance of cybersecurity in patient safety, it is apparent that cybersecurity related patient safety incident reports should be studied.

To improve patient safety and cybersecurity that are both vital for healthcare, this study suggests that researchers should take actions to fill this knowledge gap. Increased patient safety and cybersecurity will not only save resources but can help to save human lives as well. The main research agenda for future studies should consider the following research questions that can be conducted by using patient safety incident reports such as HaiPro reports as research data. Firstly, the future studies should address what kind of adverse cybersecurity incidents have affected patient safety incident reports and how. This knowledge could be used in prioritizing cybersecurity resources to the most common incident types to lower cybersecurity risks that can affect patient safety. Secondly, it should be studied what kind of healthcare processes have been affected the most by adverse cybersecurity incidents to increase resilience of these healthcare processes against cybersecurity incidents and to lower the risks to patient safety.

Reporting systems such as HaiPro, and especially the national HaiPro database, and information security incident reports reported via the system, have a lot of potential to be used in IS and cybersecurity related studies. These kinds of studies could provide valuable information to be used in improving the healthcare processes and patient safety in Finland and abroad. According to the results, linking HaiPro data and IS is emerging as HaiPro reports have been used as research data in IS related studies during the past few years and the number of studies is also likely to grow in the future. Nevertheless, the low number of studies about the topic refers that even if modern healthcare is known to be dependent on the information systems and cybersecurity, HaiPro data has not aroused wide attention in the research community and that there are IS and cybersecurity related areas that have not been studied by using HaiPro reports as research data.

This finding alone provides new information about the potentiality of HaiPro reports to be used in future studies.

In addition to the main future research agenda described above, this study proposes research questions for future cybersecurity related studies using patient safety incident reports as research data. The list of questions is not complete and should be extended as the knowledge from the topic is increased. These research questions are categorized by using a Socio-technical approach presented by Kayworth and Whitten (2010) that includes three primary objectives, *Ensuring compliance*, *Maintaining cultural fit* and *Balancing information security and business needs,* that should be all addressed for an effective information security strategy. By using these objectives, the following research questions for future research are proposed:

Ensuring compliance (Ensuring compliance with legislation and standards)

- Were requirements from legislation and standards met in cybersecurity related patient safety incident reports?
- How does the level of organization's cybersecurity compliance affects the amount of cybersecurity related patient safety incidents reported?

Maintaining cultural fit (Ensuring that security guidelines are aligned with organizational values and culture)

- Were IS guidelines align with organizational values and culture in IS related patient safety incident reports?
- What is the user experience on reporting cybersecurity related patient safety incidents and how could it be improved?
- Have employees been instructed to report cybersecurity related patient safety incidents and how?
- Does the organization's culture support reporting cybersecurity related patient safety incidents?

Balancing information security and business needs (Ensuring that risk calculations are business driven)

- What kind of adverse cybersecurity incidents have affected the patient safety incident reports and how?
- What kind of healthcare processes have been affected the most by adverse cybersecurity incidents?
- How to use cybersecurity related patient safety incident reports in improving processes and practices?
- How could cybersecurity related patient safety incident reports be used in organizational risk management?

Studying these objectives can provide information that could be used to improve several services and processes in healthcare such as the following: level of

compliance, cybersecurity, future patient safety incident reports and reporting systems, culture related to incident reporting, organizational risk management, and eventually to improve the patient safety. When considering healthcare is listed as one of the critical infrastructure sectors that if damaged, would have a major negative impact on the whole society (Church et al., 2003; European Commission, 2019), studying patient safety incident reports can help to improve privacy, security, and resilience of the whole nation and its people.

7.10 Limitations

This literature review contained similar limitations than the literature reviews described in chapters 3 and 5. The limitations of this review were related to the used search engines and databases, the used search string, and the data evaluation. More relevant articles could have been found with different search engines and with a modified search string. When considering the small number of relevant articles found, it is possible that several relevant articles could have been found by using some other search database. Additionally, this literature review studied articles written in English only.

8 INFORMATION SECURITY INCIDENT REPORTS IN HEALTHCARE

The previous literature review on patient safety incident reports and cybersecurity showed that the data gathered via HaiPro patient safety incident reporting system has been used to learn from the incidents and to improve the services and processes in healthcare sector. One of the benefits from using an incident reporting system has been the possibility to provide information about how to improve the patient safety.

Even so, the literature review revealed that HaiPro reports have not been studied from the cybersecurity perspective or used to improve cybersecurity. Furthermore, according to the literature review, there has been no research that would have studied the information security incidents reported via the HaiPro system.

Since the importance of the healthcare and cybersecurity was known, an important gap of knowledge was identified, and a new study was needed. To fill this gap of knowledge, this study aimed to answer to the following research question: How to improve cybersecurity in healthcare with developing information security incident reporting?

8.1 Accessing HAIPRO reports for research purposes

As mentioned by Kotulic & Clark (2004) gathering security related data for research purposes can be difficult because of its sensitive and confidential nature. Therefore, it was assumed that studying information security incident reports can be difficult for the same reasons. Adverse cyber actors are known to be interested in healthcare data that can be sold on black markets with high prices (Trendmicro, 2017b). Healthcare data is confidential and should be protected from theft, corrupt or modifications (Stachel, et al. 2015). Futhermore, healthcare data is also highly regulated in many countries (Flaumenhaft & Ben-Assuli, 2018) which may not make access easier to this kind of data for research purposes.

The studies included in the previous literature search that used HaiPro reports as research data, used two different ways to obtain the research data. The first and most often used method was to study incident reports via a healthcare organization that can provide access to reports reported by their employees. The second, but less used method, was to obtain the data from the national HaiPro database that contains reports from all organizations using the system.

In both cases a research permit is needed. In the organizational context the research permit is processed according to the organizational rules. Depending on the organization these rules can vary. On the other hand, in the national context the research permit applications are dealt with by the organization controlling the HaiPro research (SPTY, 2020).

Based on these details, the national HaiPro-database contains more incident reports than any of the organizational databases. The quality of data between these two can also be different. Assumably the national database includes a wide range of data, while in an organizational database an actively reporting unit might produce a relatively great number of reports. Also, under-reporting or miscoding the report have been noted by previous studies using HaiPro data (Jylhä et al., 2016; Syyrilä et al., 2020.)

Considering that the national HaiPro database could offer a wide range of data and because the lack of studies using the national HaiPro database was noted in the literature search, a research permit application was submitted to the organization controlling the HaiPro research. One reasoning presented in the literature search for the low number of studies using the national HaiPro database for research purposes was that access to the organizational database could be faster and easier than the national database. Later, this presumption did turn out to be true.

Over one year after submitting the research permit application to the SPTY, an answer was received that the SPTY cannot grant a research permit to information security incidents reported via the HaiPro system. The reason behind this was that even though the information security incidents had been reported via the HaiPro system and stored in the national the HaiPro database; it is required that the research permit for information security incident reports is granted by the target organization, not by the SPTY. In other words, it was not possible to get a research permit to any information security incident reports reported via HaiPro from the SPTY. What the SPTY can do is to grant a research permit to patient safety incidents only. What is more, if one wanted to study information security incidents in the national HaiPro database, the researcher must have a research permit from every organization individually.

Because getting a research permit from all healthcare organizations that have reported information security incidents via HaiPro seemed to be impractical, the research permit application was submitted to one Hospital district that was known to be a user organization of the information security reporting feature in HaiPro. The research permit to the organization's information security incidents was granted in one month, including discussion between the researcher and the organization and receiving all research data specified in the research permit

application. This supported the idea that a researcher can obtain access to HaiPro incident reports faster and easier via one healthcare organization than via the SPTY.

8.2 Reporting and handling information security incidents via HAIPRO

Because this was the first time when information security incidents reported via HaiPro system were studied, the reporting and handling of information security incident reports is presented in this chapter. This helps the reader to get an overview of the subject as well, before the HaiPro data is analyzed.

Reporting information security incidents in the HaiPro-system is conducted via a web-based form. The HaiPro-system is used via internet connection to the national HaiPro-infrastructure and access between the user organization and national HaiPro-infrastructure over the internet is required. After the reporter has opened a link to the HaiPro-website on his or her work computer's web browser, that has access to the HaiPro-infrastructure, the available reporting types are shown. From these options, the reporter can click a link named: *information security incident report*.

The following figure shows the information security incident reporting template used in HaiPro. This reporting template was obtained from Awanic Oy with a permission to be used in this work. As mentioned in Figure 15, all mandatory fields in the template are marked with an asterisk. Two *Search*-buttons on the top of the template can be used to search for the reporter's department and the department where the incident happened. The search results depend on the organization and organizational structure.

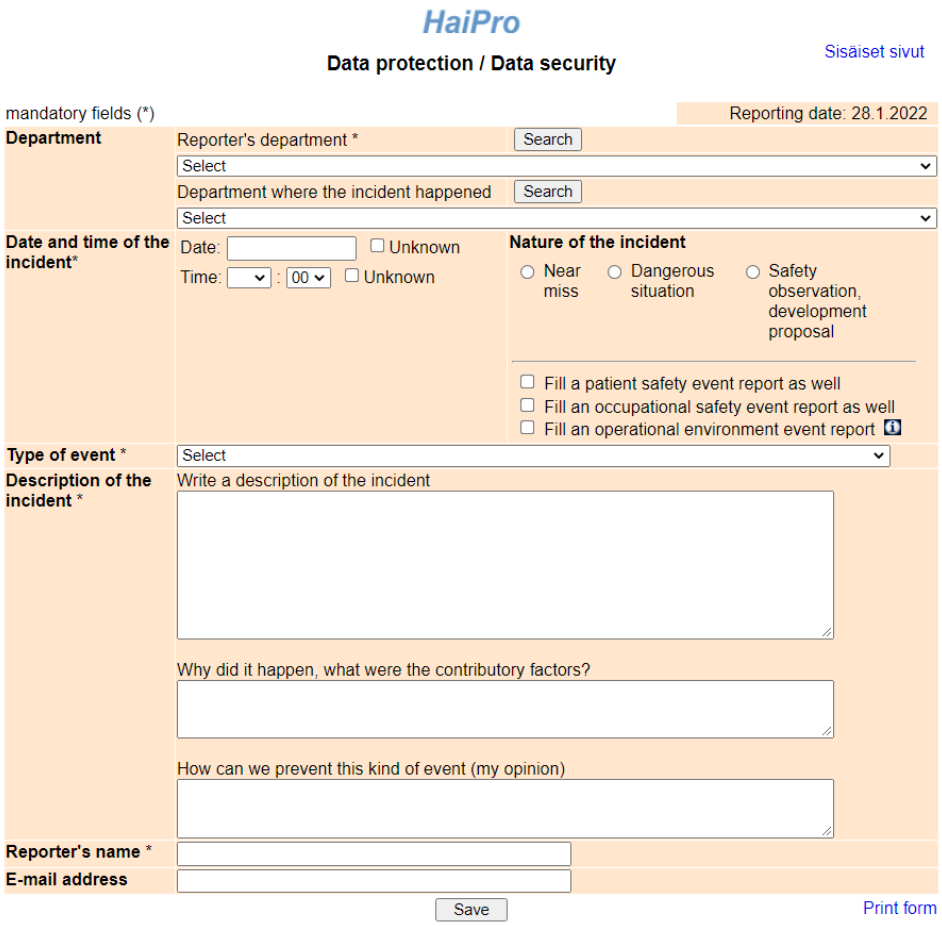

Figure 15. Information security incident reporting template

At the bottom of the reporting template the reporter is asked to leave his or her name and an email address to be contacted if needed. Submitting an email address is optional. These details such as the name of the reporter or email addresses were not included in the research data and therefore were not studied.

For security and privacy reasons names and email addresses are information that are required to be studied carefully. Although, for example information whether an email address was saved with the report or not (yes or no) could tell how many of the reporters of information security incidents wanted to enable that he or she could be contacted in case of additional details about the reported incident was needed. Assumably, because of the high number of incident reports with missing data, the number of reported email addresses could be low supporting the finding that information is often missing, and that the analyst has not been able to contact the person who reported the incident due to the missing contact details. This could be studied in more detail in future studies.

After the reporter of the information security incident has saved the report into the HaiPro system, the report will be moved into the handling process and can be analyzed by the organization's HaiPro analyst. A process model for describing the handling process of an information security report was not available. However, the handling process of an information security incident report follows a similar process model as handling a patient safety incident report. The handling process of a patient safety incident report is described in Figure 35 in the appendix.

After no additional information is needed, the analyst will analyze the incident and fill in details about the analyzation into the incident report. If the incident report requires further actions, the analyst himself or herself can specify the actions needed and persons in charge or contact the person responsible for patient safety who can decide about the specified actions and persons in charge. Actions implemented will be reported to the analyst and into the HaiPro system. After all actions have been implemented and entered into the system, or if no actions are needed, the observation is marked as ready in the HaiPro system. If additional information is needed, the analyst can contact the reporter directly via email if the reporter has entered his or her email address in the reporting phase. If there are no direct contact details on the report, the analyst can try to gather additional information about the incident by contacting employees of the organization via group email targeted to the departments specified in the report, for example.

In the HaiPro system the risk related to the information security incident can be evaluated during the handling process of the incident report. In the handling process, the person analyzing the report can evaluate the risk by using a 5x5 risk-matrix. An example of 5x5 matrix with similar categories and risk levels to the used HaiPro risk-matrix can be seen in Figure 36 in the appendix.

In practice, the risk evaluation is carried out by considering the category of probability against the category of consequence severity. The 5x5 risk-matrix contains five different categories for probability from *rare* to *almost certain* and five different categories for harm severity from *negligible* to *serious*. For each harm category there is a description in the risk matrix such as for the *almost certain* probability category which is described as "an incident that occurs all the time and is likely to occur also in the near future".

The descriptions for different probability categories are general and could also fit to other type of incidents than information security incidents. Nevertheless, the descriptions for harm severity categories are defined for healthcare organizations and patient safety incident reporting. For example, whereas the *negligible* harm severity is described as "a harm that is almost zero, mostly discomfort", the *serious* harm severity is described as "an incident that causes death, serious harm or

permanent injury, or the incident have an effect on a large group of patients or leads to long-term disability, or the length of hospital stay increases more than 15 days".

As a result of the risk evaluation, information security incidents will be categorized with one of the following risk levels:

I Insignificant risk
II Minor risk
III Moderate risk
IV Significant risk
V Severe

In addition to these five risk levels, in the HaiPro-system it is possible to skip the risk evaluation phase and not evaluate the risk of the incident. In this case, the risk category of the incident will not be available. The research data contained several incidents without the information of the incident's risk category. Therefore, it can be said that there is a sixth option in use for the risk level information security incident. In this work this sixth option, for not selecting the risk category is described as *Not available* (N/A).

8.3 Data collection and methods

The research data consisted of information security incident reports reported via theHaiPro system. All reports in the research data were obtained from one public hospital district that had been using the HaiPro reporting system for several years.

Before contacting the target organization prior information about the number of possible information security related incidents reported via HaiPro was gathered from the public internet. It was then assumed that the target organization should have reported at least one hundred information security related incidents via HaiPro. This assumption was supported by the size of the target organization and documents found from the internet where two public hospital districts reported their annual number of information security incident reports. In one organization, the number of information security related reports in one year was 57 (Vaasa Central Hospital, 2018) and in the other the annual number was 110 (Päijät-Hämeen hyvinvointiyhtymä, 2015).

A discussion with the representatives of the organization was also held prior to submitting the research permit application for this study. This discussion revealed the approximately number of information security incident reports reported in the organization. According to the representatives, the reporting system had provided

valuable information for the organization about patient safety incidents. Yet, the information security incident reports had not been carefully examined in the organization and the idea of studying them was seen interesting and worth of supporting.

After the research permit application from the organization was granted, the research data was collected by extracting the target reports from the national HaiPro database by an employee of the target organization. The data was received in an excel spreadsheet containing all information on security incidents reported in the organization via HaiPro. As the possibility to report information security incidents was added into the HaiPro system a few years earlier, the data included reports reported between 1.1.2018 to 3.5.2021.

The research data consisted of 275 information security incident reports and the analyzation was conducted using descriptive statistics. Descriptive statistics was chosen based on the literature review on patient safety incident reports that provided information about the methods used in studies studying incident reports such as incidents reported via HaiPro. Descriptive statistics can be used to describe the characteristics of the data (Fisher & Marshal, 2009). In the analyzation the built-in variables that were included in the information security incident reports was used.

From the research data, the following variables were identified and analyzed:

1. Date and time
2. Reporter's unit
3. Unit where the incident occurred
4. Nature of the incident
5. Patient safety incident reported as well (yes / no)
6. Type of the incident
7. Description of the incident
8. Why the incident occurred?
9. Reporter's view on how this kind of event could be prevented in the future
10. Risk class (1 to 4)
11. Information security sub-area affected
12. Effect on data protection
13. Conditions of the incident
14. Proposed measures to prevent a recurrence of the incident

From this list, it can be seen that the variables included in the research data included more variables than the information security incident reporting template presented in Figure 15. These additional variables (variables 10, 11, 12, 13 and 14)

were included during the information security incident report handling process and by the analyst who is handling the incident report. Therefore, the variables 1-9 were fulfilled by the incident reporter and the variables 10-14 were fulfilled by the analyst.

8.4 Characteristics of the reports

A total of 275 information security incident reports were analyzed. According to the data, the annual number of the reported incidents varied. In 2018, when the information security incident reporting via HaiPro was implemented in the target organization, a total of 50 incidents were reported. In 2019 the number more than doubled to 102 reports and in 2020 decreased to total of 66 reports.

The number of information security incidents reported per month can be seen in Figure 16. In this figure, the monthly number is drawn from 2018 to 2020. Reports from the beginning of the 2021, when the data was extracted, were excluded from Figure, because the rest of the year was not covered in the data sample.

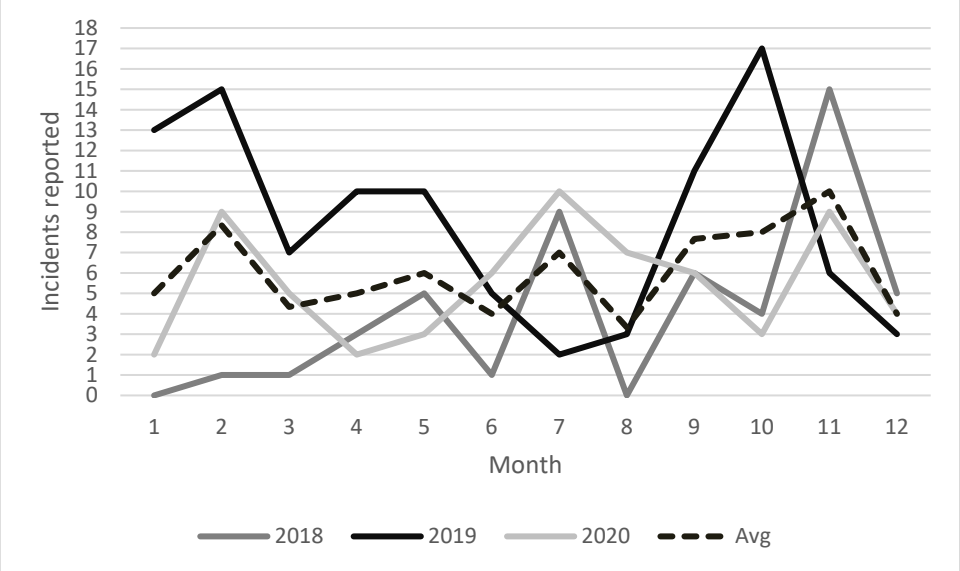

Figure 16. Information security incidents reported per month

Other excluded reports from the chart included 40 reports that did not include date information and three reports where the report was dated before the year 2018. Even though most of the reports included a date, the excluded reports signaled that in the HaiPro system there is or has been a possibility to report an information security incident without information on when the incident occurred. If comparing the increasing ID-numbers of reports that had date information to

ID-numbers of reports that did not include a date, the ID-numbers of reports without a date were from between 2018 to 2021. According to this finding the possibility to report an incident without a date was still implemented when the data was gathered.

From these 40 reports without a date, it was impossible to determine when the incident occurred. Even if the date when the incident was reported could be resolved by using other variables such as ID-numbers or variables not included in the data sample, the actual date when the incident occurred could not be determined. The three reports dated before the information security incident reporting was implemented in the target organization were dated in 2004, 2010 and 2017. The report dated late 2017 could be, for example, a test report before the information security incident reporting feature was implemented. Yet, reports dated 2010 and 2004 indicate that incidents were reportedly dated years before the HaiPro reporting system or its information security incident reporting feature existed (Ministry of Social Affairs and Health, 2008). It is possible that there is a bug or an error in the system that allows or has allowed this kind of behavior. To minimize human errors and miscoding, in these kind of cases, the reporting system could ask the reporter to recheck the date.

As seen in Figure 16, the highest number (17) of information security incidents reported per month was in October 2019. When comparing the total average of six reports per month, the increase in the number of reports per month was significant. In 2018, when the information security incident reporting feature was implemented in the target organization, the increasing number of reports is clearly visible. Nevertheless, zero incidents were reported during August 2018. After the implementation, this was the only month with no incidents reported during the three-year sample.

On average, the highest number of incidents have been reported between September and November. The highest monthly number of reports (ten reports) were reported in November and the lowest number of reports (three reports) were reported in August. The low monthly numbers can be affected by the holiday seasons during June and July and at the end of the year. However, in 2018 and 2020 several incidents were reported in July, during a holiday season in the country, which tells that information security incidents have been reported during holiday seasons as well.

When considering the daily numbers of reports and the fact that most of the days in the sample have no incidents reported, one day was different. In November 2018 seven information security incidents were reported in one day. This means that more incidents were reported during that day than on average in a month in the

three-year data sample. In the sample data, the reports also included a separate field for the day of the week when the incident occurred. A total of 235 reports (85 %) included this information. The reports and the reported day of the week when the incidents occurred, are shown in Figure 17.

When analyzing the following results, it is important to note that the target organization is a public healthcare organization where at least some of the functions are operating around the clock. In Figure 17, it can be clearly seen that most of the incidents have reportedly occurred during the weekdays and on weekends the number of reported incidents was significantly lower. The two most common days in the reports were Tuesday (47 reports) and Wednesday (44) and both are in the middle of the week. Both Sunday and Saturday had less than 15 incidents reported, whereas Tuesday, Wednesday, Thursday and Friday all had at least 40 incidents reported. The number of incidents reported on Monday was between the weekend and other weekdays with a total of 34 incidents reported.

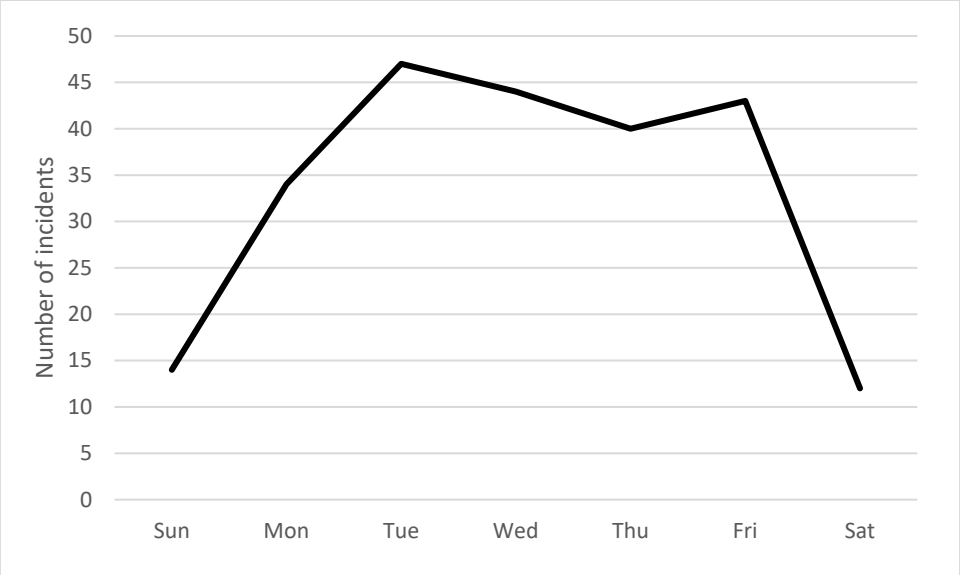

Figure 17. Information security incidents reported per day of the week

Reasons for the high number of incidents occurring on weekdays and not on weekends, or during the holiday seasons, are assumably related to the operation of the target organization. Most of the appointments are scheduled on weekdays and more employees are also working on weekdays. Additionally, work tasks that are related to IS such as configuration changes might have been performed during weekdays, as well. When more employees are at work, they might also have more time to detect and report this kind of incidents. On the other hand, these results tell that information security incidents have been occurred on weekends and

during holiday seasons as well, when the number of employees at workplace is presumably lower.

8.5 Descriptions of the incidents

One of the mandatory fields to be filled in the information security incident reporting template is the following field: *Write a description of the incident*. This field and the information written into it is a vital part of the incident reporting as it contains the reporter's description about what happened when the incident occurred. As seen in Figure 15, the reporter writes the description into an open text box and in free form, meaning that the description and its style depends on the reporter.

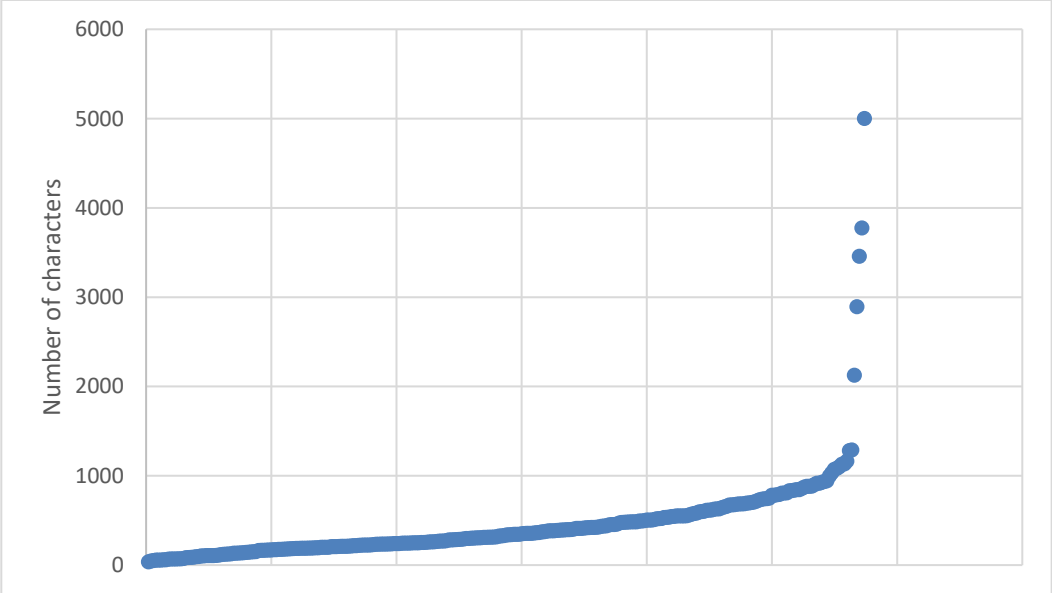

Figure 18. Number of characters in the incident descriptions

Figure 18 shows the number of characters written in the description of the incident reports in the research data. From the graph it can be seen that the majority (95 %) of the descriptions contained less than 1000 characters and in four incident reports the descriptions contained more than 2000 characters. At the minimum, the description contained 36 characters, and at the maximum 5001 characters. The median length of description was 337 characters and an average of 451 characters.

The shortest description in the research data was: "System X crashed in department Y". In this description the detailed information was replaced because of the confidential nature of the data and the "X" covers the name of the system and "Y" represents the name of the department. Another report with less than 100

characters in the description described: “X patients’ details were sent to department Y”, where X covers the number of patients and Y the name of the department where the patient details were (accidentally) sent in a physical form.

8.6 Example reports

In this chapter, five different information security incident reports are represented. These reports work for the following reasons. Firstly, this is the first time when such information security incidents reported in healthcare have been studied, and by examining these five reports an overview of the reported information security incidents in the research data will be given. Secondly, the reports show the variety among the incidents, their descriptions, and analyzations. Thirdly, the selected incident reports illustrate the connection between the description of the incident and the information provided by the analyst. In addition, the example reports show what information was provided by the reporter and what information was provided by the analyst of the incident report. Finally, these examples enable a discussion of the selected incident reports and provide information on how to increase cybersecurity in healthcare with developing incident reporting.

The example reports have been sorted by the length of the description of the incident. The first table describes an information security incident reported with a short description, the second table describes an incident with a median length description and the third and fourth tables show an incident with an average length description. The fifth table contains a significantly longer description of the incident than average. All tables contain three columns, the first column from the left describes who reported the information, the reporter or the analyst. This information tells what the reporter has reported about the incident and what information the analyst of the report has added into it. It should be noted that the analyst could have also edited the information filled in by the reporter and that there was no edit history available as to whether he or she has edited any of the information. The reporter instead cannot add information to the analyst’s fields.

The column in the middle of the tables describes the name of the field in the information security incident template. These fields are shown in Figure 15. The third column from the left finally shows the answer to the field provided by the reporter or the analyst. As some of the fields in the reporting template were open text boxes, where the reporters and analysts could write free text and other fields included preconfigured options to be selected, to improve the readability and to

ensure that the reader could separate the preconfigured options from the free texts, all free text answers in the tables have been shown inside quotation marks.

All the following descriptions of the incidents have been translated from the original language used in the reports into English. The names of the systems, departments, personnel and other information that could be used to identify the reporter or other data subjects has been anonymized and covered by capital letters. Hence, the reporter's department, the department where the incident occurred, date and time have not been included in these examples. If a field is empty in the table, it means that there was no information reported into this field.

8.6.1 Example report one

Table 13. Example report one

Person	Field	Reported information
Reporter	Description of the incident	"System X crashed in department Y"
	Nature of the incident	Adverse event
	Type of the incident	Software, device, or other malfunction
	Report a patient safety incident as well	No
	Reporter's view on how to prevent a recurrence of the incident	
	Why did it happen?	
Analyst	Information security category affected by the incident	
	Effects on data privacy	
	Conditions and other contributing factors	
	Estimated risk level	II
	Proposed measures to prevent a recurrence of the incident	Inform about the incident
	Write the proposed measure or justify why no action is required	
	Description of the implementation of the measures	"Z Devices act as a backup"

The information security incident report seen in Table 13 contains the shortest description of the incidents in the research data. Other information besides the short description reported were the nature and type of the incident that both seem to fit the description of the incident. As the System X crashed, the incident refers to an *Adverse event* and this can be related to *Software or device* -category. Additionally, a selection was made not to report a patient safety incident with this information security incident report.

In this example, what the reporter did not report was his or her own view how to prevent a recurrence of the incident, or why the incident took place. Both can be due to the lack of knowledge or information about the system and the IT-environment that can make it difficult to propose preventing measures or to guess

why the incident occurred. What is clearly missing from the description is the effect of the incident to the operation of the reporter's department or working duties. From this report it cannot be determined if the incident had for example a negative impact to the operation of the whole department, a limited impact to the reporter's work or no effect at all. When reporting a system crash only, this incident report seems more of a notification of a system availability than a report of an incident that had an effect on information security.

As seen in Table 13 the analyst of this incident had estimated the risk level at level II and proposed that *Inform about the incident* is an adequate measure to prevent a recurrence of the incident. For the description of the implementation of the measures the analyst had described that "Z devices act as a backup". Nevertheless, the analyst had not filled in the details to the following fields: *Information security category affected by the incident, Effects on data privacy, Conditions and other contributing factors* or *Write the proposed measure or justify why no action is required*.

The reason behind the missing information from the analyst can be due to the lack of information that the reporter had provided about the incident. Based on the reported details, it may have been difficult to fully analyze the incident and determine the details such as the effects on data privacy. However, it is unknown whether the reporter gave his or her contact details when reporting this incident and if the analyst had asked for more information about the incident.

8.6.2 Example report two

Table 14. Example report two

Person	Field	Reported information
Reporter	Description of the incident	"For several days employees from the upper floor have their printed papers going to the printer on our floor. The printed papers contain personal information. This does not seem to end even if the papers have been carried to the right floor and therefore, I report this incident."
	Nature of the incident	Near miss
	Type of the incident	Data confidentiality
	Reporter's view on how to prevent a recurrence of the incident	"There should be some kind of warning if one is selecting a printer which is not his/her "home printer""
	Why did it happen?	
Analyst	Information security category affected by the incident	
	Effects on data privacy	
	Conditions and other contributing factors	
	Estimated risk level	

Person	Field	Reported information
	Report a patient safety incident as well	No
	Proposed measures to prevent a recurrence of the incident	
	Write the proposed measure or justify why no action is required	
	Description of the implementation of the measures	

Table 14 contained the information of information security incident reported with a median length description. Besides the description, the report included the nature and type of the incident. In contrast to the previous incident report with a short description, this report also included the reporter's view on how to prevent a recurrence of the incident. Yet, the reporter had not answered the question *Why did it happen?*

As written in the description, the reporter had noticed that another employee or employees have printed papers containing personal information going to a wrong printer. The reporter had identified that these documents had been printed from another floor and that this was not the first time it happened. Additionally, the reporter told that printing papers to the wrong printer had not ended even if the papers had been carried to the right floor.

Compared with the incident seen in Table 13, the description of this incident is longer and in more detail. The reporter described what had happened, described a possible root cause of the incident and gave a development proposal that would prevent a recurrence of the incident. However, the description provides room for speculation and arouses several questions such as: How the reporter identified the origin of the papers or where did he or she take the papers.

If the incident is due to human error and there are, for example printers that have been named similarly, is it possible that this problem is wider and that there have been several persons who have printed accidentally to this "wrong printer", or to several other wrong printers? The reporter wrote that he or she had carried the papers to the right floor. Even if the reporter were right about the floor where the papers had been printed from, where exactly had he or she taken these papers? To someone's desk or next to another printer? Is it possible that the reporter of the incident had carried the papers containing personal information to a wrong place and risked the confidentiality by him or herself? If the reporter carried the papers from the wrong printer to the right printer, the person who printed the papers could think that everything is working normally, or that there is a delay before the papers are printed and continue the printing to the wrong printer.

The description did not tell how the reporter ensured the origin of the papers or if they are safe after leaving them on another floor. Furthermore, it remained unclear whether the reporter had identified the person who had printed these papers, or if there had been more than one person who had accidentally used the wrong printer. If the reporter would have had identified the person who printed the papers, assumably the most effective way to prevent a recurrence of the incident could be contact directly the person and tell him or her that he or she is printing papers that contain personal information to a wrong printer. The reporter did not tell if he had contacted anyone in the upper floor about the incident. As it was the reporter's last change to prevent a recurrence of the incident, the reporter fulfilled an information security incident report, instead.

As seen in Table 14, the only field where the analyst filled in information was *Report a patient safety incident as well* where the analyst selected option *No*. In other words, the analyst decided that there was no need to report a patient safety incident with the information security incident, and did not fill in any other details related to the incident. For example, the analyst did not estimate the risk level of the incident or propose measures to prevent a recurrence of the incident. Furthermore, the analyst did not take any consideration on the reporter's view on how to prevent a recurrence of the incident or what is the right thing to do if someone finds papers that have been printed to a wrong printer. Healthcare organizations can have lockable waste bins that are designed to keep confidential papers secure until destruction. If this kind of waste bin is in use and instructed to be used in these kinds of cases, the analyst could have contacted the reporter directly and give these instructions to him or her. If the reporter did not leave his or her contact details, the analyst could have contacted a wider group to instruct the employees.

The reporter had proposed that there should be a warning if a user is selecting other printer than his or her home printer. The analyst could need assistance from the IT-department or other service provider to consider this proposition, however, the analyst left empty the field where he or she should justify why no actions was needed. According to the report, the IT-department was not contacted about the case at all. Considering the papers contained personal information, the data protection officer in the organization should have been contacted.

In summary, in this incident report the reporter was clearly worried about the situation where sensitive information was frequently printed by a wrong printer. Additionally, the reporter was concerned that the incident would recur again in the future. The reporter had been trying to take care of the problem in his or her own way by taking the papers to the correct floor but without the desired effect. By

reporting the incident, the reporter asked for help to prevent a recurrence of the incident. Unfortunately, according to the information in the report the incident was poorly analyzed, and the analyst did not provide any help in the case.

8.6.3 Example report three

Table 15 describes an information security incident report with an average length description. In the description, an employee expressed his or her concerns related to used IT-devices. The person reported about a location at work where used computers and hard drives were stored without supervision and that there was a possibility that these devices could be accessed by outsiders. Furthermore, the reporter asked whether these devices had been erased or wiped in accordance with "security rules" because he or she was worried that these devices contain confidential information or patient details. At the end of the description, the reporter warned about the possibility that someone could take a hard drive and obtain access to confidential information.

Table 15. Example report three

Person	Field	Reported information
Reporter	Description of the incident	"There are used computers and hard drives in location X that can be accessed by anyone, even outsiders. Are these erased/wiped as they should be according to information security rules, or is there a possibility that these devices contain confidential information, even patient details? Anyone passing by could take a hard drive, put it into their pocket and restore the data."
	Nature of the incident	Adverse event
	Type of the incident	Data confidentiality
	Reporter's view on how to prevent a recurrence of the incident	"Data drives that are no longer in use should be erased and wiped immediately and stored in a locked place before final destruction"
	Why did it happen?	
Analyst	Information security category affected by the incident	
	Effects on data privacy	
	Conditions and other contributing factors	
	Estimated risk level	
	Report a patient safety incident as well	
	Proposed measures to prevent a recurrence of the incident	
	Write the proposed measure or justify why no action is required	
	Description of the implementation of the measures	

Besides the description, the reporter had reported the nature of the incident as *Adverse event* and the type of the incident as *Data confidentiality*. In the reporter's view on how to prevent a recurrence of the incident, the reporter wrote that devices that are no longer in use should be erased and wiped immediately and stored in a locked place before destruction. The field *Why it happened* was left empty.

Based on the description, the reporter was at least somewhat aware of IT and the risks related to information security. The reporter had identified that the devices in location X included hard drives, that are computer parts used to store data in a digital form. The reporter had also noticed that the location where the used devices were stored, for a shorter or a longer period of time, could be reached by other people not part of the organization. The reporter did not specify the *information security rules* that he or she was referring to, but the description signals that the reporter knows that data should be secured during its whole life cycle including the time after the use of the device and before its destruction.

In the reported case, the concern that the reporter raised was related to the possibility that someone could take a hard drive, put it into their pocket and gain access to confidential information. In such a case, the person will commit a crime if he steals a device and could be possibly face other charges as well, if the person would restore or process the data that has been stored on the device. However, the concern on accessing confidential data could be justified especially if there was a suspicion that the data on the devices had not been erased before storing them in the reported location. It is known that removing files from digital media will not destroy the data. There are tools available that can be used to restore files from hard drives and commercial services such as the company called Ontrack that has the ability to restore files even from physically damaged hard drives (Ontrack, 2022).

Interestingly, the nature of the incident was reported as *Adverse event*, even though there were no theft or theft attempt reportedly occurred. If the term *Adverse event* is understood as defined by Stakes (2006), as an incident that caused harm to a patient, the reported nature of the incident was incorrect. In accordance with the description, the correct nature of the incident would have been *safety observations / development proposals* as the reporter had made a safety observation related to the devices that have been stored insecurely and provides a development proposal to decrease the risks related to devices that are no longer in use which contain confidential information. The type of the incident was reported as *Data confidentiality*. Considering the possibility that the used

devices still contained confidential data, then the *Data confidentiality* was the correct term to describe the type of incident.

Granted that according to the report, the reporter had experience on IT and information security, but he or she failed to enter any information into the field *Why did it happen*. It would have been interesting to know whether the reporter knew why the devices were stored insecurely or why they would still contain confidential information. In any case, the reasons why the devices were there was not specified.

As seen in Table 15, the analyst did not provide any information on the incident report. For instance, the information security category affected by the incident could have been difficult to answer if there were no hard drives stolen. Yet, by following the description of the incident, categories such as *Physical* security or *Hardware security* or both could have been selected to describe the possible information security categories affected by the incident because the reporter had reported the location where used devices (hardware) were stored and could have been accessed by outsiders (physical security).

The effects on data privacy could have been difficult to determine because no theft or device misuse were reported. The description however strongly refers to data confidentiality and selecting the category *Confidentiality* could have been reasoned by the analyst. In this case, the conditions and other contributing factors could have provided interesting details such as what were the reasons behind the used computers and hard drives being stored in this location and if they did contain confidential information. However, this information was not written to the report by the analyst.

If the analyst did not have the information required, he or she could have requested additional information from another party such as the IT department or IT-service provider, and give them a chance to improve the operation and prevent a possible information security incident before it happens. It can be questioned whether the analyst had even the right to ask additional information about the incidents, which is also a duty in order to prevent information security incidents?

It is possible that storing used devices in the reported location could have been against the organization's rules and or against the agreement between the organization and its IT-service provider, for example. Nevertheless, according to the report, the analyst did not provide any information about the incident or how the situation could be improved. In addition, it remained unclear if any other party was informed about this information security incident report. If a hard drive would

have been stolen after the report and confidential data leaked to the public, what would have been the role of the report in the investigation and possible sanctions?

In summary, the example report three seen in Table 15 described an information security incident report where an employee had reported about an unsafe location to store used computers and hard drives and he or she was worried that the devices might contain confidential information that could be stolen. Parts of the report could have been categorized more accurately, however; the message was clear: used devices should be secured. The reporter also proposed practical ideas on how to improve the situation. However, the report was poorly analyzed, and the analyst had not specified any actions to improve the situation.

8.6.4 Example report four

Table 16 describes an information security incident report with an average length description. The description of the incident can be separated into four sections: Firstly, the reporter describes a situation where a system was offline because of a maintenance break, but the reporter was not informed about the break beforehand. Secondly, the reporter described that he or she could not find information about the maintenance break from the organization's intranet. Thirdly, the reporter described two different persons who were aware of the maintenance break and because of the break, one of them was using the backup system. Lastly, the reporter tells that the backup system did not fully work.

Table 16. Example report four

Person	Field	Reported information
Reporter	Description of the incident	"System X was down because it was under maintenance, but we had not been informed about it beforehand. There was no information on the intranet. We called to person A, he knew about the maintenance break. We took the backup system/device into use. Person B knew about the maintenance break and was already using the backup system, but we did not know about it. The backup system/device did not fully work."
	Nature of the incident	Near miss
	Type of the incident	Software, device, or other malfunction
	Reporter's view on how to prevent a recurrence of the incident	"Such important information should come to our notice at an early stage. There are no clear instructions available about how to proceed on such occasions."
	Why did it happen?	"Fortunately, nothing bad happened. However, in a case of emergency, we could have not been able to contact Person B because we did not know that he was using the backup system"

Person	Field	Reported information
Analyst	Information security category affected by the incident	Something else
	Effects on data privacy	
	Conditions and other contributing factors	No contributing factors identified, normal situation
	Estimated risk level	III
	Report a patient safety incident as well	No
	Proposed measures to prevent a recurrence of the incident	Inform about the incident
	Write the proposed measure or justify why no action is required	
	Description of the implementation of the measures	"Person C and Person D were contacted about the situation. There was information available about the maintenance break on the intranet. Considering the reporter's department, it would be better if they would be informed as department B was."

According to the first section of the description of the incident, there was an ongoing planned maintenance break for System X, but the reporter and his or her coworkers did not know about the break. As known, healthcare organizations have complex IT-environments with a great amount of different systems (Jalali & Kaiser, 2018) and it is known that IT systems need to be updated regularly to keep the system up to date, running, and secure. Therefore, reasons for this kind of maintenance break can be caused by software that needs to be updated or system that needs to be reconfigured, for example. Even though the harm from the maintenance breaks to the operation of the organization can be minimized by carefully planning the changes, some of the changes may require that the system is not used when the changes will be made and must be taken offline.

If a system needs an Ad-hoc update or reconfiguration, the system may have to be taken offline within short notice. In such a case, the information to the users of the system must also be provided in a short time accordingly. If the system is maintained and or configured by a third party, the maintenance break must be planned in cooperation with all relevant stakeholders.

According to the incident description, there has been a lack of communication between the reporter's work unit and the employees responsible for the maintenance break. Some of the users had been informed about the incident but due to one reason or another, this information was not provided to the reporter's unit. This signals that the communication on maintenance breaks should be improved to consider all relevant stakeholders.

As described in the description, the reporter could not find any information about the maintenance break from the organization's intranet. Because the reporter tried to find the information about the ongoing maintenance break from the intranet,

assumably maintenance breaks were usually informed via the intranet site. Besides the direct communication between the different stakeholders related to the maintenance break, by communicating about breaks via the organization's intranet, it could ensure that stakeholders with access to the intranet are able to find the information where direct communication has failed. As stated by the reporter, in this case both direct communication and communication via the intranet failed.

This information signals that the maintenance break was not carefully planned, and that the communication between the relevant stakeholders had failed. The target organization should revise the communication plan used in the maintenance breaks to ensure that all relevant stakeholders will be informed about upcoming breaks beforehand. If this communication fails, there should be a backup channel such as an intranet site that could be used to provide the information as well. It is important to ensure that the communication plan and information channels have been successfully communicated to the users, and that both the employees responsible for the communication and the end users are using the same channels.

For example, if employees have been told that a message about ongoing maintenance breaks will be shown on the intranet, then all maintenance breaks should be informed via the intranet. Otherwise, the employees can be confused if a system or several systems are offline without prior notification on the intranet. This can have a negative effect on the employees' work and lead to an overload of the IT-helpdesk when employees are trying to contact the helpdesk because of the problem. These problems could be avoided with proper communication between the relevant stakeholders. Therefore, communication is a crucial part of planning maintenance breaks.

In the third section of the description of the incident, the reporter informed that there were two persons who were aware of the maintenance break and that at least one of them was using a backup system. It remained unknown whether these two persons were informed about the maintenance break beforehand or if they had noticed or heard about it after the break started. The reporter himself or herself knew that there was a backup system available but was not using it because he or she did not know about the maintenance break. Again, proper communication regarding planned maintenance breaks could have ensured that all relevant employees would have been using the backup system during the break. The user must know when they should use the backup system, otherwise the value of the backup system can be limited.

Interestingly, the reporter ends the description by stating that the backup system or device did not fully work. This description indicated that there was a

malfunction or system error with the backup system that the reporter experienced when he or she tried to use it after learning that there is an ongoing maintenance break, and that other employees were using the backup system already. Nevertheless, the reporter did not describe the problem with the backup system in more detail. It is possible that the problem was due to a human error and caused by the user. If the use of a backup system has not been instructed properly, the users might not know how to use the system when needed. For this reason, the users should have been trained in using the backup system and this training should be renewed regularly.

In addition to the description of the incident, the reporter had selected *Near miss* as the nature of the incident and *Software, device or other malfunction* as the type of the incident. In the reporter's view on how to prevent a recurrence of the incident, the reporter wrote about two things: Firstly, "Such important information should come to our notice at an early stage" and secondly: "There are no clear instructions available on how to proceed on such occasions."

The nature and type of the incident seemed to be aligned with the description of the incident. It could be argued if the category *safety observation / development proposal* would have been more accurate for the nature of the incident as the potential harm and its severity from the incident was not clearly reported. Nevertheless, this can be difficult to estimate without proper knowledge of the operation of the organization and the reporter's unit. As written by the reporter in the field *Why did it happen?* The potential harm from the incident in case of an emergency could have caused a communication error between the reporter's unit and person B.

The analyst of the incident had selected *Something else* as the information security category affected by the incident. This selection was surprising because by selecting the category, the analyst analyzed that the correct category for this information security incident was something else than the categories available in the HaiPro system. When considering the lack of information about the maintenance break, the right category could have been the *Something else,* as none of the categories available refer to a lack of communication. Although, for the reported problem with the backup system, the right category could have been different depending on the problem with the backup device or system. Therefore, in this case there could have been several categories chosen for the information security categories affected by the incident.

For effects on data privacy, the analyst had not selected any category available and left the field as blank. As the description referred to a maintenance break which caused that the system was not available, the category *Availability* would have

been the correct category to be chosen when analyzing the incident. This could have been selected because the backup system also did not fully work. Additionally, *Usability* could have been chosen depending on the problem faced with the backup system or device.

The analyst had selected that there were no contributing factors identified and that the situation was normal. This selection could have been different, as the incident occurred because of a lack of information and communication before and during a system maintenance break. Selecting any other factor from the list could have been preferred. For example, *Unit working methods and procedures* could have been selected because of the lack of communication or the category *Training and orientation, competence* could have been selected for the same reason or if there was a lack of knowledge in the use of the backup system. The category *Communication and information flow* could have been selected because the information about the maintenance break did not reach the reporter before or during the break. Also, the *Equipment and supplies, tools and machines, information systems* could have been selected as the conditions and other contributing factors because the system was offline and there was an error with the backup system. Hence, it was difficult to find reasoning why the analyst had analyzed that there were no contributing factors related to the incident. Additionally, this example shows how one incident could have been reported in several different ways.

The analyst had selected *Level III – Moderate risk* for the estimated risk level of the incident which was the most selected risk level in the research data. As seen in Table 16, the analyst selected that there was no need to report a patient safety incident with this information security incident. For proposed measures to prevent a recurrence of the incident the analyst selected *Inform about the incident*. Considering the incident and its description informing alone could not have been enough to prevent a recurrence of the incident because the problems described signaled a lack of planning of the maintenance break and communication before and during the break. However, this selection can be justified when taking into account the actions described in the last row of Table 16 for the description of the implementation of the measures (to prevent a recurrence of the incident).

According to the description of the implementation of the measures, the analyst escalated this incident report to a higher level in the organization by contacting two persons mentioned in the original text, with at least one being a management level employee. This finding was interesting as the analyst selected for the proposed measures to prevent a recurrence of the incident *Inform about the*

incident and not *Escalate to a higher level or consult experts* that would describe more accurately the actions taken.

In contrast to the reporter's description, according to the analyst there was information available about the maintenance break on the organization's intranet. The analyst did not specify the origin of the information or whether the information was available beforehand or during the maintenance break. Nevertheless, there was a contradiction between the descriptions given by he reporter and analyst. If it was true that the information was available on the intranet, the description given by the reporter could be questioned and asked why he or she did not find the information when looking for it during the maintenance break?

Without evidence such as system logs or screenshots of the used communication channels and the information provided on the intranet about the maintenance break, it can be difficult to determine who was correct and what actions should be taken to prevent a recurrence of the incident. There were just two different opinions about the incident: Firstly, the reporter who was claiming that there was no information available on the intranet, and secondly, the analyst who was claiming that there was information available on the intranet. Considering that the analyst selected *Inform about the incident* as the proposed measures to prevent a recurrence of the incident, it would have been interesting to know what information was provided and to whom. Hopefully, the inform about the incident was more than providing a message to the reporter or his or her department that there was information about the maintenance break available on the intranet.

As shown in Table 16, the analyst left empty the field *Write the proposed measure or justify why no action is required*. In other words, the analyst did not specify the actions to be taken to prevent a recurrence of the incident. As claimed by the analyst in the end of the last field in Table 16; "*Considering the reporter's department, it could be better if they would be informed as the department B was"*. Even though it was noted that the information about the maintenance break was available on the intranet, it was admitted that the communication was lacking considering the reporter's department and that they should have been informed the same as another department (department B) was. Without specifying the actions that were taken or that will be taken to prevent a recurrence of the incident, this description signals that according to the analyst, it would have been better to improve the communication to the reporter's department, but it remained unclear whether any actions to do so were taken.

In summary, the reporter of this information security incident reported about System X that was not available because of a maintenance break. Nevertheless, the

problem was not the maintenance break itself but a lack of communication about the preplanned maintenance break, and that the reporter did not know about it beforehand. The lack of communication caused the reporter and his or her department not being prepared to use the backup system, nor were using it when the maintenance break started resulting in a communication problem with other healthcare workers who were informed beforehand who were already using the backup system. Additionally, the reporter could not find any information about the maintenance break from the organization's intranet. After the reporter had learnt about the maintenance break from another employee, he or she started to use a backup system. Reportedly, the backup system did not fully work. According to the reporter, nothing bad happened, but in a case of emergency the situation could have been different. The outcome of the analysis was that there was information available on the intranet and that the reporter's department could be informed in a way that another department was.

Overall, the information security incident report described in Table 16 contained more detailed information compared to the other report with an average description, or to the reports with shorter descriptions. This was the only information security incident report where all fields available for the reporter were fulfilled. The analyst of this report had provided more information to this incident report compared to the other example incidents. The analyst had however left two fields empty and therefore none of the example incident reports shown in the previous tables contain information in all available fields.

Despite the greater amount of information from both the reporter and the analyst compared to the other example reports, again the analyzation could have been better. When an incident that might reoccur has been reported, the analyst should be able to clearly describe what have been or what will be done to prevent a recurrence of the incident. It is difficult to see how a recurrence of the incident could be prevented by adding an analyzation to the incident report stating that there was information available on the intranet and that the communication could be better. It remained completely unclear why the backup system available for the reporter did not fully work, and if any actions were taken to ensure its functioning in the future. Furthermore, the analyzation did not take into consideration the reported lack of instructions available for the reporter on how to proceed in such occasions.

8.6.5 Example report five

Table 17 describes an information security incident report with a long description of the incident. As written by the reporter, the incident was caused due to incorrect

information in an information system that caused a delay to an operation for a patient. The description can be separated into three main sections; the first paragraph described the incident and its consequences; the following three paragraphs described the actions taken by the reporter and other employees to establish the scope of the incident and to mitigate its effects. The last two paragraphs contain a discussion about the reasons behind the incident and how to solve the problem permanently.

Table 17. Example report five

Person	Field	Reported information
Reporter	Description of the incident	"An admission note to operation X for a patient A was made in (Date and Time). For an unknown reason, information XB was saved into system Y resulting in the level of urgency for the operation X was lowered. Employee B called to the reporter to ask about operation X when the incident was detected. The reporter immediately made corrections to the information. The incident caused a three- and half-hour delay to the operation X. I have reported the incident and its cause to the patient information system and consulted employee C about it. Similar incidents seem to have been occurring several times during the past few weeks but not before that. Therefore, I decided to minimize the additional risks during my night shift and immediately consulted employees D and E, so they were aware of the possibility of the recurrence of the incident. In addition, I discussed with employee F about the incident and informed employees in department G if they could ensure the integrity of the information related to these operations. Solving this problem took time and resources from me when working in position Z. Yet, a possible temporary solution for fixing the problem was found by accident. According to my and Person B's observations, exactly during the past few weeks (but not earlier) there have been several times when information X had not been saved as XA into the system Y resulting in the level of urgency of operation X was lowered. These have been admission notes at least from the departments H and I, and the same personnel have successfully completed admission notes before. During the night shift, person B working as X, kindly demonstrated to me how to make the note into system Y from their point of view. The person making the admission note is not able to change or affect the urgency of the admission note in any way. When the admission note for operation X for a patient is

Person	Field	Reported information
		made one must select between options A, B or C. However, if one tries to change this option after the admission note has been made, the option will be changed to D. Employee K told that he noticed this phenomenon today for the first time and because he felt that the behavior of the system was strange, he changed the level of urgency as A from the option menu for the admission notes he had made. Also, Person L told that she had just noticed the option D for the first time and wondered about it as well. According to my, employee's B, and C understanding, there have been no informing of end users beforehand about possible changes in the system Y or its practices. This problem must be solved. The reason for this feature to change the level of urgency automatically as D when editing an admission note, is likely to prevent the person not to change accidentally the level that he or she has already chosen. Is there a possibility that this is a nonfunctional feature that has been implemented when installing an update to system Y? If one edits an admission note with option A and it automatically changes to option D, will the option remain as A and information X changes to XB? The person making the admission note cannot change this information and it is not even visible to the personnel working as M! I have urged the employees A, B and C to solve this problem temporarily in a way that they edit manually the admission notes with option D to contain the option A if they need to edit the admission notes (and to inform the persons in the morning shift as well). I will personally inform the supervisors in department C, so they can contact the right party to solve this problem permanently." *NOTE: To improve the readability, the original description was shortened. In addition, parts of the description were removed to ensure the anonymity of the data.*
	Nature of the incident	Adverse event
	Type of the incident	Software, device or other malfunction
	Reporter's view on how to prevent a recurrence of the incident	See the description above
	Why did it happen?	See the description above
Analyst	Information security category affected by the incident	
	Effects on data privacy	
	Conditions and other contributing factors	
	Estimated risk level	
	Report a patient safety incident as well	
	Proposed measures to prevent a recurrence of the incident	

Person	Field	Reported information
	Write the proposed measure or justify why no action is required	
	Description of the implementation of the measures	

In addition to the description of the incident, the nature of the incident was reported as *Adverse event* and the type of the incident was reported as *Software, device or other malfunction*. Both of these selections were in accordance with the description. For the reporter's view on how to prevent a recurrence of the incident and why did it happen? The reporter had written "See the description above" which refers to the description of the incident that discussed these matters. In other words, the reporter did not provide any additional information to these two fields because he or she had already written a long description of the incident including the discussion about how he or she thinks that the recurrence of the incident could be prevented and why the incident did happen.

As can be seen from Table 17, the description of this incident was long and comprehensive. Compared to the other example reports, the description of this incident was not just longer but included more detailed information about the incident such as a description of the actions taken by the reporter and other employees, as well as a discussion about the reasons behind the incident. Furthermore, the description showed how the reported had tried to solve the problem and prevent a recurrence of the incident that he or she knew that could have an effect on the patient by spending his or her time and effort and contacting several employees in the organization.

According to the description of the incident, the reporter had identified how and when the problem occurs in the information system. When editing the admission note, an unwanted change in data related to admission notes occurred and delayed an operation for a patient. The reporter found out that the same problem had occurred several times in the organization during the past few weeks, but not before. In the description the reporter presented a temporary workaround to prevent a recurrence of the incident and urged that a permanent fix was needed.

Taking into consideration the comprehensive description of the incident including a temporary workaround and recurrence of the incident, it was surprising that the analyst did not provide any information to the incident report. It is possible that this information security incident report was not analyzed by the time when the data sample was exported from the system. Yet, this incident was reported more than a year before the export. There were several information security incident reports in the research data that were reported later and included information

provided by the analyst. For these reasons it is unlikely that this incident report was not seen by an analyst.

Since the problem described in the incident description was in an information system, it is likely that the analyst of this incident should have contacted IT-personnel and or the service provider related to the information system. Contacting several parties to analyze the incident report can be slow and time consuming when considering that there can be several reasons that could cause unwanted results in information systems, and that the results can be different depending on the user's actions, used hardware, and software combinations. It is possible that this was not the only organization that had reported the possible configuration error to the service provider and if there are other organizations using the same system, the time needed for this process can be high.

Because the reporter had not separated the description of the incident into the fields available in the reporting template, it can make the analyzation of the incident slower and more difficult. The analyst of the incident report must find the answer to the question why it happened, or the reporter's view on how to prevent a recurrence of the incident from the long description. Creating statistics from the description may be difficult, as well compared to the situation where the reporter has reported the incident as instructed by the reporting template. Even though the incident report could have been improved by considering the fields in the reporting template, it does not explain the missing analyzation of the incident.

It would have been interesting to read the analyzation of this incident report and to see what the estimated risk level of this incident was, for example. Also, as mentioned in the incident description, the incident caused a delay to an operation for a patient. Therefore, it would have been interesting to see whether the analyst decided to report a patient safety incident with the information security incident or escalated it to a higher level. According to the information security incident report, a separate patient safety incident was not reported.

Overall, the information security incident described in Table 17 included the longest description of the incident. The description was detailed and showed how the reporter himself or herself had spent time and effort to solve the problem. The description also provided comprehensive information about the incident that could be used to analyze and to prevent a recurrence of the incident. Despite the description, this information security incident report was not analyzed, or the information provided by an analyst was missing. It remained unclear whether reporting this incident had any effects in the organization.

8.6.6 Summary of the example reports

The main observation from these examples was the poor quality of analysis of the information security incident reports. In addition, it was noted that even though the quality of the original incident report varied, it did not affect the quality of the analysis, nor the length of the description of the incident. The quality of the analysis was poor in general, and it remained unclear whether any actions were taken to prevent a recurrence of the example information security incidents.

The example reports showed the variety among the information security incidents and the incident reports in the research data, as well. Whereas one report described just a system that was not working as seen in Table 13, the other report described a recurring human error as seen in the Table 14. In the example report three in Table 15 an employee reported risks that he or she had noticed in the operation of the organization related to processing and storing of used IT-devices and in Table 16, an incident related to a lack of communication about a system maintenance break was reported. The last example report seen in Table 17 showed an incident related to an information system used in patient care that provided different results than earlier.

The variety was not only among the information security incidents and the incident reports, but in the analyzation of the incident reports as well. At worst, there was no information provided by the analyst as seen in Table 15 and Table 17. At the minimum, the analyst had only provided information that there was no need to report a patient safety incident report with the information security incident report, and left all other fields empty, as seen in Table 14. In Table 13, describing the incident report with the shortest description, the description provided by the analyst was also short, stating that informing about the incident is an adequate measure to prevent a recurrence of the incident because there is a backup system in case the reported system is not available.

From these example reports, the information security incident report seen in Table 16 contained the highest amount of information provided by the analyst and was the only example report that described actions that were taken by the analyst. Nevertheless, the analyst had not provided information into all available fields on the reporting template leaving two fields empty. Additionally, the actions described by the analyst did not clearly state whether the operation would be improved to prevent a recurrence of the incident or not. It was stated that the operation should be improved, not that it will be improved or that the analyst will do something about it.

The example reports showed information security incident reports with a low amount of information, and that the reporter had not provided information in all fields on the reporting template. Even though the length of the descriptions varied significantly, short descriptions did not necessarily mean that information was missing or that the description was lacking. Even so, according to the example reports, the analyzation of information security incident reports was lacking overall. The information provided by the analyst was often minimal or missing. The example reports contained information that could have been used to improve the operation and to prevent a recurrence of the reported incident. However, the example reports did not contain any evidence of actions that would have been taken to do so.

When considering the variety among the incidents, incident reports and the analyzation shown in the previous examples it is difficult to define a common type of information security incident report or a general analyzation of an information security incident report. The incidents and the quality of the reports varied and so did the analyzations, and their quality. Therefore, the example reports offered only a brief introduction to a few information security incident reports in the data sample. To provide a more detailed view to the statistics of the reports, the following chapters describe quantitative data related to all information security incident reports in the research data.

8.7 Reporter's department

Figure 19 shows the department of the employees who had reported information security incidents. As seen in this pie chart, the incidents originated from several different departments. The total number of different departments in the sample data is 63. The large number of departments that had reported information security incidents, signals that these kinds of incidents have been noticed and reported in several different departments within the organization. This finding was expected when taking into account that the healthcare sector is dependent on IS and cybersecurity.

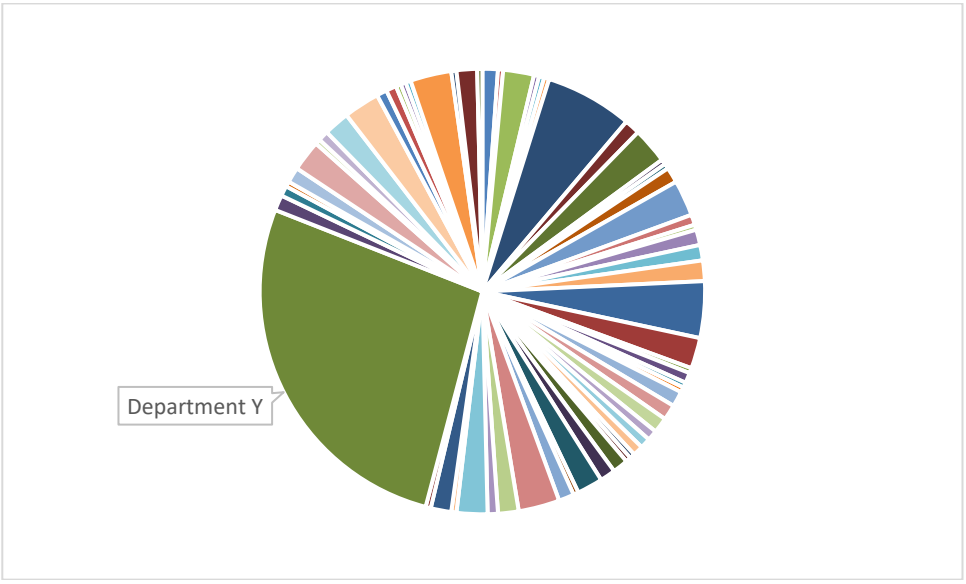

Figure 19. Reporter's department of information security incidents

Even if the total number of departments that had reported incidents was high, many of the departments had reported few incidents. From the 63 departments in the research data, a total of 45 (71%) had reported three or less incidents and 22 units (35%) had reported only one incident. A total of three departments had reported more than ten incidents. Therefore, the average amount of information security incidents per department was low.

Nevertheless, as seen in Figure 19, a total of 72 (27 %) of the reports in the sample data were reported by one single department. For anonymity reasons, this department is called *Department Y*. The reasons behind the high number of incidents reported by *Department Y* can be related to its operation that is focused on processing a high amount of patient data. The operation of this kind of department can include several functions related to confidential information such as controlling the availability, usability, storing, and disposal of patient information.

Even though over a quarter of the reports originated from *Department Y*, the department where the incidents were reportedly occurred varied. From these 72 incidents reported by *Department Y,* only 15 (21 %) reportedly occurred in *Department Y*. In fact, the 72 incidents included 25 different departments where the incidents had reportedly occurred. This means that *Department Y* had reported several incidents related to information security that had occurred in other departments in the organization. Again, this can be due to the operation of the department that can include the potential to notice and report incidents related

to information security that have occurred elsewhere in the organization when processing patient data.

For example, the incidents would have been reported after being noted by *Department Y,* and not in the department where it occurred. It is also possible that the department where the incident occurred shared the information with *Department Y,* who then reported the incident. The reasons for this kind of action could be related to the incident reporting culture where *Department Y* has a role in patient safety incident reporting in the organization.

The most common incident type in these 72 reports, reported by *Department Y,* related to confidentiality of information. Interestingly, there were only three incidents that reportedly occurred in *Department Y* but were reported by other departments. It would have been reasonable to expect that because of the nature of the operation of *Department Y,* there were more incidents that reportedly occurred in this department but were reported by other departments. The nature of the operation of *Department Y* can be organized in a way that it is not transparent to other departments, and therefore it is not likely that other departments could identify information security incidents that occurred in *Department Y,* or that the other departments in the organization trust that *Department Y* will report incidents that occurred in the department.

Despite the fact that the number of departments included in the research data were high, it was somewhat surprising that departments such as the department responsible for IT had reported only one information security incident during the more than three-year period. Furthermore, besides *Department Y*, most of the departments included in the research data were different types of nursing departments that provided a specialized area of care including the intensive care department and dialysis services department. These kinds of nursing departments are, of course, a vital part of the operation of a hospital, but in a hospital district there can be several other departments as well, from the cleaning services department to the financial department.

Cleaning services could have noted, for example, improper dumping of patient data that is known to have happened before in healthcare (Alder, 2015; Brown, 2018) and the financial department could have noted phishing emails, fake invoices, and other financial scams that cybercriminals are known to use against organizations and individuals. Even so, in the research data there were no incidents reported by these departments, even if it is likely that information security incidents take place also in other departments.

8.8 Departments where incidents reportedly occurred

In the research data, the information security incident reports include details of two departments, the department of the reporter and the department where the incident occurred. Whereas the previous chapter analyzed information about the reporter's department and this chapter considers the department where the incident reportedly occurred.

One could think that an employee notices an information security incident in his or her working department and then reports the incident. In such a case, the reporter's department would be the same department where the incident also occurred. Nevertheless, according to the results, the department that reported the information security incident was often different than the department where the incident reportedly occurred. In fact, out of a total of 162 incidents (41 %), the incidents reported occurred in a different department than the reporter's own department. In other words, it was more likely that the information security incident had been reported by a different department than where it actually occurred.

An example of this type of case would be when an employee notices that the information on two patients has been mixed up by another department. After the employee notices this, he or she reports the information security incident and becomes the reporter of the incident, using their own department, and another department as the department where the incident occurred. When considering the possibility for human errors, and that the previous studies have noted the under-reporting and miscoding of the incident reports in HaiPro (Jylhä et al., 2016; Syyrilä et al., 2020.), it is also possible that the reporter had chosen the wrong department into either selection when reporting the incident.

As mentioned in the previous chapter, the research data included only one information security incident that was reported by the IT-department. This incident was also reported as occurred in the IT-department. When considering the nature of the IT-department that includes managing information systems and services, the IT-department is likely to confront information security incidents.

This was supported by the research data that contained 25 information security incidents (9 %) that reportedly occurred in the IT-department. However, all reports except the one reported by the IT-department were reported by nursing departments. Eight of these incidents were reportedly caused by a network interruption, meaning the incidents occurred because of the IT-network or what is more likely, a part of the network was down or interrupted.

It is possible that the whole network would have been down but hence all of these incidents reportedly occurred on a different day. There were no other incidents reported that had occurred on the same day and was caused by a network interruption. It is more likely that the incident was caused by a local network problem because of the organization wide network interruption. If the organization's whole IT-network would have been down, there would have been more than one incident reported during the day.

The most interesting finding from the incidents that reportedly occurred in the IT-department, was the fact that the nursing departments had reported information security incidents related to network problems and reported that these incidents occurred in the IT-department, not in the reporter's own department. In these cases, it can be questioned if the department where the incident occurred were reported correctly. If the incident was caused by a problem in the IT-network, did it truly occur in the IT-department? And, if the incident was caused by a problem in the local IT-network did it in fact occur in the reporter's department, not in the IT-department? In real life, the IT-department can be far away from the physical location where the incident happened.

It can be difficult for an employee working outside the IT-department to know what the extent of the problem was, for example in the cases where the IT-network is not working properly. Again, this task can be even more difficult if the employee has a limited technical knowledge. Nevertheless, when considering reporting information security incidents, and that together these reports could form a picture of an incident and its impact to the operation in the organization, it is important that the reporter reports the incident based on his or her own observations. If the network problem such as a broken or misconfigured network switch had a negative impact on the reporter's department, it should be reported to have occurred in the same department. At the same time, there can be several other departments unharmed because their network connections were provided via other network switches. Improving cybersecurity awareness and knowledge among employees can help, but it is also important to have proper instructions that include examples about how to identify the department where the incident occurred.

8.9 Nature of the incidents

When reporting an information security incident via HaiPro, the reporter must report the nature of the incident. Figure 20 shows the percentage of different types of nature of incidents reported in the research data. In the data sample, a total of

257 (94 %) of the reports included this information. The most common nature of the incidents was (*patient safety) incidents*, that have caused or might have caused harm to the patient (Stakes, 2006) with a total of 121 incidents (44 %) reported.

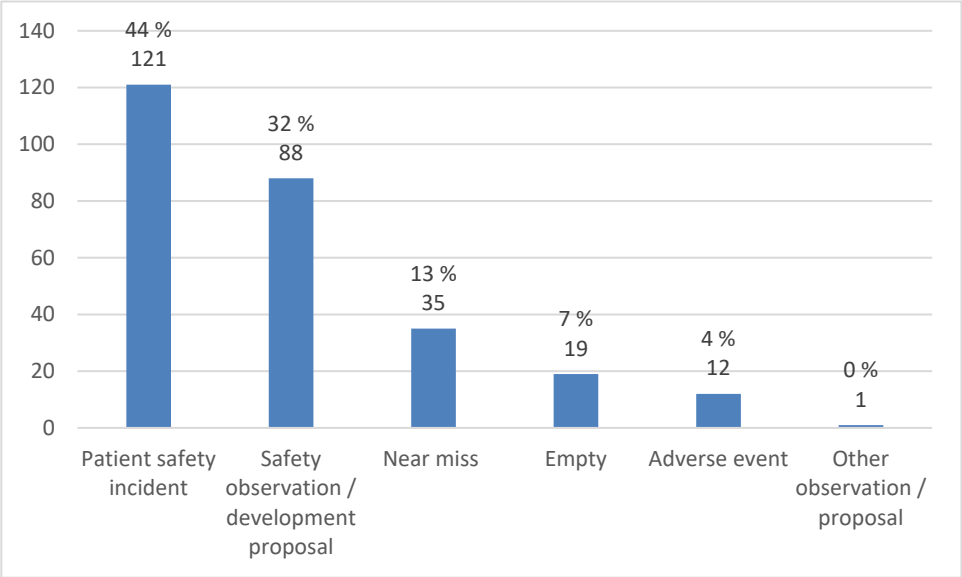

Figure 20. Nature of information security incidents

The second most common nature of the incidents was *safety observation / development proposal* that was included in 88 reports (32 %). *Near miss* was reported in 35 incidents (13 %). *Near miss* is an incident that has the potential to cause harm to the patient, but the harm was prevented whether intentionally or accidentally (Stakes, 2006).

In 12 reports (5 %), the nature of the incident was reported as *Adverse event* meaning that the incident caused harm to the patient (Stakes, 2006) and one incident was categorized as *Other observation / proposal*. In 17 incidents (6 %), the information about the nature of the incident was missing. Again, the reason behind the missing information was unclear and it remained unknown whether the data was missing or was not reported. It was not known why selecting the nature of the incident was not mandatory when reporting an information security incident.

The results described in Figure 20 show that even if the number of information security incident reports was high, the number of cases that according to the reported nature of the incident caused harm to the patient was low. In other words, and as seen from Figure 20, most of the information security incidents in the research data did not necessarily cause harm to the patient. Because of the high

number of incidents reported as *Patient safety incident,* it is still possible that the number of cases related to a harm caused to the patient was higher.

The high number of *safety observations / development proposals* hints that the reporters have observed information security related operation in the organization, and that the reporters do not report about incidents only but gave development proposals as well via the HaiPro system. As there were 35 incidents reported as *Near miss,* it was certain that there have been cases where an information security incident has been close to cause harm to the patient. Nonetheless, the most striking observation to emerge from the data was the total of 12 information security incident reports reported as an *Adverse event,* that were directly related to harm caused to a patient. This result is interesting and shows a connection between information security incidents and patient safety. According to these results, information security incidents have affected patient safety.

8.10 Types of the incidents

Figure 21 shows the types of information security incidents in the research data. From Figure 21 it can be seen that a total of 156 (57 %) of the information security incidents were reportedly related to *Data confidentiality*. Therefore, *Data confidentiality* related incidents formed more than half of all information security incident reports whereas the remaining data (120 incidents, 43 %) included several different types of incidents.

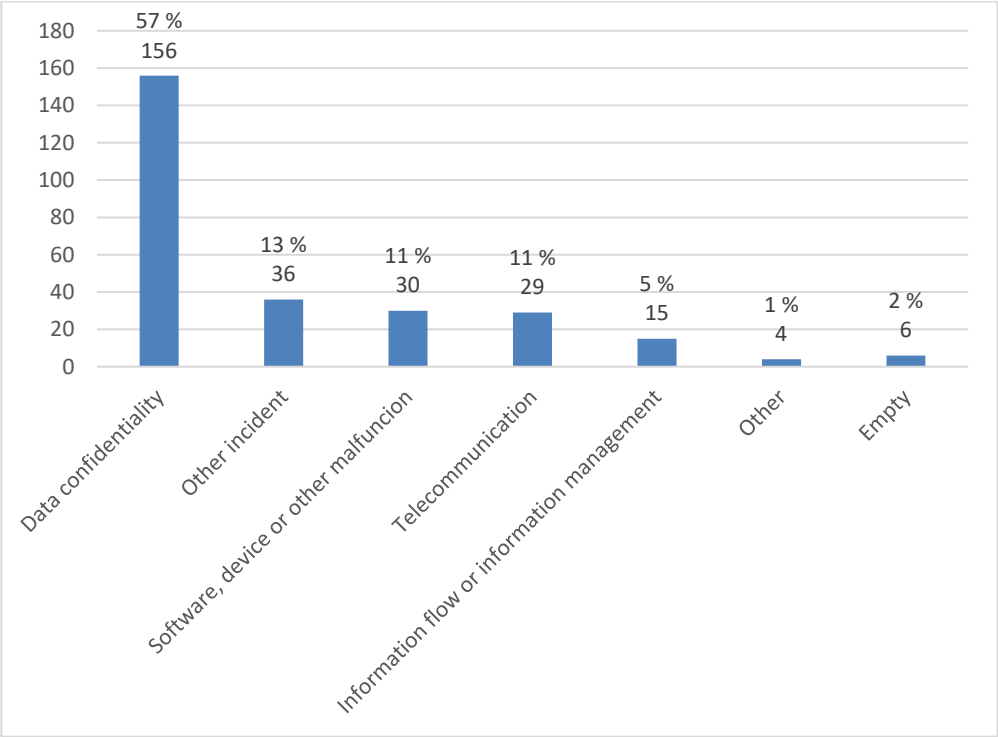

Figure 21. Types of information security incidents

The other reported incident types included *Other incident* that was selected as a type of incident in 36 reports (13 %). *Software, device or other malfunction* was selected in 30 incidents (11 %) and *Telecommunication* was reported in 29 incidents (11%). *Information flow or information management* was reported in 15 incidents (5 %). In six incidents (2 %), the information on the type of the incident was missing and in four incidents (1 %) the type of the incident was reportedly other than the types mentioned above. When compared to the other field on the reporting template, the type of the information security incident was often reported and in only a few incident reports, the type of the incident was missing. As seen in the following chapters information missing was often more common.

From a total of 156 information security incidents where the type of the incident was reportedly *Data confidentiality, a* total of 66 incidents (42 %) were reported by *Department Y*. When comparing the total amount of information security incidents reported by this department (72 incidents, 27 % of all reports), it can be seen that the majority (92 %) of the incidents reported by *Department Y* were classified as *Data confidentiality*. The remaining six incidents reported by *Department Y* included three *Software, device or other malfunction* incidents, one *Telecommunication* incident, one classified as *Other* type of incident, and one incident where this information was missing. Neverthelsss, it is important to note

that even without any of the incidents reported by *Department Y, Data confidentiality* was the most reported type of information security incidents in the data sample.

8.11 The view of the Reporter on how to prevent a recurrence of the incident

From the 275 information security incident reports in the research data, 125 reports (45 %) included an answer to the question; *How can we prevent this kind of event (in my opinion)?* In more than half of the incident reports (55 %), the reporter had not provided any answer to the question. Even though the field was left empty, the reporter could have answered the question in other fields on the reporting template such as describing the answer in the description of the incident.

For instance, as seen in example report number five, the reporter had written a long description containing his or her view on how to prevent a recurrence of the incident, but had not provided this information into the field called *How can we prevent this kind of event (in my opinion)*. Into this field the reporter had written: "*see the description above"*, instead. As mentioned earlier, it can be difficult to find the correct information or get statistics from the incident reports if the information about the incident has not been correctly reported as requested by the reporting template. Therefore, the proper way of filling in information about information security incidents on the reporting template should be instructed to all users and monitored.

When analyzing the answers from the 125 reports containing data in this field, three most common categories were identified. These categories were: verifying information and being more careful, forbidding ways of working and lastly, improving the digitalization. Verifying information and being more careful was mentioned in 43 incident reports (16 %). In 16 incident reports (6 %), the reporter referred to the ways of working should be forbidden such as writing information on physical notepads, and in 14 incident reports (5 %) the digitalization and better and more efficient use of IT-systems was seen as the key to prevent a recurrence of the reported incident. Figure 22 shows the number of incidents in these categories.

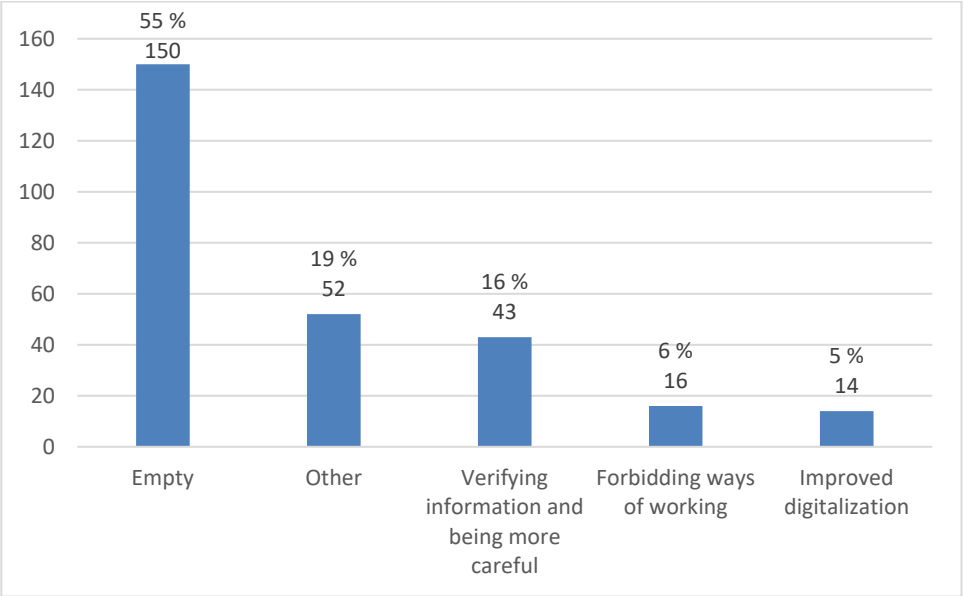

Figure 22. The view of the reporter on how to prevent a recurrence of the incident

Interestingly, the verifying information and being more careful was not emphasized on the other fields on the reporting template, as seen in the following chapters. For example, conditions and other contributing factors were often left empty or reported as unknown, instead of emphasizing factors such as training or working methods or procedures in the unit. On the other hand, this result can provide more information about the reasons behind the incident reports and also the reason for their occurrence.

Forbidding ways of working in the organizations indicated that the reporter had identified ways of working that are risky and have already led to an information security incident, that remain in use. To improve the operation of the organization, and to prevent a recurrence of the incident, this kind of information could be valuable. Nevertheless, as seen in the example reports, there is no evidence supporting the reported improvement suggestions have had any effects in practice. The request of digitalization and improving the use of IT-systems can refer to the situation where the reporters have seen that even though the healthcare has been digitalized rapidly during the past few decades, there are still processes and ways of doing things that could be digitalized and improved by using IT-systems more efficiently, and in this way a recurrence of the information security incidents could be prevented.

The remaining 52 incident reports (19 %) contained several different views on how a recurrence of the incident could be prevented that did not fall into any of the categories mentioned. Whereas most of these views were neutral or optimistic

about how the recurrence of the incident could be prevented there were few views that expressed frustration from the reporter. For example, in one incident report, the reporter wrote that "*I don't know (how to prevent a recurrence of the incident) because I have tried to inform about the incident via HaiPro*". The other reporter wrote "*In my opinion the root cause (of the incident) should have been established properly. The problem in the system must be fixed. The person representing the service provider had a significant lack of competence and the answer I got from him was frankly stupid*". Another reporter wrote "*I have learned that even colleagues cannot be trusted*".

As seen in Figure 22, most of the incident reports in the research data did not contain the reporter's view on how to prevent a recurrence of the incident. However, from the reports containing this information, three categories were identified. These categories provided information on the information security incidents and how their reporters saw that the incidents could be prevented. This information could be used to improve information security incident reporting, for example by creating a classification based on the categories and to improve the instructions related to information security incident reporting.

If all incident reports in the research data had contained the reporter's view on how a recurrence of the incident could be prevented, it would have been interesting to see how many of the incidents would have fitted into these categories. This could be tested with another data sample obtained from another healthcare organization in future studies and if implemented into the HaiPro system, the number of incidents falling into these categories could be monitored and it could provide more information on the information security incidents and how to prevent them.

8.12 Why did it happen?

Out of the 275 information security incident reports in the research data, a total of 181 reports (66 %) contained an answer to the question *Why did it happen?* On the contrary, in 94 incident reports (34 %) this field was left blank. After analyzing the answers, it was revealed that in a total of 27 incident reports (10 %), the reporter did not know why the incident happened. Whereas some of these answers contained only a question mark or text: "I don't know", the others outlined several possible reasons why the incident occurred but were still unsure whether any of these were the real root cause of the incident. Taking together, after an analyzation the total number of answers that were not sure why the incident happened or where the answer was left blank was 121 incidents (44 %).

Figure 23 shows the number of information security incident reports per category that were identified from the answers in the research data. When answering the question *Why did it happen?* The reporter can write text in an open text field and therefore the answers did not contain any preconfigured categorization. As seen from Figure 23, the most common category identified was *N/A,* and the second most common category was *Human error*.

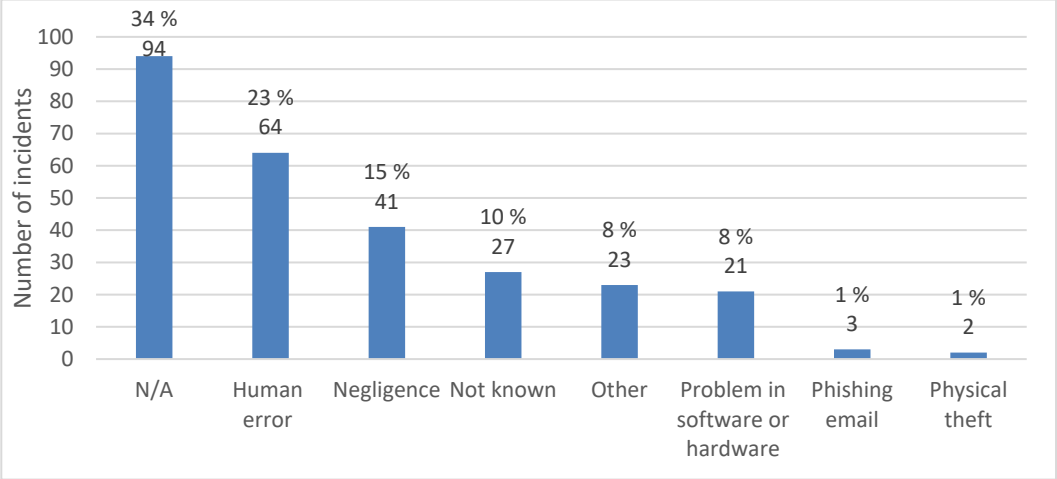

Figure 23. Why did it happen?

The term *Human error* in this context was separated from term *Negligence* as discussed by David H. Sohn (2013) in his paper, Negligence, genuine error, and litigation, that focused on the differences between different types of negative events in the health system. Sohn emphasized the importance of understanding the difference between negligence and other concepts such as human error. Whereas negligence is an incorrect decision, human error is not a decisional error, and therefore is not negligence (Sohn, 2013). A real-life example of negligence would be when a driver runs a stop sign causing a collision, whereas an example of a human error would be when a driver forgets to set a park brake in his car causing a collision. In both cases, there can be injuries from the car collision, but the type of event would be different.

An example of negligence that Sohn used in a medical context was a case where a patient was given an antibiotic, but the physician neglected to check the chart that would have stated that the patient was allergic to the given antibiotic. A human error would occur if a physician would have been mistaking “1.5 mg” for “15 mg” when administering medication. Sohn recalled that only a few cases in medical malpractice are due to negligence, whereas most of the medical errors are due to unavoidable human error (Sohn, 2013).

In the research, data human error was mentioned in 64 answers (23 %). Some of the reporters mentioned reasons behind the human error such as hurry, stress, and high workload. One reporter highlighted that it was "*hunger"* that was behind the information security incident related to a human error. Negligence was identified in 41 incident reports (15 %). This finding supports the idea of a lower number of incidents related to negligence versus human error. Nevertheless, there were more than a few information security incidents that reportedly occurred due to negligence, more than due to other categories identified from the reports such as a problem in software or hardware. This result arouses the question as to whether information security incidents have been reportedly occurring more often due to negligence than medical errors? Additionally, if negligence plays a bigger role with information security incidents than with medical errors, the reasons should be carefully studied. Negligence on the given instructions was mentioned as well as "*hurry"* and "*prioritizing urgent work duties"* such as clinical operations. One reporter wrote that *"negligence was due to the persons' own interest"*.

A problem in software or hardware was mentioned in 21 incident reports (8 %). Most of these answers referred to a system update or system changes. One reporter had reported *"A system malfunction"* and another reporter wrote *"Technology failed"*. Interestingly, the number of incident reports reportedly occurred due to this category was low when considering the amount of different systems and hardware that are in use in modern healthcare. Assumably, updates and changes of vast amount of systems could have provided a high number of incident reports related to this category as well. Even so, it must be considered that this category was identified based on the answers in the research data and was not a preconfigured categorization available for the reporters of the incidents. The number of incidents reportedly occurred due to a problem in software or hardware could have been different if this kind of categorization was available in the HaiPro system.

The last category identified based on the answers in the research data was phishing emails that was mentioned in three incident reports (1 %). Phishing emails are scam emails made by criminals to trick their victims for example to visit a malicious website or to steal personal information such as bank details (National Cyber Security Centre of United Kingdom, 2022a). Even though the number of answers related to phishing emails in the research data was low, this finding reveals that there have been reported information security incidents occurring in a healthcare organization that have been due to actions of cyber criminals.

In addition to information security incidents that reportedly occurred due to adverse cyber events, two incidents (1 %) were reported as occurred because of physical thefts and burglaries. This finding shows that even though information security and cybersecurity are often linked to electronic systems and services, there have been information security incidents reported in healthcare that have taken place because of adverse actions in the physical world, and not something happening inside computers or software only. Nonetheless, the number of reported burglaries in the research data was low, and it was not known whether the employees in the target organization were instructed to report all physical thefts related to information security via the HaiPro system, or if there was another process for reporting this type of event available. It is possible that information security has been seen to be linked with IT systems and services, whereas burglaries that are taking place in the physical world have been seen more of a physical security issue and not as information security incidents.

Incident reports that did not fall into any of the categories mentioned were categorized into category called *Other*. The total number of incident reports in this category was 23 reports (8 %). The answers to the question *Why did it happen?* included detailed descriptions about the incidents pointing to a specific process or service in the target organization or in a third-party organization. As the latest incident reports in the research data were dated in 2021, the Covid-19 pandemic was also mentioned in the data. In one report, the incident was reportedly caused because of furniture.

8.13 Information security category affected by the incidents

When analyzing the information security incident reports, the first field to be fulfilled is to select a proper information security category affected by the incident. Figure 24 shows the category of information security that was reportedly affected by the incidents in the data sample. Even though the type of the information security incident was often reported, the information security category affected by the incident was often not selected. This can be seen in Figure 24 where the category N/A (Not Available) contained a total of 122 incidents (44 %).

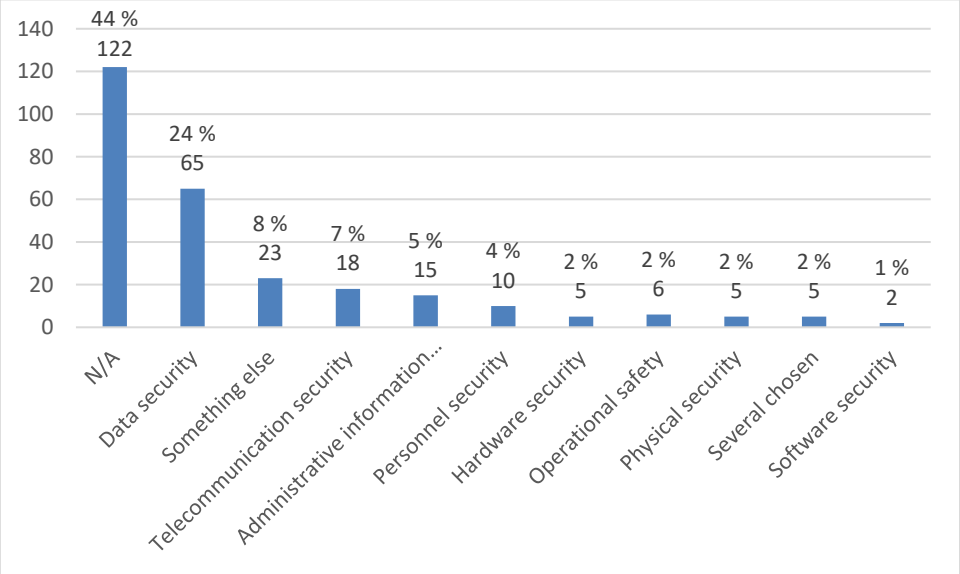

Figure 24. Information security category affected by the incidents

The origin of the used categorization remained unknown, however similar categorization has been described in the VAHTI-instructions for Finnish public organizations from VAHTI. For example, in a publication called "*Tietoturvallisuus ja tulosohjaus - Information Security and Performance Management*" from 2004, it has been described as a commonly used categorization for information security (VAHTI, 2004).

The reasons for selecting the type of the incident but not the information security category affected by the incident, can be many. One reason for not selecting any of the categories can be related to the used categorization. Whereas the categories for reporting the type of the incidents can be easy to understand and even descriptive for personnel who are not technology oriented, the categories for information security that was affected by the incident can be more difficult to identify. For example, terms such as *Operational safety, Software security* or A*dministrative information security* can be unfamiliar for many. When reporting the incident, the reporter may not choose any of the categories available, if he or she sees several options that are not familiar or self-descriptive.

Another reason for the high number of reports in the N/A category can be related to an unclear or misunderstood process of reporting. and analyzing the information security incidents. It is possible, that selecting the categories has been viewed as the duty of the analyst and therefore left unselected by the reporter, which has resulted in reports with missing information that are difficult to analyze. These scenarios, and missing data signal, suggest a lack of education and instructions when reporting information security incidents. Therefore, the

instructions for reporting and analyzing information security incident reports should be revised.

As seen in Figure 24, the most reported information security category affected by the information security incidents was *Data security* with a total of 65 incidents (24 %). The research data did not include information how the reporter or analysts behind these incident reports understood the term *Data security* or whether it was selected, because it is a general term that refers to information security.

In the TEPA Term Bank that is a free-of-charge term bank containing special language terms and definitions and maintained by the Finnish Terminology Centre, describes the term *Data security* and its Finnish counterpart *Tietoaineistoturvallisuus* (the term used in the HaiPro system), as an equivalent to the term *Information security* (TEPA, 2022). As seen in Figure 15 presenting the HaiPro information security incident reporting template, the term *Data security* is used to describe the reporting template itself.

In addition, the Australian Cyber Security Centre's Cyber Security Terminology describes the term *Data security as "Measures used to protect the confidentiality, integrity and availability of data."* (ACSC, 2022) and can be seen as equivalent to the term *Information security* as well, as it contains the classical CIA triad. According to these references and the HaiPro system itself, the term *Data security* is equivalent to the term *Information security*.

If the term *Data security* is equivalent to the term *Information security,* the categorization used in the HaiPro system to report the information security category affected by the information security incident seems to be confusing. Considering the two terms *Data security* and *Information security,* the most common information security category affected by the information security incidents was *Data security* which has been described as *Information security*. In other words, the most affected information security category affected by the information security incidents was in fact equivalent to *Information security*. Therefore, it is difficult to see why the option *Data security* was available in the HaiPro system and what value could be added by selecting it when describing the effects of the incident on information security. The current categorization used in the HaiPro system, its necessity, and relevance should be revised.

The third most common category was *Something else* with a total of 23 (8%) incident reports. The name of this category refers to the information security category affected by the incident that was seen as something else than the categories available in the HaiPro system. The fourth most common category *Telecommunication security* contained a total of 18 (7%) incidents. As seen in

Figure 24, the rest of the categories contained 15 incidents or less (5% or less) and the differences between the number of incidents in these categories were low.

Overall, a total of 210 incidents (79 %) contained no information about the information security category affected by the incident or the category was reported as *Data security* that is equivalent to the term *Information security* or reported as *Something else* than any of the categories available. According to these results, in most of the cases the information security category affected by the incident was not selected or the value of the selected category was limited. The used categorization is confusing and should be revised. Proper instructions and clear examples of the use of the categorization should be provided. Because the value provided from the current categorization is low, updating the categorization or removing it from the HaiPro system should be considered to improve the quality of the incident reports and to make the reporting process clearer and more consistent.

8.14 Effects on data privacy

Figure 25 describes the effects of the information security incidents on data privacy. Each bar in Figure 25 represents the number of incident reports per category. The first number above the bar tells the percentage of incident reports in the category, and the second number tells the number of incident reports in the category. As seen in Figure 25, the categorization used with the HaiPro system to report the effects of information security incident on data privacy follows the classical CIA triad (Samonas & Coss, 2014) that includes protection of *Confidentiality*, *Integrity* and *Availability* of data. Additionally, the used categorization included the following categories: *Usability*, *Several chosen* (if several previously mentioned categories were selected) and *N/A* (Not Available) meaning that no categories were selected.

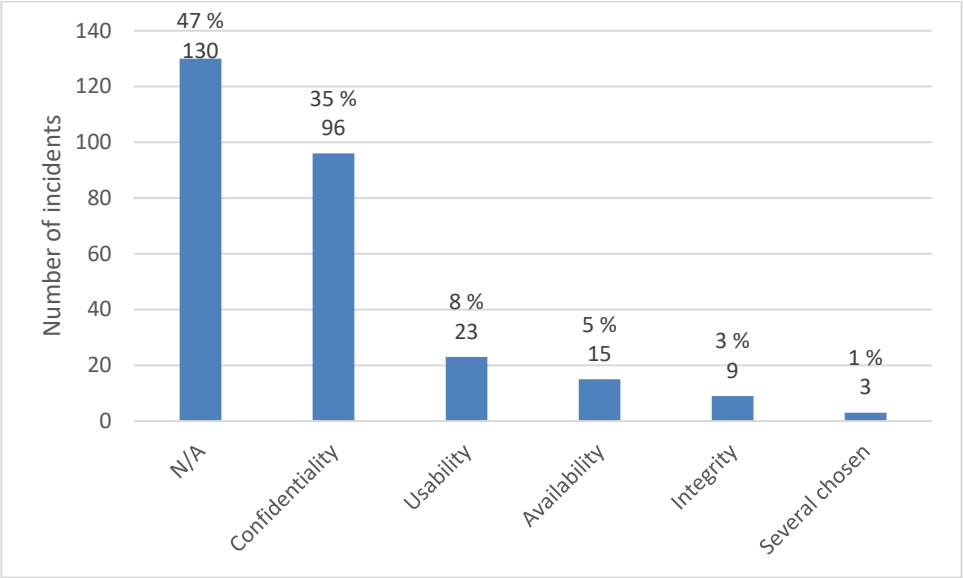

Figure 25. Reported effects on data privacy

Interestingly, in HaiPro the classical CIA triad had been expanded with the term *Usability*. As described previously, the terms *Usability* and *Availability* have different meanings although these terms have been confused at the national level (National Cyber Security Centre of Finland, 2022) and in the EU's legislation when comparing the Finnish and English versions (GDPR, 2016). Whereas the term *Usability* refers to the effectiveness, efficiency, and satisfaction in a specified context of use, the term *Availability* is seen as *"Ensuring timely and reliable access to and use of information"* (NIST 2022b, NIST 2022c).

In the context of reporting information security incident reports in a healthcare organization, adding the term *Usability* can be reasoned as conflicts between usability and security is a known issue that must be considered with information systems (Yee, 2004). Yet, it can be questioned how a healthcare employee could know the difference between the two terms *Usability* and *Availability* and manage to report the accurate effects on data privacy with the used categorization in HaiPro, if these two terms have been confused at national and international levels?

As seen in Figure 25, the category *N/A* contained the highest number of information security incidents with a total of 130 incident reports (47 %). According to this result, almost half of the information security incident reports in the data sample did not include the information about the effects on data privacy. Nevertheless, there was no option available in the HaiPro system where the analyst of the information security incident report could have told that there were no effects on data privacy. Therefore, it remained unknown whether this selection was made on purpose or why this information was missing.

There are several possible reasons for the missing categorization for effects on data privacy. Firstly, the information incident report could have been still under analyzation and the effects on data privacy were not yet categorized. In practice, the analyst might have requested additional information about the incident before analyzing the effects on data privacy. Even so, most of these incidents were reported more than a year ago and a total of 36 incidents were reported over two years ago. This result does not support an active gathering of additional information rather than forgetting to analyze the reports. What is more, gathering accurate information of incidents reported such a long time ago can be difficult.

Secondly, the analysts might not have identified any effects on data privacy from the reported incident. Therefore, these information security incident reports may have not affected any of the categories available. If this was the case, it can be questioned whether these incidents had some other effects on data privacy than the categories available and if so, what were these effects? As described, the available categorization for the effects on data privacy consists of the well-known CIA triad expanded with term *Usability* and this categorization can be seen to cover many of the incidents related to information security. However, the HaiPro data did not offer any other options such a free-text option to describe the effects on data privacy, for example if the analyst of the report would have categorized the incident by using other terms. Nevertheless, if these incidents had no effects on any of the available categories that consisted of the CIA triad, it would have been interesting to know why they were reported as information security incidents?

The third and probably the most likely reason for the missing categorization could be that the effects on data privacy were not selected and the analyzation was finished without this information. The analyst of the incident report might have not been able to select any of the categories available because of missing information, low quality of data, lack of instructions or knowledge. In addition, it is possible that the analyst of the report has deduced that a report was not an information security incident and therefore he or she had not selected any of the effects on data privacy. For these kinds of situations, the reporting system should have an option to change the type of the incident by the analyst or request the change from the original reporter.

All possible reasons described signaled that more instructions, education, and knowledge is needed. When considering the categorization used in the HaiPro system it was not reasonable to believe that almost half of the information security incidents did not have any effect on data privacy or that they had effects that should have been categorized by using other terms than available. This reasoning was also supported by the descriptions of the incidents that contained several incidents

where the effect on data privacy had not been selected even if according to the description the incident had an effect on data privacy.

According to the results, the education and instructions for reporting information security incidents and analyzing them should be revised. The reporter should have proper instructions and examples available how to report information security incidents in a way that the possible effects on data privacy could be analyzed as well. The analyst should have instructions and examples available how to analyze the effects on data privacy by using the categorization built into the HaiPro system and what to do if the information is missing, or if the incident is not related to information security. Overall, the effects on data privacy had not been properly analyzed in the target organization.

Besides the high number of information security incidents that did not reportedly have an effect on data privacy, what stands out in Figure 25, was the high number of incidents in the *Confidentiality* category. A total of 96 incident reports (35 %) were categorized in this category. According to this result, one out of three of the reported information security incidents in the research data had influenced the confidentiality of data. As the term *Confidentiality* is described as "*Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*" (NIST, 2022d), the (negative) effects on data privacy of these information security incidents have influence on preserving authorized restrictions on information access and disclosure.

In accordance with the GDPR (2016): "*Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing*." As the target healthcare organization operates under the EU's GDPR regulation, the organization is bound to report personal data breaches, such as loss of confidentiality, to the supervisory authority not later than 72 hours after the controller becomes aware of the breach, "*unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*". If the notification has not been made within 72 hours, reasons for the delay must be accompanied (GDPR, 2016). In Finland personal data breaches must be reported to the Office of the Data Protection Ombudsman (2022).

In addition to reporting the personal data breaches to the supervisory authority, the GDPR implies that if the risks from the personal data breach to the rights and freedom of natural persons are high, the data subject must be informed as well (GDPR, 2016). This communication must be conducted without undue delay, so

the data subject has an opportunity to cancel his or her credit card quickly, for example (Data Protection Ombudsman, 2022).

The research data does not contain information whether the target organization had made reports to the supervisory authority nor to the data subjects about personal data breaches related to the information security incidents reported via the HaiPro system. Nonetheless, as seen from Figure 25, and according to the descriptions of the incidents, the research data contained several reports where a personal data breach should have been reported or at least considered. Because of the high number of reports with missing information such as missing categorization of effects on data privacy, not all personal data breaches have been identified from the HaiPro system by the target organization. It is possible therefore that some of the data breaches have not been reported resulting in breaking the GDPR regulation.

To ensure that the GDPR is followed in a healthcare organization using the HaiPro or other system to report information security incidents, the data from the reports could be used to identify personal data breaches that should be reported to the supervisory authority. This data could be used to ensure compliance related to the requirement of the GDPR to also document all personal data breaches. However, depending on the organization there can be several different systems in use to report personal data breaches and HaiPro could be just one of them. Therefore, the process for reporting personal data breaches in an organization should be carefully planned and implemented with proper instructions.

The rest of the information security incident reports in the research data were categorized as follows: The third most common category for effects on data privacy was *Usability* with 23 incident reports (16%). *Availability* category contained 15 incident reports (5 %), *Integrity* category contained nine incident reports (3%). In a total of three information security incident reports several categories for effects on data privacy were selected.

Overall, the analyzed effects on data privacy were often missing from the information security incident reports in the research data. To improve the situation more education and instructions are suggested. Most of the effects on data privacy were categorized into the *Confidentiality* category meaning that the incident influenced preserving authorized restrictions on information access and disclosure. Incidents affecting *Confidentiality* of data privacy should be carefully analyzed to ensure the GDPR compliance.

8.15 Risk categories

By using the information about the used risk levels with the information security incident reports in the research data, all reports were sorted by the evaluated risk category. This enabled the possibility to count the number of information security incidents reported per risk category. In addition to the five risk categories from I to V in the HaiPro system, it is possible to skip the risk evaluation phase and not to evaluate the risk related to the information security incident report. All information security incident reports with a missing risk evaluation were categorized in the *Not Available* (N/A) category. Figure 26 presents the summary statistics of information security incidents per risk category.

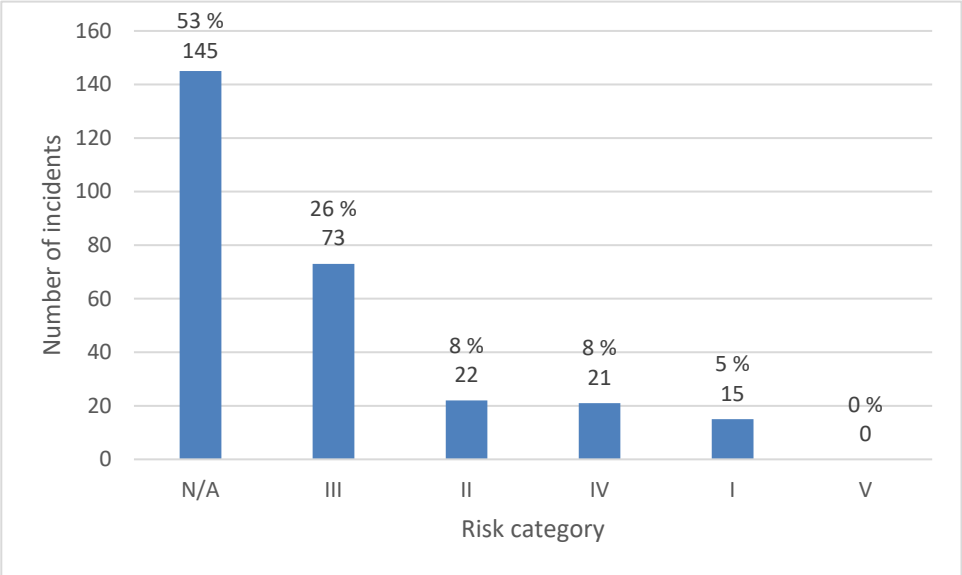

Figure 26. Risk category of information security incidents

The most striking result to emerge from the data was that the risk evaluation of information security incidents was lacking. As can be seen from Figure 26, most of the information security incidents (53%) did not include the information about the evaluated risk category. According to this result, in most of the cases risks of information security incidents reported via HaiPro system were not evaluated.

From Figure 26 it can be seen that there were no information security incidents reported that would have been evaluated as *Level V* risks. In other words, the research data did not contain any information security incidents that would have been reportedly categorized as *Severe,* meaning that both the evaluated probability of the incident and harm severity were the highest possible. In practice, the incident would have been evaluated as a *Level V* risk, if the probability was *Likely* or *Almost certain*, and the harm severity was *Significant* or *Serious*.

The research data included a total of 21 (8 %) information security incidents where the evaluated risk level was at *Level IV – Significant risk*. This result states that even though there were no reported incidents that would have been evaluated at the highest risk level possible, there were several information security incidents evaluated with significant risks. Because the research data did not contain information about the evaluated harm severity or probability it was not possible to determine how often these incidents occur or what were the evaluated consequences. Considering the 5x5 risk matrix used in the organization, it is possible that the *Level IV* risks contained incidents with different types of harm severity and probability.

In fact, for *Level IV* risks the probability of the risk could vary from *Almost certain* if the harm severity was *Minor* or *Moderate* to *Unlikely* if the harm severity was *Significant* or *Serious*. In any case, the *Level IV* risks in the research data showed that there had been several information security incidents reported where probability or harm severity of the risks was evaluated at a high level and that several risks had been evaluated as *Significant*. According to this result, there were information security incidents reported in the organization that had high risks.

Nevertheless, the connection between information security incidents and high risks was limited to the evaluated risks and some of the information security incident reports only. This connection does not mean that there is a connection between information security incidents and patient safety incidents. However, information security incident reports contained other information that could tell about the connection between information security incidents and patient safety. This information is discussed especially in chapter 8.18 Information security incidents reported with patient safety incident report.

As seen in Figure 26, the most common risk category for information security incident reports in the research data was *Level III – Moderate risk*. A total of 73 incident reports (26 %) were evaluated as *Level III* risks. Interestingly, this was more than the number of information security incident reports in other risk categories combined. *Level II – Minor risk* category contained a total of 22 (8%) information security incident reports and *Level I – Insignificant risk* category contained 5 (15 %) incident reports.

Because the possibility for lower-level risks was assumably higher, meaning that lower-level risks occur more often than high level risks, it was reasonable that in the research data there were more incidents in the *Level III* risk category than in the higher *Level IV* and *Level V* risk categories. However, this was not the case with lower-level risk categories as there were less incidents in in *Level II* and *Level I* risk categories than in the *Level III* category. This result signals that the risk

evaluation could be lacking for lower than *Level III* risks or that lower risks had been evaluated at higher *Level III* risks.

A possible explanation for these results may be that both are correct. Risk evaluation might not have been conducted for lower risks because of reasons such as limited time or that because conducting risk evaluation was not seen important because the risks were low. If the risk evaluation was conducted the risk evaluation culture could be favoring selecting mid-range risk category.

Overall, these results indicated that the risk evaluation for information security incident reports was lacking. In most of the cases the risk evaluation was missing and there was no information available about the evaluated risks. Most of the risks were evaluated as mid-range risks and there were low number of lower risks evaluated. Based on these results, risk evaluations had not been conducted for reports with lower risks or this kind of information security incidents have not been reported as much as incidents with higher risks.

Positive findings from the risk evaluations included that the risks related to information security incident reports had been evaluated in the organization. Even though there were no incidents in the highest risk category, the evaluated risks showed that there have been information security incidents reported with high risks. In general, the risk evaluation process and the risk evaluation culture could be improved in the organization. These improvement suggestions are discussed in more detail in the discussion chapter.

8.16 Conditions and other contributing factors

Figure 27 presents the summary statistics for conditions and other contributing factors reported with information security incident reports. As seen in Figure 27, the reported conditions and other contributing factors have been divided into seven different groups. A closer inspection of Figure 27 shows that more than half of the reports (62 % total) belong to the following two groups *Unknown* with a total of 74 (27 %) incidents and *Empty* with a total of 98 incidents (35 %). From these two groups, the first indicated that the conditions and other contributing factors related to more than every fourth of all information security incident reports in the data sample were unknown, whilst more than every third incident report did not include information about the conditions and other contributing factors.

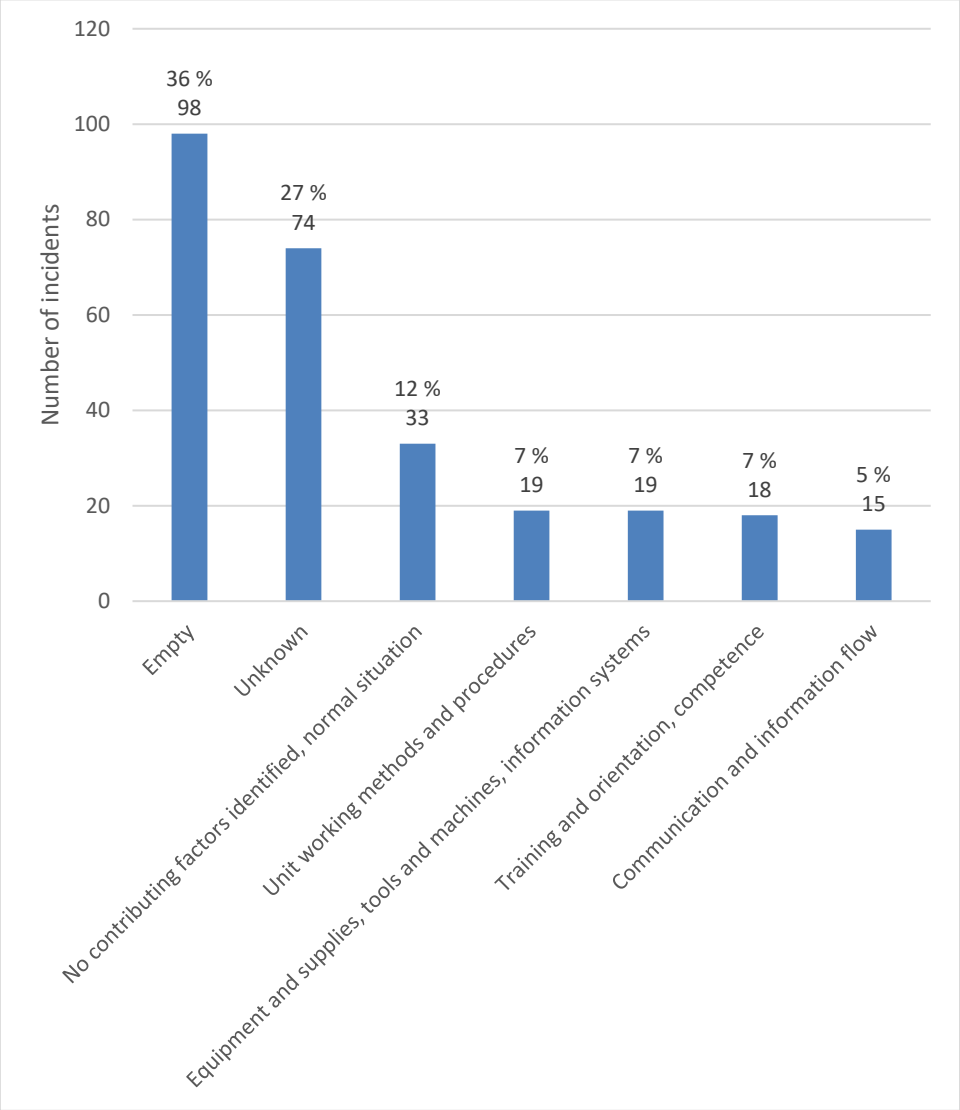

Figure 27. Conditions and other contributing factors

These results from the two most common categories signal a lack of reported information of information security incident reports. Information about the conditions and other contributing factors could have been reported with the incident, yet this information was missing. While it was possible that the conditions and other contributing factors were not known by the reporter or were difficult to analyze, it was surprising that there was such a high number of incidents where this information had been left empty and was not included in the reports at all.

Besides the missing information and underreporting of these factors, this result indicated that the handling process of information security incident reports did not provide the missing information either. As described in Figure 35, at the early

stage of the handling process of incident reports, the analyst could decide whether additional information is needed. In case of additional information being needed, the analyst can contact the reporter via email, if the reporter entered his or her email address into the system when reporting the incident or contact a larger group to gather the information. After the analyst decides that no additional information is needed, the incident will be analyzed.

From the research data it could not be determined what had been the decisions of the analysts related to additional information requests, if any, or what were the acts behind these decisions. For example, there might have been several additional information requests, emails and face to face meetings related to any of the incident report. Or there might have been zero requests. Additional information requests may have been unsuccessful to provide this missing information, or the analyst may have decided that additional information cannot be gathered. Without this information it remained unknown whether there were additional information requests related to incident reports and if these requests had provided information about missing conditions and other contributing factors.

Nonetheless, because there was a high number of incidents with missing information about conditions and other contributing factors, the analysts of the incident reports have not been able to get this information via additional information requests, or they have decided that no additional information was needed. Reasons for unsuccessful additional information requests can be many, such as the reporter of the incident might not have been reached, or he or she may not have saved his or her email address with the report. In case of contacting a larger group, the contact might not have reached any of the employees that had this information or providing information to these requests were not seen as important among the employees. The missing information arouses a question whether the conditions and other contributing factors in the incident reporting has been considered as important among employees? To improve future incident reporting, instructions related to reporting the conditions and other contributing factors should be revised.

Besides the two most common categories, *Unknown* and *Empty* for conditions and other contributing factors related to information security incident reports, the third most common category was *No contributing factors identified, normal situation* with a total of 33 (12 %) incident reports. As the name of the category suggests, there were no factors identified that could have contributed to the reported incident and that the situation was normal when the incident occurred.

It could be difficult to see what the difference between these three most common categories for conditions and other contributing factors were, as none of them

provided information about the contributing factors and as the description of *normal* situation can vary depending on the reporter. Even so, the categories *Unknown* and *No contributing factors identified, normal situation* showed that the reporter had identified the information security incident and considered the conditions and other contributing factors related to the incident. In case of the incident belonged to the *Empty* category, it was unsure if these factors were considered at all. Besides, what could be determined from the incidents in the categories *Unknown* and *No contributing factors identified, normal situation* was that these incidents did not belong to the other categories. In other words, these incidents were not affected by the other contributing factors mentioned in Figure 27 such as *Unit working methods and procedures*.

The three most common categories for conditions and other contributing factors covered 74% of all information security incident reports in the research data. However, these categories did not specify any contributing factor related to the incidents or the situation was reportedly normal when the incident occurred. As shown in Figure 27, the rest of the incident reports (26%) were divided into four different categories. *Unit working methods and procedures* contained 19 (7 %) incidents, *Equipment and supplies, tools and machines, information systems* contained 19 (7 %) incidents, *Training and orientation, competence* contained 18 (7 %) incidents and *Communication and information* contained 15 (5 %) incidents. The Figure 28 provides the results of subcategories of these four main categories of conditions and other contributing factors related to information security incident reports.

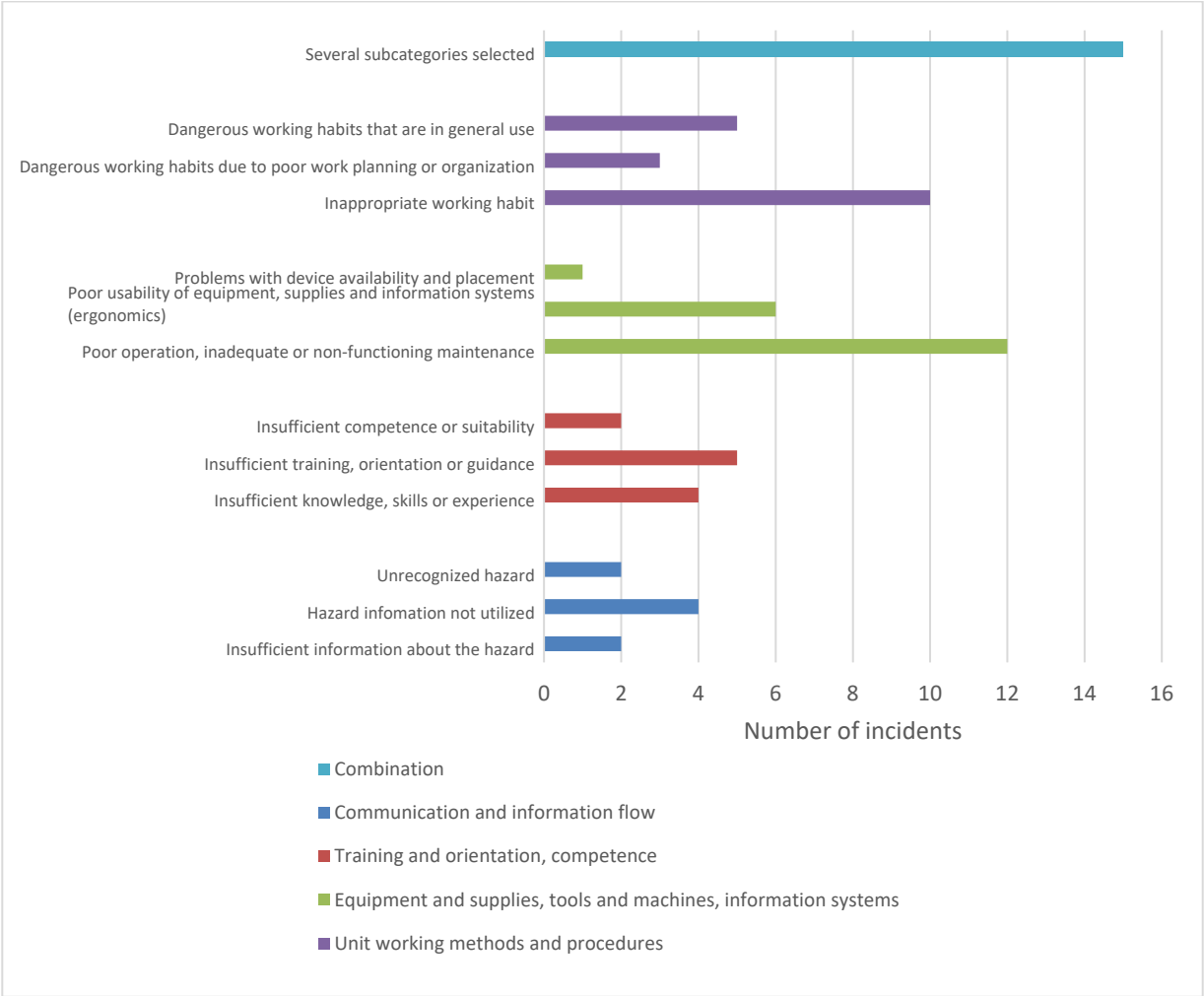

Figure 28. Subcategories of conditions and other contributing factors related to information security incident reports

As seen from Figure 28, the most common subcategory for conditions and other contributing factors related to information security incident reports was *Poor operation, inadequate or non-functioning maintenance* under the *Equipment and supplies, tools and machines, information systems* category. A total of twelve incident reports were categorized into the *Poor operation, inadequate or non-functioning maintenance* category, that was 17 % of all incident reports with this information in the data sample. The second most common subcategory in the research data was *Inappropriate working habit* under the *Unit working methods and procedures* category. This category contained ten incident reports that was 14 % of all incident reports in the specified categories.

When considering information security incident reports that were categorized with one subcategory for conditions and other contributing factors related to the incident, it was clearly seen that two main categories *Unit working methods and*

procedures and *Equipment and supplies, tools and machines, information systems* contained more incidents than *Communication and information flow* or *Training and orientation, competence* categories. One reason for this was because the research data contained several information security incident reports where several subcategories for conditions and other contributing factors were selected. As shown in Figure 28, several subcategories were selected in 15 incident reports (5 % of all incident reports).

Overall, most of the information security incidents reportedly occurred without any specified conditions or contributing factors identified or in a normal situation. The most common category for this subject was *Empty*, meaning that the reporter had not reported whether there were any conditions or other contributing factors related to the incident or not. In addition, the analyzation of these incidents had not provided the missing information. The minority of the reports were categorized with specified conditions and other contributing factors and their subcategories. No significant differences in the number of reports were found between the four main categories. The two most common subcategories were *Poor operation, inadequate or non-functioning maintenance* and *Inappropriate working habit*. Nonetheless, the number of incidents in all subcategories were low.

8.17 Proposed measures to prevent a recurrence of information security incidents

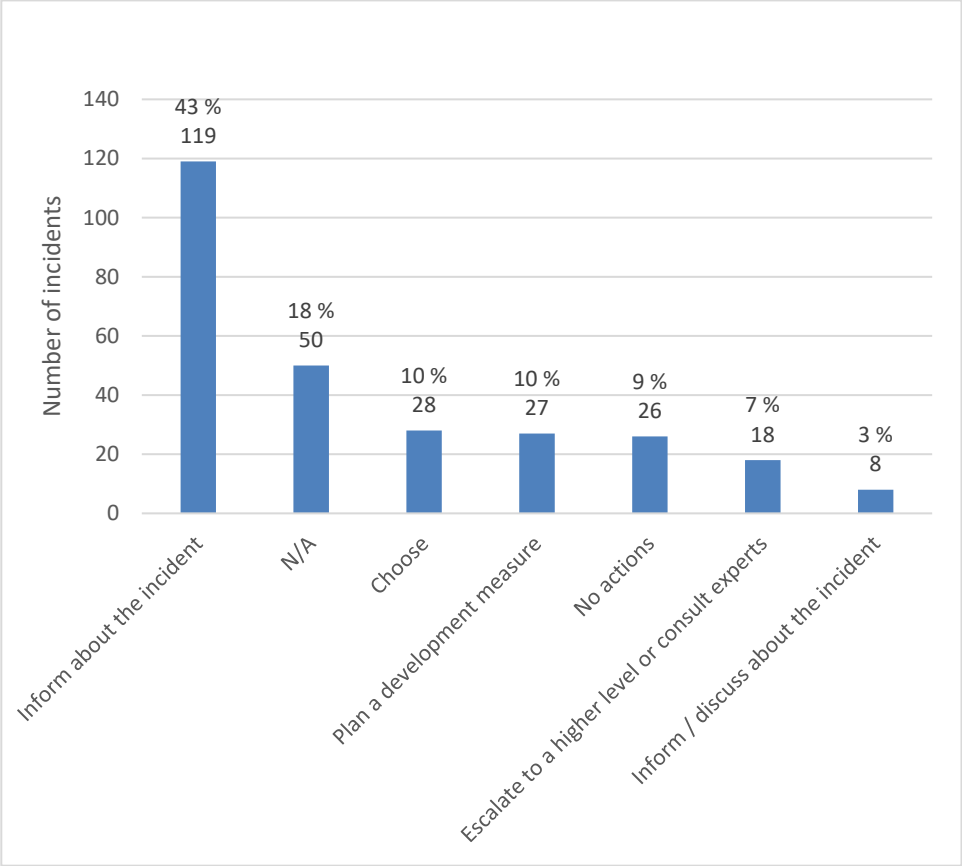

Figure 29. Proposed measures to prevent a recurrence of information security incidents

The Figure 29 presents the results of the proposed measures to prevent a recurrence of information security incidents. As seen in the figure, the HaiPro system contained five different options for proposed measures; *Inform about the incident, Inform / discuss about the incident, Plan a development measure, Escalate to a higher level or consult experts* and *No actions*. Additionally, the research data contained incident reports where the value of the selected option were *Choose* or empty (*N/A)*.

According to the HaiPro instructions for patient safety incident analyzation; when the analyst has made the selection for the proposed measures to prevent a recurrence of the incident, an open text box will become visible where the analyst should write the target(s) who should be informed about the incident (Awanic, 2020b). Providing that the analyst has saved this information, the target(s) to be informed about the incident should have been saved into the HaiPro database.

In research data there was a field that was related to the proposed measures to prevent a recurrence of information security incident. This field was called *Write the proposed measure or justify why no action is required.* Next, the number of incident reports in categories shown in Figure 29 are described with the information written into the related field.

From Figure 29, it can be seen that the most common category selected in the research data was *Inform about the incident* that contained total of 119 incidents (43 %). Considering the high number of incidents in the *Inform about the incident* category, this result signals that the analyst had often decided that informing a person or persons about the incident is enough to prevent its recurrence. This result could be expected as many of the incidents were related on data confidentiality and the reported risks were low or moderate. For example, in a case where the confidentiality of data has been affected by an information security incident, but the risk level has been estimated as low, informing the related parties such as the working department and the supervisory authority about the incident can be reasonable. As mentioned earlier, if the risks from the personal data breach to the rights and freedom of natural persons are high, the organizations operating under the EU's GDPR are also bound to inform the data subject without undue delay.

From the 119 incidents in the *Inform about the incident* category, a total of 68 incidents (57 %) contained a written argument why this category was selected. Most of these arguments focused on explaining that there had already been a discussion or informing about the incident, the incident had been taken care of (signaling that a recurrence of the incident will be prevented in the future) or that there will be a discussion or informing about the incident in the future. In one written argument, the informing was reportedly conducted by leaving a written note next to a machine to inform the next user, whereas another argument emphasized the risks of leaving such written notes.

Even though the category *Inform about the incident* was selected, some of the incident reports contained information that there has been or will be a discussion held about the incident to prevent a recurrence of the incident. Therefore, these incident reports could belong to the category *Inform / discuss about the incident* as well, and signaled about misclassification between these two categories.

As seen in Figure 29, the number of incidents in the next category *Inform / discuss about the incident* were the lowest with a total of eight incidents (3 %). Comparing the two categories on the left in the figure *Inform about the incident* and *Information / discuss about the incident* show that the analyst of the incidents often chose the first category that included informing targets about the incident,

but rarely selected the latter that would have included a discussion about the incident. According to this result, the analyst had often decided that informing about the incident was enough, and no discussion was needed. Hence, informing about the incident was seen as a more effective way to prevent a recurrence of the incidents than discussing them. This result is somewhat unexpected as informing can be seen as one-way communication method where the information about the incident will be provided to the targets, whereas a discussion enables a two-way communication where other parties can participate on the discussion about preventing the recurrence of the incident. None of the incident reports in this category included additional information about the proposed measure nor a written argument why this category was selected.

In a large organization with many units and departments, large number of workers and working methods, the discussion should be seen as an opportunity to provide effective methods to prevent information security incidents that can be various and related to specific tasks and working methods instead of one-way communication. Even so, informing about the incidents could be related to the culture in the organization that supported one-way communication. For example, in a hierarchical organization the supervisors may think that after the information has been provided to their subordinates the recurrence of the reported incident will be prevented and if not, the supervisors have at least fulfilled their duties to inform about the incident and transferred the responsibility to prevent a recurrence of the incident to their subordinates.

Even though this could follow the rules of an organization and its hierarchy, this kind of practice can be problematic for several reasons. If the incident has been related to generally used working methods for example, the subordinates might not actually have an opportunity to prevent a recurrence of the incident even if the supervisor has informed the employees about the incident. In a case where the supervisor has sent the information to the employees but not discussed about it, he or she might not even know how the recurrence of the incident could be prevented and at what costs? It is also possible that informing about the incident has been seen as easier than the discussion and therefore preferred. In practice, after the targets have been informed about the incident, the task is completed right away and no further actions such as arrangements for a discussion are needed. Therefore, after the targets have been informed the incident then it will be out of sight, out of mind.

The Plan a development measure category contained a total of 27 incidents (10 %). According to this result, planning a development measure to prevent a recurrence of the incident was proposed with the minority of the reported information

security incidents. From these 27 incident reports, a total of 20 reports contained additional information about the proposed measures or reasoning why there were no actions needed. Only 14 incident reports (5 %) included a detailed information about how to improve the processes or operation to prevent a recurrence of the incident.

A low number of incidents in this category signaled that often the development measures were not seen as necessary to be added into the report. The reasons for this can be due to the nature and type of the incident that could be difficult to prevent with development measures, such as incidents occurred because of human error. Additionally, it can be unknown for the analyst how this kind of incident could be prevented and what development measures should be planned to prevent the recurrence of the incident. This could be due to the high level of information security in the organization where it can be difficult to propose development measures to improve the situation that is already on a high level. On the other hand, the lack of information and poor-quality information incident reports in the data sample referred to a situation where it was difficult to identify and propose possible development measures.

Lack of knowledge about information security or factors related to the incident could be affecting on the low number of proposed development measures to prevent a recurrence of the incidents. Considering the data on the research sample that contained a large amount of information security incidents where information was often missing, the lack of reported information and information security knowledge was more likely the cause behind this result than the high level of information security. At worst, the lack of reported information and low level of knowledge could lead into a situation where information security incidents continue to recur and will be not prevented because missing information makes it difficult to identify the root causes of the incidents and the lack of knowledge does not support the identification nor planning of the development measures.

Nevertheless, the results from this category showed that there were several information security incidents reported where the analyst had proposed that development measures are needed to prevent a recurrence of the incident. This indicated that the recurrence of these incidents could be prevented by improving the operation and that the analyst had identified this kind of development measures to improve the situation.

The Escalate to a higher level or consult experts category contained a total of 18 incident reports (7 %). Based on this result, the percentage of information security incidents reports that had been escalated to a higher level or where experts were consulted was low. According to the analyst guide for HaiPro, when analyzing

patient safety incident reports, the analyst is required to report at least one reason why the incident report has been escalated (Awanic, 2020b).

From these 18 incident reports in this category, a total of 13 (72 %) incident reports contained a written description into the field *Write the proposed measure or justify why no action is required*. Three descriptions referred to a direct escalation to a higher level. In these three incidents reports the target role of the escalation in the organization was described as well, whereas the rest of the arguments varied from describing the challenges related to a particular IT-system to questions asking what could be done to improve the operation and prevent a recurrence of the incident? One description simply stated that "The person must be held liable for his/her behavior". Incident reports in this category did not contain information why the incident had been escalated to a higher level or why experts were consulted. It also remained unknown what happened after the escalation or consulting with experts.

Even without information about the reasons for escalating the incident or consulting with experts, the low number of incidents in this category signaled that the analysts had often decided that there was no need to escalate the information security incidents to a higher level or consult with experts. This could be due to the high number of incidents with a low risk level where informing about the incident had been seen as adequate measure to prevent a recurrence of the incident. In the research data, none of the incidents with a risk level I were proposed to be escalated to a higher level or that experts should be consulted. Incidents with a risk level II, the total number was two incidents. Therefore, information security incidents with a low risk level had not been proposed to be escalated to a higher level or that experts should be consulted.

Even though the total number of incidents with estimated risk levels III or IV was 94 (34 %) incidents, the number of incidents with these risk levels that were proposed to be escalated to a higher level or consult experts was low as well. It would have been reasonable to think that incidents with a high risk level were escalated more often to enable immediate actions from the higher level or from the experts. Nevertheless, according to the results, there was no connection between the estimated risk levels and the proposed measures to prevent a recurrence of the incidents. In risk category III, a total of 12 incidents reports were escalated. From a total of 18 incident reports in the highest estimated risk category (risk category IV), only in four incidents the proposed measure was to *escalate to a higher level or consult experts*, whereas in six cases the proposed measure was *inform about the incident*, meaning that even if the risk from the incident was estimated to be

high, informing about the incident was seen as an adequate measure to prevent the recurrence.

In a total of 26 information security incidents (9 %), the proposed measure to prevent a recurrence of the incident were reported as *No actions*. By selecting this category, the analyst had decided that there were no actions to be taken to prevent a recurrence of the incident. Most of the incident reports with this proposition included a written argument why there were no measures needed.

The reasoning of these arguments varied. Whereas some of the written arguments included information about measures that had been already taken to prevent the recurrence of the incident, some concluded that it was not known how a recurrence of this kind of incident could be prevented. One report stated that the department is not responsible for the system that caused the incident neither can it repair technical systems. The argument continued, however, that the department responsible for the system was not informed about the incident and that they will not be able to fix the situation because the information was not shared between the reporter's department and the department responsible for the system.

One wrote that he or she did not know how this incident could have happened and therefore cannot propose any measures to prevent a recurrence of the incident. Another one wrote that the incident was an accident (human error) and was due to his or her own actions but described in detail that the risks from his actions were very low because of the data involved was publicly available. In three arguments it was stated that an IT-service provider had been already informed about the incident, and this was seen as the reason why there were no measures proposed. In seven cases the argument was not written including six incidents with a risk level III and one incident with a risk level IV.

A total of 28 incident reports (10 %) contained a term *Choose* as the proposed measure to prevent the recurrence of the information security incident. Even though the term *Choose* might indicate that there were measures selected, the analyst could have selected an option for *Choose* from the list for different measures. The term *Choose* was not a default option, it must be selected from the list. In other words, it seems that in 10 % of all information security incident reports the analyst had selected *Choose* as a proposed measure to prevent a recurrence of the incident. This result was confusing, and it was difficult to understand why this option was available in the HaiPro system and what the analysts meant when they selected this option. Interestingly, none of the incident reports with this selection included a written argument why this selection was made or whether measures were needed to prevent a recurrence of the incident or not.

In a total of 50 information security incident reports (N/A = 18 %), the proposed measures to prevent a recurrence of the incident were missing. This result was somewhat expected as all the previous variables analyzed had several incident reports with missing information. Unlike with the option *Choose*, empty information was the default option and did not require the analyst to make any selection for it. Therefore, this section could have been bypassed intentionally or unintentionally. Again, none of the incident reports contained a written argument about why there were no measures proposed or if measures were needed to prevent a recurrence of the incident or not. Common to all incident reports with the missing selection was that they also lacked information on several other variables. It was likely that the lack of reported information had affected to the missing proposed measures to prevent a recurrence of the incident.

Considering the number of incident reports in the following categories: *No actions* with 26 incidents (9 %)*, Choose* with 28 incidents (10 %) and *N/A* with 50 incidents (18 %), a total of 104 information security incident reports (38 %) did not include any proposed measures to prevent a recurrence of the incident. Because none of these categories proposed any measure to prevent a recurrence of the incident, the use of these categories or options should be revised. When analyzing the incident reports, one option should be enough to report that there are no actions needed, and it should be mandatory to give a written argument why this selection was made.

In addition to the fields *Proposed measures to prevent a recurrence of the incident* and *Write the proposed measure or justify why no action is required,* the research data contained information recorded into a field called *Description of the implementation of the measures*. From the 275 information security incident reports, 105 incident reports (38 %) contained text in this field. Conversely, a total of 171 incident reports (62 %) did not contain any description. The low number of descriptions of the implementation of the measures could be reasoned as the overall number of proposed measures to prevent a recurrence of the incident was low as well.

In the written descriptions terms such as reminding, informing and discussing were often mentioned. In one description a laborious and long process to implement the measures was emphasized. It was possible that this could have been the case with other incidents as well, but it was not recorded into the HaiPro system.

Overall, the results from this section showed that informing was often seen as adequate action to prevent a recurrence of information security incidents. Options such as planning a development measure, escalate to a higher level or consult

expert were less proposed. Even so, proposed measures were often missing, even with incidents with a high estimated risk level. Interestingly, the least proposed measure included a discussion about the incident. The results signaled that the measures to prevent a recurrence of the information security incidents were not often proposed and that the culture in the target organization may not support escalating incident reports to a higher level or discussing about these measures. It should be documented what happened in case the experts have been consulted or if the incident has been escalated to a higher level, now this information was missing.

What is more, proposed development measures can contain valuable information for the organization. Nevertheless, according to the high amount of missing information in the sample data, this value had not been recognized. Incident reports with high estimated risks but without proposed measures on how to prevent a recurrence of the incident nor reasoning why no measures are proposed should be identified and examined to prevent a recurrence of incidents with high risks. Proposed development measures could be used to improve the operation of the organization, prevent a recurrence of the incidents and the users should be encouraged to propose them. Proposing development measures can be supported for example by improving information security incident reporting and the overall quality of the reports.

8.18 Information security incidents reported with patient safety incident report

As shown in Figure 15, the information security incident reporting template in HaiPro includes an option to fill in three separated incident reports that will be linked to the original information security incident report. These three reports are patient safety event report, occupational safety event and operational environment event report. From these three types of reports the research data contained information on whether a patient safety event was reported with the information security incident report or not. In this chapter, the main characteristics of the information security incident reports reported with a patient safety incident report will be described. According to the literature review on patient safety incident reporting and cybersecurity, this was the first time when information security incidents related to patient safety incidents have been studied.

In practice, when reporting an information security incident, the reporter can choose an option “report a patient safety incident as well”. If the reporter chooses this option, the system guides the reporter to fulfill a patient safety incident report

on a different patient safety incident reporting template using the HaiPro system. The information on both two reports will be gathered into the HaiPro database even though they remain as two separate reports.

The research data contained a total of 44 information security incident reports (16 %) that included information that the reporter had also filled in a separate patient safety incident related to the information security incident. The reporter's department and the department where these 44 incidents reportedly occurred varied. The incidents were reported by 27 different departments and occurred in a total of 24 different departments. Figure 30 shows the number of information security incidents reported with a patient safety incident report per department. In Figure 30, the vertical axis shows the number of incidents reported and the horizontal axis shows the names of the departments that have been replaced with a number to ensure the anonymity of the departments.

As seen in Figure 30, in most of the cases departments that had reported these kinds of incidents had reported one incident. Of the 27 departments, ten had reported more than one incident. The highest number of information security incidents reported with a patient safety incident report per department was shared between two departments that both had reported four incidents. According to the data, departments have reported few information security incidents with a patient safety incident and there was no single department that would have reported these kinds of incidents significantly more than other departments.

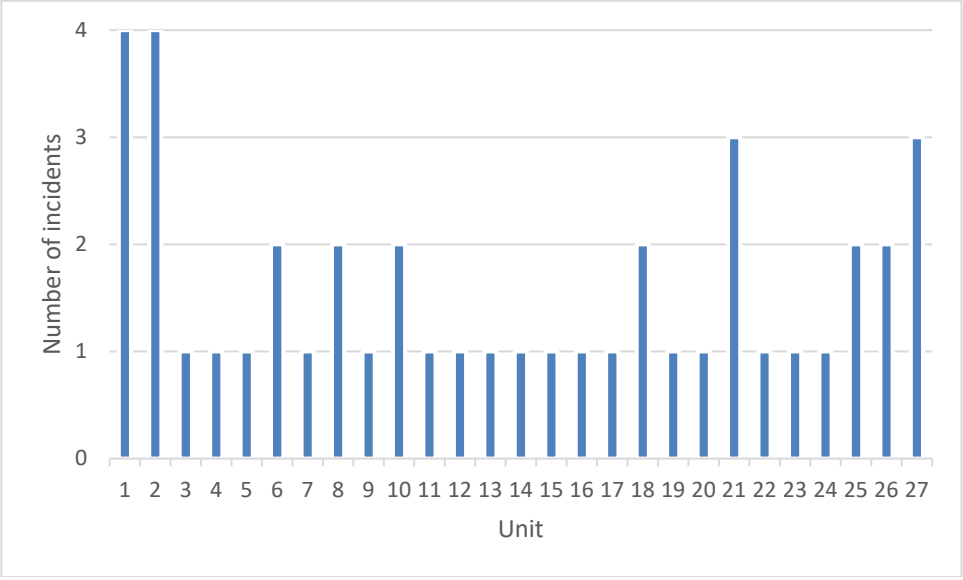

Figure 30. Number of information security incidents reported with a patient safety incident report per department

Surprisingly, even though more than one in four of all information security incident reports in the research data were reported by one single department, *Department Y* had not reported any of the information security incidents linked with patient safety incidents. This result could be due to the nature of incidents that *Department Y* reported where there was no reason to fill in a separate patient safety incident report. It would be a good idea to discuss with *department Y* about these results to ensure that they know when a separate patient safety incident should be reported.

While these 44 incidents were reported by 27 different departments, they had reportedly occurred in 25 different departments. Figure 31 shows the number of information security incidents that were linked with patient safety incidents occurring per department. Again, the number of incidents is shown on the X-axis and the department on the Y-axis. As seen in Figure 31, in most of the cases there had reportedly occurred a few (one to three) incidents per department.

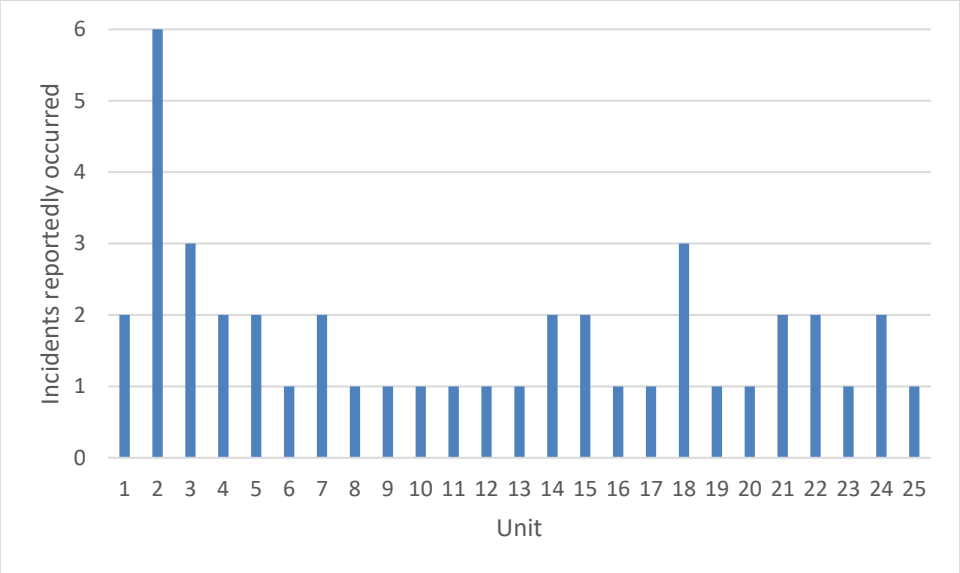

Figure 31. Number of information security incidents reported with patient safety incident report occurred per department

Even so, it can be seen from Figure 31 that department number two had a higher number of incidents than others. This department was the IT-department with a total of six incidents, although as mentioned earlier, there could be miscoding of reporting if the reporter had, for example reported that an incident related to the IT-network in the department had actually occurred in the IT-department, instead of his or her own department.

Figure 32 describes the reported nature of the information security incidents reported with patient a safety incident. From these 44 incidents, nine incidents were reported as *Near miss*, 12 incidents were reported as *Adverse event,* and 16 incidents were reported as *(Patient safety) Incidents*. In five cases, the incident was reported as *Safety observation / development proposal,* and in one incident the information was missing.

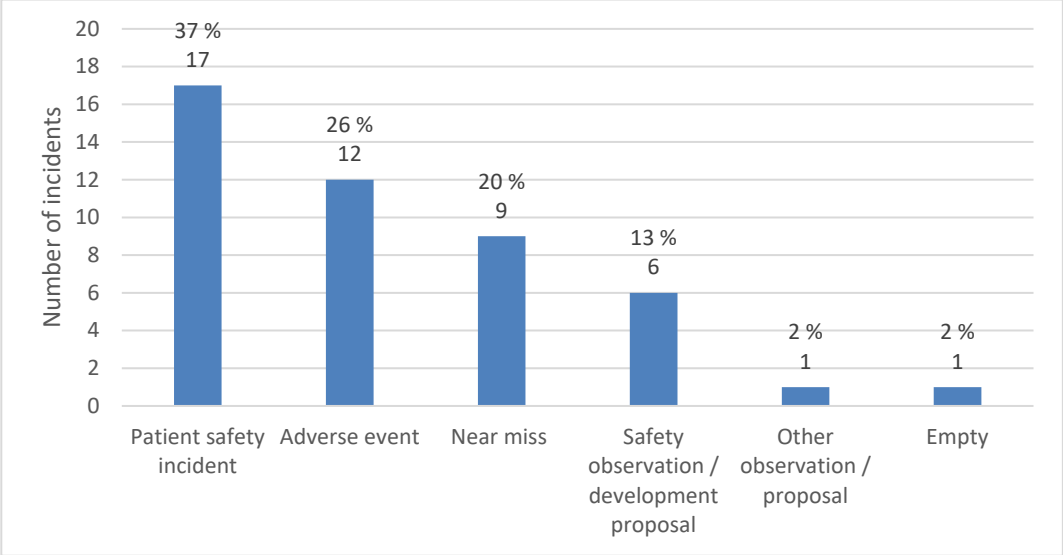

Figure 32. Nature of information security incidents reported with patient safety incident report

Considering the incidents reported as *Adverse event,* all these incidents contained a separate patient safety incident report as well. This was expected, of course, as incidents that caused harm to the patient were also patient safety incidents. Neveretheless, the total number of information security incident reports linked with patient safety incident reports was different than the number of information security incidents reported as Adverse events. This result indicated that even if there was a separated patient safety incident reported, not all cases included harm caused to the patient.

Figure 33 describes the type of the information security incidents reported with a patient safety incident report. The most common type of such incidents was *Information flow or information management* with a total of 16 incident reports (35 %) and the second most common type was *Data confidentiality* with 15 incident reports (33 %).

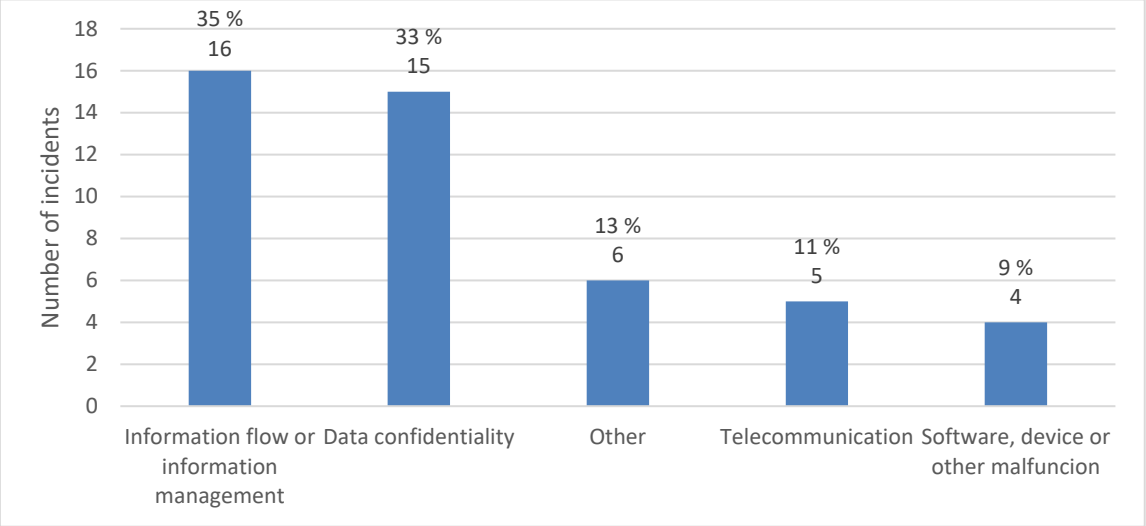

Figure 33. Type of information security incidents reported with patient safety incident report

When comparing the numbers seen in Figure 33 to the most common types of information security incident reports in the whole research data that were seen in Figure 21, there were a high amount of reports in the *Data confidentiality* category in both figures. However, what stood out in Figure 33 was the high number of incident reports related to *Information flow or information management*. According to this result, information security incidents that have been reported with patient safety incidents were more often related to *Information flow or information management* than information security incidents that had not been reported with patient safety incidents.

It is important to note, however, that these reports provided only a brief overview to the information security incidents reported with patient safety incident reports because the number of these kind of incident reports in the research data was low. The connection between information security incidents and patient safety incidents can be still seen from this research data. In addition, this brief overview showed that it is possible to study information security incidents related to patient safety incidents. Considering that this was one of the first studies to study these kinds of incident reports, this area should be studied more in the future.

8.19 Risk management of information security incidents

Before concluding the research contribution and implications for practice from the analyzed information security reports, this chapter discusses the risk management of the incident reports in the research data and the used risk categorization in the

HaiPro system. Risk management and the "risk based" approach has been preferred by standards and best practices such as ISO27001 and CSF (ISO, 2013; NIST, 2018). According to the results, there were several problems related to the risk management of information security incident reports.

The high number of missing risk evaluations signaled that the risk evaluation of information security incident reports had not been considered as important in the organization. Additionally, this result hinted at a lack of a risk management culture with information security incident reports in the organization. When more than half of the reports failed to include risk evaluation, it could be questioned whether the employees in the organization had been educated and instructed on how to conduct risk evaluation in a proper manner.

Missing risk evaluations meant that there was no information about the risks related to the reported information security incident reports. As instructed by Awanic, the risk evaluation is conducted to enable analyzation of high risks from the evaluated risk data (Awanic, 2020b). Without this information the evaluated risk data will be inadequate and analyzations made from this data could be insufficient. Overall, the lack of risk evaluations related to information security incident reports could also decrease the value of the report.

The low level of risk evaluations of information security incident reports aroused a question related to patient safety incidents: What was the rate of risk evaluations related to patient safety incident reports? If the risk evaluation culture in the organization was not encouraging to evaluate risks related to information security incident reports, was this also the case with patient safety incident reports? The risk evaluation can be seen less valuable when considering information security incident reports compared to patient safety incident reports. However, if the risk evaluations had not been conducted for patient safety incidents, it can inform the situation regarding the neglecting of risk evaluation and risk management overall.

There was no information found from the research data that would have reasoned why the risks were not evaluated during the incident reporting and analyzation process. For example, there was no information if an error occurred when conducting the risk evaluation, or if the risk evaluation was partially completed but not fully completed because of some reason such as lack of time. Even so, this was an interesting result that should be considered when improving information security incident reporting.

Even though the research data did not contain any information on security incidents reported as *Level V* risks, there were several incidents that had been evaluated at a lower risk level. It was worth noting that when using the 5x5 matrix

in the risk evaluation phase, the probability or harm severity of the incident could be evaluated as the highest possible, if the other factor was evaluated lower resulting in a lower risk level than *Level V*.

For example, the harm severity could have been evaluated as *Serious* if the probability of the risk was evaluated as *Rare, Unlikely,* or *Possible*. In this case, the risk level would have been *Level III – Moderate risk* or *Level IV – Significant risk*. The description of the *Possible* in the risk matrix was described as "events that occur occasionally". Therefore, the harm severity of the risk could have been evaluated as the highest possible and the probability of the risk as *Possible* without the risk being evaluated as a *Level V* risk.

On the other hand, the probability of the risk could be evaluated as *Almost certain,* if the harm severity was evaluated as *Negligible, Minor or Moderate*. Again, in this case, the risk level would have been *Level III – Moderate risk* or *Level IV – Significant risk*. The description for the harm severity *Moderate* in the risk matrix was described as "minor inconvenience or injury that requires minor actions, or the length of hospital stay increases more than three days". Therefore, the probability of the risk could have been evaluated as the most likely and the harm severity as *Moderate* without the risk being evaluated as *Level V* risk.

Taken together, the probability and the harm severity of the risk could be evaluated as *Possible* (events that occur occasionally) and *Moderate* (minor inconvenience or injury that requires minor actions, or the length of hospital stay increases more than three days) resulting in a lower than *Level V – risk*. With this combination, the result of the risk evaluation would have been *Level IV – Significant risk*.

From the research data, it was not possible to determine what was the evaluated probability or harm severity of the incident, only the result of the risk evaluation was shown. Hence, it remained unknown what was the total number of incident reports where the harm severity of the risk had been evaluated as *Serious,* or where the probability had been evaluated as *Almost certain,* for example.

The information about the chosen probability and harm severity could provide a more detailed view into the risk evaluation of information security incidents. In addition to the evaluated risk level, more detailed information could be used to improve detection of information security incidents with the highest reported possibility, or the highest reported harm severity. From the incidents that have occurred in the organization, besides the incidents with the highest evaluated risk level, the organization and its risk management should be interested in incidents with the highest possibility or the highest harm severity.

Considering the research data contained all information security incident reports reported in one healthcare organization, the results signaled the risk evaluation culture in the organization. All previous risk evaluations conducted on information security incidents in the organization resulted in lower than *Level V*, meaning that there has not been any information security incident report that would have been evaluated at the highest risk level in the organization.

For a person conducting the risk evaluation, it can be difficult to evaluate an incident as a *Level 5* risk if the person knows that his or her risk evaluation differs from all previous information security incidents, and that it would be the first time when risk evaluation will result in the highest risk level possible. Presumably, evaluating the first *Level 5* risk would stand out among the information security incident reports in the HaiPro system or, for example, in reports conducted from the incidents reported in the organization. The first *Level 5* would therefore arouse attention in the organization and possibly require some additional information about the case. If this would be the case, conducting a risk evaluation that will result in *Level 4* or lower could be seen easier and less laborious to conduct and as a part of the risk evaluation culture in the organization.

This kind of risk evaluation culture could lead to a situation where the results of risk evaluations are not accurate and the potential benefits from the risk evaluation would not be achieved. Inaccurate risk evaluation does not provide correct information about the risks related to information security incidents that could be used to improve the operation and eliminate or control the risk in the future. Furthermore, a risk evaluation culture that favors the risk evaluator to evaluate risks at *Level 4* or lower and avoiding *Level 5* risks could hide high level risks and lead to improper risk management in the organization.

When considering the operation of the healthcare sector is a part of the critical infrastructure and includes protecting the lives of the patients, at worst, the lack of accurate risk management can have dire consequences if high level risks have not been evaluated or managed correctly. To ensure that the risk evaluation is accurate and appropriate, the evaluated risks of information security incidents reported via HaiPro, or other reporting system, should be monitored regularly. Conducting reports from the evaluated risks related to an information security incident could provide valuable information for monitoring. For example, the HaiPro system offers tools that could be used to conduct reports from the incidents reported via the system and provide statistics about incident per risk category, as well. The organization's risk management should audit these reports regularly.

Nevertheless, it is possible that the risk evaluation was accurate and the culture in the target organization was not avoiding evaluating highest risk as possible. With

that being the case, no information security incident that would have met the requirements for a *Level 5* risk occurred. Even so, the organization should be aware of the evaluated risks and monitor the risks regularly.

There are known limitations regarding risk management that should be considered with the HaiPro data as well. Risk management, such as evaluating risks related to information security incident reported via HaiPro is often based on human judgement and humans are known to misperceive and systematically underestimate risks (Hubbard, 2020). Limitations regarding qualitative risk rating systems has been noted by Cox and Babayev (2005) and Hubbard (2020) who claimed the risk management is already broken and should be fixed, and that the effectiveness of risk management itself should be measured and not be based on subjective perception only.

Therefore, it is suggested that the risk management process used in the organization should be audited and evaluated at regular intervals. Risk management should also cover risk management used with the HaiPro system. If the same risk evaluation process and matrix is used with several different incident types, such as for evaluating patient safety incidents and information security incidents, it should be ensured that the process and matrix are compatible with all use cases. Instructions and education on risk management should be provided to all persons who conduct risk evaluations.

8.20 Research contribution and implications for practice

Table 18 lists the main findings in this investigation.

Table 18. Main findings on information security incident reports

Number	Finding
1	Users did not report information security incidents properly
2	Analysts of the incidents did not analyze the reported incidents properly
3	The reported incidents were not handled based on the risk of the incident
4	The reported incidents rarely lead to any actions to improve the operation and prevent a recurrence of the incident
5	The overall quality of the reported incidents was low

The main goal of chapter 8 was to determine how to improve cybersecurity in healthcare with developing information security incident reporting. The main outcome was that the quality of information security incident reports must be ensured and a proper risk-based approach on analyzing and processing the reported incidents must be implemented and maintained. By addressing the findings of this study and taking them into account in information security

incident reporting development, cybersecurity in healthcare can be improved. Next, the main research contribution and implications for practice are discussed.

The results showed that information security incident reporting should be developed by revealing several problems related to incident reporting. Incident reporting can be more familiar in a patient safety context in healthcare, even so, information security incident reporting has a potential that is yet to be utilized. In addition, a connection between information security incident reports and patient safety incident reports was shown. and information security incident reports reported with patient safety incident reports were studied for the first time. Based on the literature review described in chapter 7, this was also one of the first studies to analyze information security incidents reported in healthcare.

A total of 275 information security incident reports reported between January 1, 2018 and May 3, 2021 were obtained from one healthcare organization using the HaiPro incident reporting system and were analyzed using descriptive statistics. The analyzation provided new knowledge about incidents that employees working in a healthcare organization have reported related to information security. The results showed the variety among the reported incidents, and their analyzation indicated information security incidents have affected several different areas from information security to the operation of the organization.

One of the most interesting findings was the connection between reported information security incidents and patient safety. According to the results, the information security incidents have affected patient safety and there have been several reported information security incidents that were directly related to harm caused to a patient. This was the first time when the link between the two incident report types, information security incident reports, and patient safety incident reports have been studied.

The results provided not only information about the reported incidents, but new knowledge related to problems in reporting them. The main concern on this matter was related to the low quality of information in the incident reports. Often the most common answer or selection in the information security incident report was *Not available* (N/A), meaning that both the reporter and the analyst of the incident failed to provide any information in the field in the reporting template. The number of answers containing a question mark only or “I don’t know” were high as well. Furthermore, there was no increase in the quality of the reports observed during the studied reporting period.

Besides the missing data, another important finding were the problems related to the analyzation and processing of the reported information security incidents.

When analyzing the reported incidents, the analyst has an opportunity to provide the missing information about the incident and ask for additional information from the employees in the organization. Nonetheless, based on the research data, the analyst often failed to provide such information. In addition, proposed measures from the analyst to prevent a recurrence of the reported information security incident were often missing, even with incidents with a high estimated risk level.

The majority of the reported information security incidents in the research data were reported by nursing departments. Even so, it was unlikely that the occurrence of information security incidents had been limited to nursing departments. For example, financial departments that are known to be targeted by cyber criminals had not reported any information security incidents in the organization. These results signal that not all departments in the organization report information security incidents via the incident reporting system.

The reasons for this could be that the system itself was not familiar to other than certain nursery departments and that there was simply a lack of knowledge about what and how information security related incidents should be reported. Because the HaiPro system was developed for patient safety incident reporting, it can be assumed that the system was more familiar to certain nursery departments than other departments in the organization, and it was possible that the HaiPro system has been seen as a specific system for certain departments, not a system that could or should be used by other departments as well. There might also be guidance and or culture that support this kind of operation in the organization. At worst, the employees from the other departments do not dare to use the system if they see it as a tool that belongs to a certain department to use, and therefore they do not use this possibility to report information security incidents via the reporting system that would provide valuable information for improving the operation and prevent a recurrence of the incidents.

One can only guess what kind of unreported information security incidents could have happened in other departments. However, if some departments neglect to report information security incidents, important information will be missing, and this can lead to a situation where situational awareness is lacking in the organization. Situation awareness is important especially for the management level to help make the right decisions (Endsley, 1995). For this reason, if situation awareness is lacking, the decisions could be based on inadequate information. This can have long-term consequences if, for example, resources have been planned and spent to improve the operation and to prevent incidents in departments that have

only reported information security incidents while other departments have been ignored because they have not reported incidents.

To improve information security incident reporting, the following suggestions should be considered. Firstly, the organization must ensure that it has a clear and practical process for reporting information security incidents. This process should be applicable to all departments in the organization and the organization should have a role defined that is responsible for maintaining the process. The continuity of the role should be ensured as well so that in case of personnel changes, the role can be defined to another employee.

If there are multiple systems or processes used for incident reporting, the use of them and the cases where they would be used should be carefully planned and instructed. Using several systems or ways for information security incident reporting can be confusing to employees and it can be difficult to figure out which system to use or what process to follow. An employee can also feel that the same incident must be reported several times using different systems or processes. At worst, the employee may not report the incident at all if the process is not easy to follow. What is more, several systems can be more expensive and have higher maintenance costs compared to a single system.

Of course, if there are special needs for certain departments or functions in the organization for incident reporting, then there could be a need for more than one reporting system. For example, there could be one process and system to report information security incidents for the IT-department and another process and or system for the rest of the organization. The reasons for this kind of arrangements could be related to the skills and tools available for the employees in the IT-department that can enable a more detailed view of the incident compared to employees working in another department. Because the IT-department can be responsible for information security incident management and response as well, information security incident reporting could be integrated into the IT-department's processes such as information security incident management and therefore separated from the system used by other departments.

The data sample included only one incident reported by the IT-department. Because it is likely that more than one information security related incidents have occurred in the IT-department during the more than three-year period, this finding signaled that the IT-department has another process and or system in use for reporting information security related incidents.

Whether there are one or several ways to report information security incidents in an organization, all valid processes and their possible users should be clearly

defined. If there are no reasons to upkeep several different processes for reporting information security incidents, it could be simpler and cheaper to define and maintain one process for the whole organization. In this way, the information would be gathered via one process and by using one system. This could also make it easier to utilize the gathered data. With several different systems and processes for reporting there is a risk that the value of incident reports will be lowered if the different types of reports are difficult to compare and statistical usage is laborious. In addition, if changes to the reporting processes are needed, these changes should be performed on all systems and processes in use.

To ensure that information security incidents will be reported by every department in the organization, the reporting culture and education should be improved. Firstly, the valid reporting process or processes should be clearly defined and approved by the management. Then these processes should be communicated to all relevant employees. For example, if all information security incidents should be reported via the HaiPro system in the organization, this process should be first defined and have approvement from management and only then communicated to all employees and departments. In this way, management support has been ensured before the process will be communicated to all employees.

For an average employee it can be difficult to know what kind of incidents should be reported and how they are reported. Nevertheless, it is important that the employees understand why all incidents need to be reported. If the management level in the organization is unable to explain why reporting of information security incidents is needed and what value the incident reporting could provide, why would the employee report these kinds of incidents? Therefore, the importance of reporting information security incidents should be educated among the organization, and management should actively and visibly support the reporting. The education should include examples of good information security incident reports and should be available for all employees in the organizations who can potentially notice information security incidents. In a healthcare organization, there can be several tasks and jobs that include working with computers, other digital devices, and services so it would be reasonable to ask if this kind of education should be mandatory for all employees.

Considering the research data that showed missing information in the incident reports, the reporting instructions should ensure that the reporter fulfills all necessary information when reporting an information security incident. In several information security incident reports, even basic information about the incident was missing. For example, six percent of the reports did not include the nature of the incident reported and a total of 40 incidents (14 %) had no date. Without

specific date information, it can be impossible to analyze the incident report or investigate why the incident occurred.

Even though manual monitoring of the incident reports will be needed to ensure the quality of the reports, the software used for reporting the incidents could guide the reporter to report all necessary information and automatically check the validity of the given information. There was no reason found why, for example, the reporting template should allow the reporter to save an answer containing a question mark only. Besides, all unnecessary options such as "choose" should be removed from the reporting template to ensure that the reporter cannot select options that do not provide any information about the incident. In future, artificial intelligence could be used to improve incident reporting.

In the research data, more than half of all information security incident reports were reportedly related to *Data confidentiality*. The high number of this kind of incident reports signaled that incidents related to data confidentiality were reported actively in the organization. One reason behind this can be that healthcare organizations process sensitive information such as patient data including information in physical form as well. There is also a long history of handling sensitive information in healthcare and guidelines for this kind of operation can be found from the Hippocratic Oath from ancient Greece, written centuries before computers appeared (Wikipedia, 2021).

As seen in the results, there were several cases where information security incidents were reported with the *Data confidentiality* classification and caused by a human error and where the information was in physical form. An example of this kind of incident was a piece of paper containing patient information written by a healthcare employee and found in the laundry by a worker in laundry services. Considering workers in the healthcare organization's laundry services can potentially get to know sensitive information intentionally or unintentionally when working, it should be ensured that this risk has been taken into account by the healthcare organization's risk management, correctly managed, and monitored properly. What is more, this example risk does not apply to laundry service workers only, but to the whole supply chain that is related to the laundry service, including possible third parties and subcontractors. For this reason, the security measures and risk management should cover the whole supply chain. One risk mitigation for this kind of risk would be to ensure that all employees whose work duties include the possibility to get to know sensitive information have signed a non-disclosure agreement.

Proper agreements and instructions for reporting incidents in the whole supply chain could be valuable to the organization as they can reveal flaws in the processes

and provides a chance to improve the operation and prevent similar incidents in the future. For example, in addition to signing a non-disclosure agreement, the laundry worker should be instructed what to do in case she or he discovers sensitive information in a physical form such as on paper, and information on who should be contacted and how, whose duty is to write the report about the case, and, in the end, what should be done with the physical form of sensitive information? If it is known that sensitive information has been regularly found from laundry, there should be a process that includes proper disposal of sensitive information found in such a manner.

The results showed that there was a contradiction between the estimated risks and the proposed measures to prevent the recurrence of information security incidents. Even if the risks from the incidents were estimated as high, the proposed measures to prevent the recurrence of the incident could have been missing or marked as *inform about the incident*. Incidents with high risks should be carefully analyzed and the measures to prevent high risk incidents should be proposed. Even so, it can be questioned who is responsible for identifying these measures as they can require expertise, time, and effort. For an analyst of the incidents, this task can be difficult. Therefore, the escalation to a higher level or consulting with experts to prevent information security incidents at a high-risk level should be preferred. This option was rarely used at all. Risk management education should be revised and implemented for all employees evaluating risks in the organization.

Taken together, the problems in the incident reporting and the analyzation indicated a lack of situational awareness. Situational awareness is an essential part of cybersecurity and continuous security monitoring (NIST, 2012) and should be addressed by cybersecurity management. Learning from past incidents have been noted in several studies (Mehrizi et al, 2022) and cybersecurity management should be interested in learning from the reported incidents and ensuring the good quality of the reports. If low quality reports or their analyzation are observed, there should be actions from management to increase the quality of future reports.

It is difficult to learn from incidents that have been reported with inadequate information. If problems are in the analyzation of the reported incidents, the management should take actions to improve the analyzation and make sure proper measures are taken to prevent a recurrence of the incidents. Again, it is difficult to learn from incidents that have not been properly analyzed. Rigorous analyzation and proposition of improvement suggestions to all reported incidents may not be possible in practice. Hence, prioritization should be carried out based on the risk levels. This requires that the analyst must at least analyze the risks related to all

reported information security incidents and determine the proper risk category for every incident.

8.21 Limitations

This study was limited to information security incidents reported in one healthcare organization via one reporting system. It is assumed that studying reports from the national HaiPro-database would provide different results, as it contains reports from several different healthcare organizations. Limitations of this study included the reporting type as well that consisted of information security incidents reported via one reporting template. The reporting template could be different depending on the organization and therefore provide different kind of data to be studied. Additionally, the missing data and low overall quality of the reports and analyzations should be considered.

9 RESULTS AND PAR MODEL

9.1 Main findings and development of the model

Table 19 considers the main findings from the analyzed ISPs, cybersecurity awareness, and incident reporting. Table 19 consists of three columns. The column on the left describes the area of the study, the column in the middle describes the main findings on the area. and the column on the right shows the conclusions drawn based on these findings.

Table 19. Main findings and conclusions

Area	Main findings	Conclusions
Information security policies	ISPs did not consider the current or projected information security threat environment.	ISPs failed to provide vital information to users about cybersecurity in the organizational context. ISPs did not support cybersecurity awareness nor reporting of incidents.
	ISPs were focused on ensuring regulatory compliance rather than linking the ISP to the organizational strategy.	
	ISPs did not consider reporting security incidents.	
Cybersecurity awareness	Employees had not participated in cybersecurity education or training.	Cybersecurity awareness was lacking. Cybersecurity education, training and instructions were insufficient. Cybersecurity awareness did not support reporting of incidents.
	Employees were not instructed about what to do in case of cybersecurity incidents.	
	Employees had not read the organization's cybersecurity instructions.	
Incident reporting	Users did not report information security incidents properly	Incident reporting and handling of the reported incidents failed because of the problems in cybersecurity awareness. Incident reporting failed to provide accurate information to management. Management did not have information to improve the operation of the organization such as improving cybersecurity awareness and the organization's ISP.
	Analysts of the incidents did not analyze the reported incidents properly	
	The reported incidents were not handled based on the risk of the incident	

In the beginning of this study, the initial state of the model for improving cybersecurity management in healthcare was introduced. At the initial state, the model showed that three areas: cybersecurity awareness, information security policy, and incident reporting are parts of cybersecurity management and when improving cybersecurity each area should be considered. Even so, what the initial model did not describe was the relationship between these areas.

Based on the main findings described in Table 19, this study concludes that information security policies, cybersecurity awareness, and incident reporting are

interconnected parts of cybersecurity management, and that this interconnection should be considered when improving cybersecurity management in healthcare. As seen in Table 19, ISP was connected to cybersecurity awareness; cybersecurity awareness was connected to incident reporting, and incident reporting was connected to ISP. Problems in one area affected other areas as well. Therefore, improving one area is likely to have a positive affect also to the other areas.

With this information, the initial model for improving cybersecurity management in healthcare was improved. In the developed model, the three areas were connected to each other in a cyclical form and arrows were used to highlight the possibilities that improving one area can have to other areas and to visualize the cyclical nature of the improvement process.

The initial state of the model could have been expanded and widened. However, when developing the model, it was thought that a simplified model with less text would be the most suitable for highlighting the finding that ISPs, cybersecurity awareness, and incident reporting are interconnected parts of cybersecurity management, and that this interconnection should be considered when improving cybersecurity management in healthcare. A simplified model was also seen to be useful when visualizing the improvement of the model for both, future studies and for guiding improvement of cybersecurity in healthcare organizations.

Hence, in the improved model, the names of the areas were shortened. Information security policy (ISP) was shortened to *Policy*. This was justified as there were several names used for such a policy as discussed earlier, such as information security policy, data security policy or cybersecurity policy. In this context, the policy refers to the policy or policies used in the organization for cybersecurity management. Cybersecurity awareness was shortened to *Awareness* because the context was known and in the same way, the incident reporting, including handling and processing of incident reports were shortened to *Reporting*. The reporting phase could have been separated into two phases: reporting and handling of the reports. However, because in this study the two were studied together, the last phase contained both as well.

In addition to the visualization, a set of rules were included to the improved model. The purpose of these rules was to enable the model for improving cybersecurity management. In other words, without following the rules the model will not be effective. Each of these rules were based on the findings presented in this study. For example, the first rule *Policy must consider cybersecurity threat environment* was based on the findings of chapter 6, that showed that healthcare ISPs did not consider the threat environment and therefore failed to provide vital information to the next phase (Awareness). Another example considering the following rule:

The quality of incident reports is monitored and improved if necessary. This rule was based on the findings of chapter 8, that showed the low quality of reported incidents that did not improve during the analyzed time period.

The next chapter introduces the improved model.

9.2 PAR model for improving cybersecurity management in healthcare

Figure 34 describes the PAR model for improving cybersecurity management in healthcare. The name PAR derives from the first letters of each section as follows:

P = **P**olicy
A = **A**wareness
R = **R**eporting

Figure 34 shows the visualization of the PAR model. As seen in Figure 34, **P**olicy, **A**wareness and **R**eporting form a model with a cyclical nature. Similar to the initial version of the model seen in Table 3, these three areas are parts of cybersecurity management. Nevertheless, the PAR model describes the relationship between the three factors that form a cycle for continuous improvement of cybersecurity management.

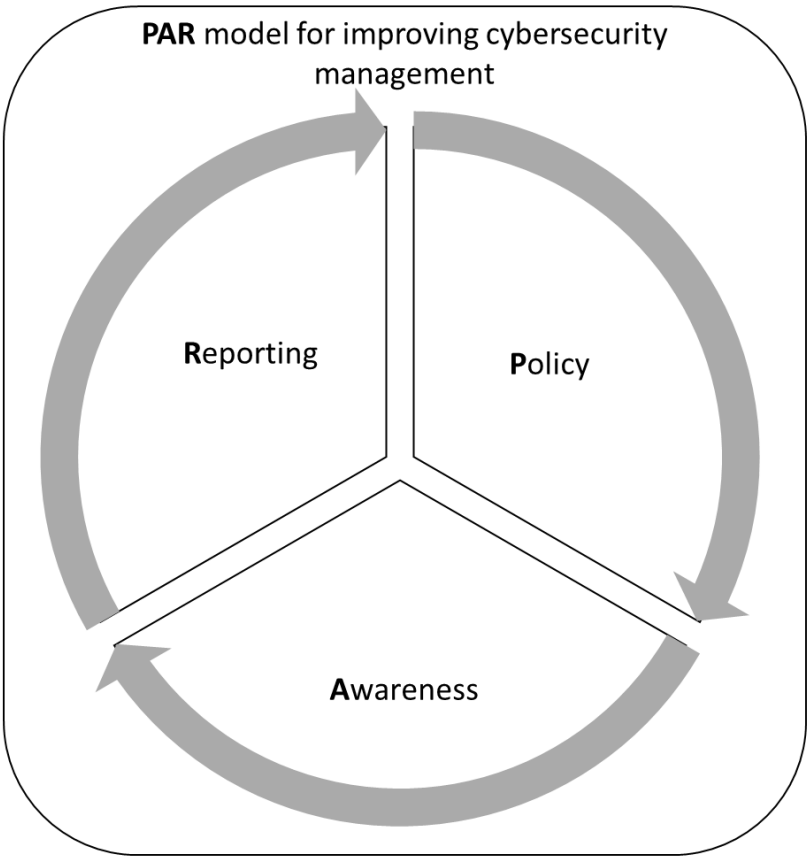

Figure 34. PAR model for improving cybersecurity in healthcare

The PAR model can be started from any of the phases. The description of the cycle begins from the **P**olicy that is approved by management. The PAR cycle goes as follows:

Policy is approved by management, and it defines the organization's objectives for cybersecurity and links cybersecurity to organizational strategy and business needs. **P**olicy considers the information provided by the previous **R**eporting phase (the arrow on the upper left) such as high-risk incidents reported and handled in the organization. The **P**olicy will be communicated to all relevant parties, and it forms a base for the **A**wareness (the arrow on the upper right).

Awareness ensures that cybersecurity education and training is mandatory for all users. **A**wareness takes care that the **P**olicy and its content is educated and instructed to all relevant parties and that they know what to do if an incident occurs and how to **R**eport incidents properly (the arrow on the bottom).

Reporting utilizes **P**olicy and **A**wareness. Users know how to report incidents properly with the help of **A**wareness and the reports are handled based on the risk evaluation which considers organization's business needs covered in the **P**olicy.

Reporting provides situational awareness and risk-based information to management. Management uses this information to improve **P**olicy and **A**wareness (the arrow on the upper left). After this, the cycle starts again with improved cybersecurity.

To enable the PAR model in cybersecurity management the following rules must be adhered to:

- **P**olicy must consider the cybersecurity threat environment.
- **P**olicy is linked to the organizational strategy and business needs.
- **P**olicy must consider reporting of cybersecurity related incidents in the organization.
- **A**wareness: Cybersecurity education and training is mandatory and regular for all employees, including the management.
- **A**wareness: Mandatory education includes reading the organization's cybersecurity instructions and policies.
- **A**wareness: Mandatory education includes instructions for what to do in case of cybersecurity incident occurs.
- **A**wareness: Users are educated to report cybersecurity related incidents properly.
- **R**eporting: The quality of incident reports is monitored and improved if necessary.
- **R**eporting: The analyzation of reported incidents is monitored.
- **R**eporting: A "risk-based" process for handling cybersecurity related incident reports is implemented.
- **PAR:** The operation of the PAR model is assessed regularly.

10 DISCUSSION

Geoff Walsham suggested in his article *Doing Interpretive Research* (2006) that interpretive research could construct contribution by considering the following:

- *Audience* (what is the primary audience of the work?)
- *Literature* (what literature is the study aiming to contribute?)
- *Claim to offer* (what does the work claim to offer that is new to the audience and the literature*?)*
- *Use* (how should others use the work?)

The primary *audience* of this study was the top management of healthcare organizations that holds the ultimate responsibility on cybersecurity in the organization, cybersecurity management professionals, and researchers interested in cybersecurity management. Stakeholders that could benefit from this study were described in more detail in chapters 10.1 and 10.2. The l*iterature* this study aimed to contribute was interpretive IS literature and literature on healthcare cybersecurity.

What this study *claimed to offer* that was new to the audience and literature was an insight to cybersecurity in healthcare by analyzing information gathered from organizations and users operating in the healthcare sector, and creating a new model that could guide cybersecurity management in healthcare with information security policies, cybersecurity awareness, and incident reporting. Lastly, it is suggested that the primary audience can *use* this study when improving cybersecurity in healthcare or when carrying out research on the subject. Additionally, this study can be used for personal reading and discussion related to cybersecurity management.

10.1 Answering the research questions

The answers to the main research question and sub-research questions SQ1-SQ7 are described below.

Main research question: What kind of model could guide cybersecurity management in healthcare with information security policies, cybersecurity awareness, and incident reporting?

The PAR model can guide cybersecurity management in healthcare with information security policies, cybersecurity awareness and incident reporting. The PAR model is described in chapter 9.2 in more detail. Additionally, cybersecurity management in healthcare requires that healthcare organizations have cybersecurity management professionals who are familiar with cybersecurity standards and frameworks and can put them into practice. This includes involving other professionals and top management in improving cybersecurity in the whole organization.

SQ1: How to improve cybersecurity in healthcare with developing cybersecurity awareness?

The level of education was low among both personnel and management due to the lack of cybersecurity management. Cybersecurity awareness must be improved starting from the management level. Multiple learning methods such as onsite and online learning should be used.

SQ2: What areas of cybersecurity management have been studied by previous literature?

Firstly, this study found out that cybersecurity management in healthcare is an emerging research topic. Previous literature has been concerned with *Ensuring compliance* with national and international standards and legislation rather than *Maintaining cultural fit* or *Balancing information security and business needs* which has been the least studied research focus in the healthcare sector. From the ISO / IEC 27001 domains, the studies often covered I*nformation security policies* and *Human resource security* whereas domains such as *Supplier relationships*, C*ryptography* or O*perations security* were the least studied domains.

SQ3: How have information security policies in healthcare been studied by previous literature?

This was one of the first studies to provide a holistic view on the literature related to information security policies in healthcare. Previous literature had focused on Monitoring and Policy Development phases and not Risk Assessment, Policy Implementation, Policy Enforcement or Policy Retirement phases. The studies were more often referring to national policies or international standards rather than to the existing organizational policies. Previous studies have been more interested in what standards and policies say about ISPs and the ISP development than analyzing ISP documents that were already in use.

SQ4: How to improve cybersecurity in healthcare with developing information security policies?

> ISPs should be improved to consider information security threats and the organization's strategy. The target group of the ISP must be defined, and the ISP should be communicated to all relevant parties. When communicating the ISP, the security measures taken should be based on the organization's information classification. The healthcare organization's top management must ensure that they have enough knowledge to take these measures into account with the ISP.

SQ5: How have patient safety incident reports been used in cybersecurity related studies?

> Patient safety incident reports have not been used in cybersecurity related studies. Only a few patient safety incident reports and IS related studies were found but no studies were found studying cybersecurity related patient safety incident reports. This was one of the first studies to address this issue.

SQ6: How to improve cybersecurity in healthcare with developing information security incident reporting?

> First, the quality of information security incident reports must be improved. Secondly, healthcare organizations must implement and maintain a risk-based approach on analyzing and processing the reported incidents.

10.2 Practical implications

The following stakeholders were identified who can benefit from the practical implication of this study: Healthcare organizations and their top management, personnel responsible for cybersecurity management, healthcare employees, policymakers, actors responsible for cybersecurity situational awareness, other parties interested in improving cybersecurity in organizations in healthcare and other sectors. The following chapters describe the overall benefits of the practical implications of this study per identified stakeholder.

Top management holds the ultimate responsibility for security of the organization including cybersecurity. In practice, top management can use the implications described to evaluate and assess the operation of their own

organization and the organization's cybersecurity management. Again, the implications can be used separately or in combination. For example, top management can use the PAR model to consider the implications for improving cybersecurity awareness and estimate whether the cybersecurity education in their organization could be improved as suggested in this study.

Cybersecurity professionals. The practical implications of this study will help personnel responsible for cybersecurity management such as CISO's (Chief Information Security Officers) to better understand how to improve cybersecurity in a healthcare context with developing awareness, security policies and incident reporting. These all have been seen as work duties and responsibilities of CISO's (Whitten, 2008) and this study can help them to perform their work in practice. The implications can be used separately or in combination. It is possible, for example, to consider the PAR model as a whole or the implications for practice about how to improve the ISP in case the organization needs a new or revised security policy.

Policymakers can use the information from this work when creating new or renewing the existing legislation. Other national actors such as cybersecurity agencies and emergency supply agencies can use the knowledge provided when creating a situational picture of the current cybersecurity situation among healthcare organizations.

Other parties interested in improving cybersecurity. Overall and in a healthcare context, this dissertation provides practical implications that can be considered when improving cybersecurity. Many of these implications can be used, besides healthcare organizations, in other sectors as well. For example, when improving cybersecurity awareness among employees, creating better security policies, or developing incident reporting, organizations can benefit from these implications despite the organizational context. In this way, the results from this work can benefit several areas and sectors.

Adverse cyber actors. It must be mentioned that security related information such as security measures taken or missing can be used against the organizations. When considering information related to critical infrastructure organizations this knowledge could be used against the whole society. For example, information on cybersecurity weaknesses, that have been reported with information security incidents, could be abused by adverse cyber actors when planning and executing cyberattacks. The practical implications of this dissertation have been intended for improving, not weakening, cybersecurity and should be not abused or used for exploitation.

Next, the practical implications are discussed per topic.

10.2.1 Literature reviews

Cybersecurity management in healthcare – Literature review. The analyzation of the previous literature on cybersecurity management in healthcare showed that the previous studies had focused on *Ensuring compliance* rather than *Maintaining cultural fit* or *Balancing information security and business needs*. This finding was interesting because *Ensuring compliance* was emphasized in the analyzed ISPs as well. In other words, both the academic studies and healthcare organizations had emphasized *Ensuring compliance*. As stated in the socio-technical approach by Kayworth and Whitten (2010), an effective information security strategy should consider all three objectives mentioned. To improve cybersecurity, healthcare organizations and their management should consider all three objectives in their operation.

Management of ISPs in healthcare. The implications from the literature review related ISPs in healthcare were mainly theoretical. Only a few studies were found studying ISPs used in healthcare organizations. Even so, management of healthcare organizations and cybersecurity professionals could benefit from the increased research in this area and therefore should encourage and support researchers to study ISPs further in the future. In practice, the management of the healthcare organization could steer and control the studies conducted in their organization to study this area. The cybersecurity professionals in turn can contact universities and mention this gap of knowledge and help the possible researchers plan the research on the subject and offer help with the research permit application process.

Patient safety incident reporting and cybersecurity – literature review. This literature review showed that cybersecurity related patient safety incident reports have not been studied before. It was already known that patient safety incident reports had been used to improve patient safety, but it was not known if or how cybersecurity might have affected to patient safety incidents, or if by improving cybersecurity the patient safety could also be improved. This was one of the first studies to address this issue and the given research agenda for future studies will help to provide new information that can be used to improve both cybersecurity and patient safety in practice.

As a conclusion from the three literature reviews: To increase scientific research and knowledge on cybersecurity in healthcare, organizations should take an active role and support future research on the subject and encourage researchers to study

also the less studied areas such as cybersecurity and patient safety incidents or balancing information security and business needs. By increasing research on cybersecurity in healthcare would not only benefit the scientific community but help the healthcare sector to better understand cybersecurity in their operations. This will eventually lead into improved cybersecurity in healthcare, help national actors to form and maintain more accurate situational awareness on cybersecurity in healthcare, and promote policymakers to also consider this situation in future regulation.

10.2.2 Cybersecurity awareness

This study showed that the level of cybersecurity education was low in all target organizations. Furthermore, cybersecurity education was lacking among the personnel, as well as among management. It is unlikely that this level was chosen on purpose, but a result from a lack of overall knowledge regarding cybersecurity in the organizations. By considering the results of this study, healthcare organizations can improve their cybersecurity by increasing cybersecurity awareness among their employees.

It is suggested that improving cybersecurity awareness is started from top management. There are two reasons for this: First, the level of cybersecurity education among the management of healthcare organizations was low and secondly, it is the top management who holds the ultimate responsibility for cybersecurity. However, this is easier said than done. If top management has not realized that they need such an education, they are not likely to spend their time on it and this is where cybersecurity professionals and policymakers are needed.

Even if healthcare organizations were seen focusing on ensuring compliance with their ISPs, the same cannot be said about the cybersecurity awareness and education that was lacking overall. It can be questioned if the current level of cybersecurity awareness and education complied with laws and regulations for personnel security. In other words, ensuring compliance had not been considered with cybersecurity awareness and education. The lack of cybersecurity education should have been noted in audits and reported to the management. Now it remained unclear if the top management knew about the low level of cybersecurity education and awareness in the organization.

Healthcare organizations and their top management should take immediate actions to ensure that they have a specific person in their organization responsible for cybersecurity. The person responsible for cybersecurity should have time to take care of this responsibility and knowledge on how to improve cybersecurity.

Adding this responsibility to perform in addition to other duties can be difficult even for a person with cybersecurity knowledge. If the role would be defined to a person without cybersecurity knowledge the benefits can be limited. Even if a person has experience in IT, he or she may not have knowledge on how to improve cybersecurity. Knowledge of frameworks such as CSF and standards such as ISO27001 should be required. Top management should ensure that proper and regular auditing will be conducted in the organization covering cybersecurity education.

Cybersecurity professionals must revise the organization's induction and education programs and take care that they have mandatory cybersecurity education for all employees, including top management. When developing such education, cybersecurity professionals should cooperate with the personnel responsible for the education in the organization, if available, and aim to add cybersecurity into the existing education programs, whenever possible.

Cybersecurity professionals should consider two aspects when providing cybersecurity related education: a general cybersecurity education and cybersecurity education that focuses on the operation of the organization. As shown in this study, both need to be improved. The aim of the general cybersecurity education is to provide a basic knowledge on cybersecurity such as explaining what cybersecurity is or how to create secure passwords. As this is general information on cybersecurity, and it applies to all organizations without the need to focus on the organization's operation or sector, the material could be provided by a third-party organization or material that is freely available on the internet could be used. In some countries, national cyber security actors such as the National Cyber Security Centre of the United Kingdom (2022b) provide material that could be used for these kinds of purposes.

The goal of cybersecurity education that focuses on the operation of the organization is to educate employees in considering cybersecurity in the context of their organization. That is, in addition to the general cybersecurity education, the employees must be educated how to take care of cybersecurity in a healthcare organization, and especially in the organization where they are working. This is because the general cybersecurity that suits everyone, and to all organizations, does not tell how cybersecurity should be considered in the healthcare sector, or in the organization. This education should explain, for example, how cybersecurity related regulation should be considered in the healthcare sector, how cybersecurity can affect patient safety or the process for reporting information security incidents in the organization.

As seen in Figure 10, many of the respondents did not know what to do in case their computer would be infected with a malicious program, or when a critical service for their work is not available. Cybersecurity professionals must ensure that all users have been instructed on the applicable procedure for when their computer has been infected with a malicious program, and how to report cybersecurity incidents. As mentioned, there are several ways to educate employees and several different ways how people want to learn and to get information on cybersecurity. This does not mean that the person responsible for cybersecurity would have to educate all employees by themself, but to be able to coordinate and audit the cybersecurity education in the organization instead. As seen in this study, when improving cybersecurity awareness, a multiple of ways to provide the education should be used such as gamification, onsite lectures, and online courses.

It would be interesting to know how many of the target organizations had any cybersecurity management professionals hired, probably few if none. The lack of cybersecurity awareness could lead to higher risks related to cybersecurity. Because healthcare is part of the critical infrastructure, the effects of possible cybersecurity incidents will not be limited to the healthcare sector only but affect the security of the whole society. If the organization already has cybersecurity professionals, they can use the information provided by this investigation to evaluate the cybersecurity awareness in their own organization. In case similar deficiencies are observed, the cybersecurity professionals can use the suggestions presented in this study to improve the cybersecurity awareness among the employees and to justify the need for resources to this process if needed.

Policymakers should be interested in cybersecurity in the critical healthcare sector. Interestingly, the results of surveys regarding cybersecurity awareness in the healthcare sector conflicted with the results of the two national VAHTI-barometers. This finding should draw attention at a national level and among policymakers. If the differences in cybersecurity awareness between healthcare organizations are as wide as seen in this study, the policymakers should consider what actions should be taken to ensure cybersecurity awareness across the whole sector. It is unbearable if healthcare workers do not know what to do if their computers have been infected with a malicious program or when a critical service for their work is unavailable. According to the results of this study, the policymakers have failed to require and oversee how healthcare organizations take care of cybersecurity awareness among their employees.

If future improvements will be performed by increasing regulation, the policymakers should consider that to meet possible increased requirements, the organizations are likely to need more resources. In this case, it would mean that

healthcare organizations will need more cybersecurity professionals. In practice, cybersecurity professionals can be difficult to find because it is known that companies are desperate for cybersecurity workers worldwide (Fortune, 2022). The worldwide need for cybersecurity workers is likely to increase salary requests for cybersecurity professionals.

10.2.3 Information security policies

ISPs in healthcare. The analyzation of ISPs used in healthcare, provided information that will help organizations to improve their security policies and cybersecurity. None of the analyzed ISPs were fully compliant with the ISO27002 standard. Overall, healthcare organizations could improve their ISP by following the ISO27002 standard. By carefully following the standard and its guidelines when creating a new or auditing an existing policy will guarantee that all mandatory requirements for an ISP are met. Nevertheless, ensuring compliance should not be the only reason to create an ISP because maintaining cultural fit and balancing information security and business needs should be considered as well. Healthcare organizations should ensure that they have adequate knowledge, preferably cybersecurity professionals who can take these aspects into account when improving the organization's ISP. To improve cybersecurity in healthcare the persons participating in the development and approvement of the ISP should consider the following aspects when working with the policy.

The ISP must be approved by the management of the organization, and this applies to healthcare organizations as well. Still, not all ISPs analyzed contained this information. The first thing to do to improve ISPs in healthcare organizations is for top management is to ensure that they have considered and then approved their organization's ISP, and that this information has been documented, preferably into the ISP document. Without the approval from top management, the validity of the ISP can be questioned.

Before approving the policy, top management must understand its content. In practice, even if the ISP would be written by others than the persons in the organization's top management, they should require that before approving the policy, it must be presented on how the requirements for the ISP, such as in the ISO27002 standard, have been met in the policy. As mentioned, the majority of the ISPs analyzed in this study did not meet the ISO27002 requirements. If the policy to be accepted does not meet the requirements or best practices for ISP, it should not be accepted but returned to its development. The existing ISPs could be compared to these requirements as well. Again, if the organization does not have internal resources for this kind of auditing or an assessment process for the

ISP, the organization's top management should use third parties to assess their ISP against the selected requirements.

Additionally, if the ISP has been written in a way that top management does not understand its content, it should be estimated how other target groups such as employees and subcontractors could understand it. As shown in this study, more pages in the policy document does not always mean that more best practices have been followed. In practice, less can be more and a shorter policy document can meet more requirements and have more value in practice. Top management in healthcare organizations must understand that the organization's security policies, that are publicly available, and poorly written or against the best practices, can affect the view of the organization, its management, and security measures.

Before creating or renewing an ISP, the purpose of the policy should be considered. The reason why an ISP is needed must be understood by both top management and persons participating on the policy development. It can be difficult to create an ISP with a practical value if it is not known why the organization needs one. The analyzed ISPs often referred to ensuring compliance by referring to requirements from regulations, legislation, and contracts. Many stated this with one sentence, whereas one organization listed tens of different laws starting from the constitution that are affecting their ISP. Listing several different laws without further explanations signals that even the writer did not know what should be considered in the ISP and listed these laws just in case.

If the main reason for creating an ISP in the organization is to ensure compliance, it would be a good idea to clearly define and document what are the guidelines followed in this work such as standards or best practices. After this, it should be ensured that these guidelines have been followed. This will not only provide information about the used frameworks for a possible auditing process but help to renew the ISP in case the selected standards or best practices will be updated or changed.

As the majority of the analyzed ISPs did not meet the ISO27002 requirements, healthcare organizations had not ensured compliance in accordance with the standard rather than ensuring that they have a policy document. The results from were seen in long and disorganized ISP documents. Even if the main reason for creating the ISP would be to ensure that the organization has such a document, the usability of the document should not be forgotten. An ISP that is long and rich in professional terminology, may be difficult to understand and consider in practice.

It should be cybersecurity professionals who are able to consider, use and refer to relevant standards and best practices such as the ISO27002 standard when

creating and renewing the organization's ISPs. Now the ISPs analyzed did not include, for example any consideration for the current or projected information security threat environment. This does not only give an impression to the public that the healthcare organizations and their cybersecurity professionals may have forgotten to add the estimated threat environment to the organization's ISP's top priorities, but that they may have not even considered information security threats. None of the ISPs analyzed considered information security threats to their operation or how to protect from them in their ISP. This finding was surprising as healthcare organizations are dependent on cybersecurity and the ISP is known to be one of the most important information security controls.

To improve the situation, healthcare organizations must ensure that they first know what information security threats are and use the skills of cybersecurity professional to form a picture about the organization's information security threat environment. Then the cybersecurity professionals should describe in the ISP how this threat environment has been considered in the organization's operation. It will not be enough, if the cybersecurity professionals or other writers of the policy can write an ISP, but they must be able to describe how the ISP and its content will be taken into action. This must be required by top management as well. If the organization's current or projected information security threat environment contains information that cannot be published, such as information that could be used against the organization, yet the ISP is still published, the threat environment should be presented in a way that does not risk the organization's operation.

As required in the ISO27001 standard, organizations should have a documented process for managing information security incidents. In practice, these processes describe how the organization manages information security incidents, events, and weaknesses (ISO27001, 2013) to ensure quick, effective, and an orderly response. Even though the process document itself can contain information that is marked as confidential and should not be published, the analyzed ISPs did not mention that the organizations have this kind of processes but referred to different types of deviations and sanctions when referring to exceptions instead. If the organization does not have such a process documented, it should be created. The ISP should tell whether the organization has procedures for incident management or not, and the users should be encouraged to report all information security incidents rather than intimidate them with possible sanctions.

Another major flaw in the studied ISPs was that only a few ISPs addressed requirements created by the organizational strategy. Once more, this provides an impression available to the public that healthcare organizations, and their cybersecurity professionals, have not added a description to the ISP on the

connection between the ISP and the organization's strategy. It even seemed like the ISP was something separate from the strategy of the organization. At worst, this may be true; the ISP may have not been connected to the organization's strategy at all, but created as a separate policy document.

Referring to the Socio-technical approach by Kayworth & Whitten, (2010), an effective information security strategy considers three objectives: Ensuring compliance, maintaining cultural fit, and balancing the information security and business needs. These objectives should be seen also in the organization's ISP. Now the analyzed ISPs did not cover any of these objectives. Top management must ask before approving the policy; How is this policy going to support our organization's strategy? Likewise, the cybersecurity professionals should be able to describe how the organization's strategy has been considered in the ISP.

After the ISP has been approved by top management, the policy must be communicated to all relevant parties such as the employees of the organization and external parties. Several studied ISPs failed to describe to whom their ISP will be communicated to. The persons creating or renewing the ISP document should ensure that they define the target group of the policy, and preferably add this definition to the policy document. In this way, the reader from the top management to all relevant parties will know to whom the policy is targeted.

When planning the communication of the ISP, cooperation with communication professionals is recommended. The owner of the policy document such as CISO or other employee leading the work should determine the level of confidentiality for the policy document. One of the reasons for determining the confidentiality level is to help in selecting the proper level of protection for the document.

A proper communication channel and media should be chosen for the ISP. For example, an ISP marked as public information can be accessed by anyone and could be available on the organization's public website, whereas an ISP marked as internal should be available for the organization's employees only and available on the organization's internal website, but not on the public website. Using the organization's existing information classification policy when determining the confidentiality of the ISP is preferred. In case the organization does not have such a policy; it should be created.

Again, all relevant parties should be considered when choosing the level of confidentiality for the ISP. If the ISP will be marked as internal and published on the organization's intranet, it should be planned how external parties can reach the document when needed. If all employees are meant to follow the ISP, the level of confidentiality cannot be defined at the highest possible if it will prevent

communicating the policy to them. As seen in this study, some of the healthcare organizations had published their ISP with a note that the policy document can be found from the organization's restricted intranet only, even if they were all available on the public internet. What is more, one organization had marked the ISP as confidential although this ISP was available on the internet as well. The latter example meant that the organization's confidential material was available on the public internet.

Before publishing, the person responsible for the ISP should check that there is no such conflict between the ISP's level of confidentiality and the chosen level of protection. If the ISP contains confidential information that prevents communicating the policy to its target group, the benefit from such a policy can be questionable. It can be necessary to remove the confidential information to another policy document or to express the information on a more general level.

To policymakers this investigation showed that healthcare organizations have not followed one of the most recognized standards for information security policy when creating the ISP for the organization. If the target organizations had used other standards when creating the ISPs, it had not been mentioned in the policies. The policymakers should consider this information when planning new regulations or requirements for the healthcare sector. By emphasizing the importance of standards and best practices, the policymakers could help the healthcare organizations to meet the requirements for an ISP and create better ISPs overall. In addition, this could ease the work from the policymakers as they could refer to an existing standard without a need to create guidelines and instructions themselves. In this way, the policymakers could not only save their own but also the resources from the healthcare organizations.

By recommending using internationally recognized standards, the policymakers could improve the standardization in the whole healthcare sector and improve cooperation between the organizations. Organizations operating in the same sector and following the same standard could help each other to improve their cybersecurity and provide data that is more comparable. Furthermore, considering that healthcare is part of the critical infrastructure, through standardization the policymakers could improve the cooperation between all critical sector organizations and help to create a more accurate situational picture at the national level, and therefore increase the resilience of the whole society.

In private healthcare organizations, the use of standards can improve the competitiveness of the organization. It is easier to choose a company that has been audited and holds a certificate for their security, compared to a company that does

not follow a standard or does not have certification. Hence, the standardization can be a competitive factor for the healthcare organization.

10.2.4 Information security incident reports

The findings of this study have several important implications for future practice. Taken together, these implications can be used to develop better processes and tools for information security incident reporting, analyzation of the reported incidents and preventing their recurrence. Improved information security incident reporting will help healthcare organizations to improve their cybersecurity.

Previously it was known that patient safety incident reports have been used to improve patient safety in healthcare and that there have been several studies on this subject. Regardless, this was one of the first studies to study information security incidents reported in the healthcare sector. The investigation showed that studying information security incident reports can provide information that can be used to improve cybersecurity in healthcare. Furthermore, until now, information security incidents reported with patient safety incidents had not been studied.

It was also known that patient safety is a global priority and that many of adverse patient safety incidents have been preventable (WHO, 2020). Now that we know the importance of patient safety and the connection between cybersecurity and patient safety incidents, healthcare organizations should start to consider cybersecurity as a factor that can have an effect on patient safety. This is a fundamental aspect that should be considered by healthcare organizations and all stakeholders from top management and cybersecurity professionals to policymakers. Healthcare organizations should communicate that they have considered this aspect to the public as well to increase awareness and trust towards the organization and their services. Top management of healthcare organizations must address cybersecurity in their organization's strategy and operation as they often address patient safety. However, as seen with the ISPs, in healthcare the organization's strategy and ISP were often not linked to each other.

According to this study, information security incident reporting has a potential that has not yet been utilized. Continued efforts are needed to make it easier and more profitable to report information security incidents. The current reporting template, for example, should be revised and simplified in a way that will lead the reporter to fill all necessary information in the correct manner. Considering the patient safety incident reports have been reported via a nationally developed tool for years, and used to improve the operation of healthcare organizations, the

national tool for reporting information security incidents should be of interest, besides researchers, to healthcare organizations, policymakers, national cybersecurity agencies, and other critical infrastructure actors.

The reason behind the current situation can be that the potential may have not been recognized because of the lack of overall knowledge related to cybersecurity as seen in the surveys conducted on cybersecurity awareness, and because the healthcare organization has limited cybersecurity resources. Although the potential of information security incident reporting for improving cybersecurity was shown, this study also showed that there are several problems in the current incident reporting and pointed out where and how these problems occur. The identified problems occurred during the whole lifecycle starting from the reporting template and the terms used to the analyzation and actions taken.

These problems should be considered in healthcare organizations to improve both cybersecurity and patient safety. The main concern in the analyzed reports was related to the low quality of the information security incident reports and their poor analyzation. Additionally, it was shown that the reported information security incidents often did not lead to actions to prevent a recurrence of the incidents, and that this is likely due to the problems related to the quality of the reports and their poor analyzation.

To improve information security incident reporting, it is suggested that cybersecurity professionals should consider the problems shown and ensure that they have a proper process for reporting information security incidents implemented in their organization. Now it remained unclear whether the target organization had such a process. Instructions for reporting information security incidents should be a part of the organization's cybersecurity education program that is mandatory for all employees. If such a process does not exist in the organization, top management should require that cybersecurity professionals must create one and then top management must approve this process before its implementation.

It is likely that top management in the healthcare organizations are not the ones to follow or analyze the reported information security incidents. Yet, the management level should require that the reported information security incidents, their analyzations, and the actions taken to prevent a recurrence of the incidents be reported to them in a compiled form on a regular basis. Preferably, the cybersecurity professionals should participate in this reporting and be used in the analyzation of reported incidents. According to this study, and mainly because of the low quality of the incident reports and their analyzation, cybersecurity

professionals have not monitored the quality of the reports nor participated in their analyzation.

The healthcare organizations, top management and cybersecurity professionals should be interested in preventing a recurrence of the reported information security incidents. Changes such as a sudden increase in the number of reported incidents should draw attention and reasons behind these changes should be investigated. Even so, because of the limited resources, rigorous analyzation and proposition of improvement suggestions to all reported incidents, this may not be possible in practice. Therefore, a reasonable approach to tackle this issue could be to implement a risk-based prioritization to be used in the analyzation of reported information security incident reports and ensure that the limited resources are spent to prevent a recurrence of information security incidents with high risks.

10.3 Theoretical implications

In this chapter, the main theoretical implications of the dissertation are discussed. Overall, theories around cybersecurity, cybersecurity management, and cybersecurity in healthcare seem to be developing and gaining more attention in the academic world. The mix of using standards and theories can be seen in previous studies and this dissertation is no exception. Theoretical implications introduced in this dissertation such as the PAR model or combining the objectives of the socio-technical approach from Kayworth and Whitten (2010) and the domains of the ISO / IEC 27001 standard can be further developed, compared, or used otherwise in future studies. Hopefully, these implications can act as building materials for new theories when studying cybersecurity despite the target sector.

This study provided an insight into healthcare cybersecurity and the PAR model itself contributed to the existing literature on cybersecurity management in healthcare by describing the relationship between policies, awareness, and incident reporting. One of the strengths of the PAR model is that it was developed with data gathered directly from organizations and employees operating in the healthcare domain. Before this study, such a model did not exist. Even though the development of the model was based on empirically gathered data, the PAR model and its effectiveness needs future studies and testing. Next, the theoretical implications of this dissertation per chapter (chapters from three to eight) are discussed.

Cybersecurity management in healthcare is an emerging research topic and the number of studies published per year is likely to also grow in the future. Even so, this study showed several shortcomings in the previous literature regarding

cybersecurity management that can be considered in future studies. In this study, a new framework combining the socio-technical approach by Kayworth and Whitten (2010) for effective information security strategy and the ISO / IEC 27001 standard for information security management was introduced. By combining the objectives of the socio-technical approach identified in the studies and the ISO / IEC 27001 domains included, the outcome provided information about domains that have or have not been studied with the research. In practice, the framework provides quantitative data about the covered and uncovered areas of effective information security management from the literature. What is more, the use of this framework is not limited to the healthcare sector only but can also be used in other sectors in future studies.

Cybersecurity awareness in healthcare. The level of cybersecurity education was lower in the target organizations than in the organizations that had participated on the national VAHTI-barometers. This showed that even though there had been surveys and information gathering conducted regarding cybersecurity awareness in organizations at national level by a national actor, there was room for scientific research on the subject. As shown, scientific research can support the data gathered at national level but provide information from a different point of view. The results from the scientific research can conflict with the nationally gathered data as well. Without scientific research on the subject, there is a risk that situational awareness can be lacking if it is based on the data gathered by one actor only. This can lead to a situation where actions are made and resources are spent, based on insufficient information.

Management of ISPs in healthcare. This study provided one of the first synthesis on literature related to management of ISPs in healthcare. The results showed that the literature related to the topic was limited and more research in this area of study was needed. The organizational-level process model for ISP management introduced by Knapp et al. (2021) was probably used for the first time in this context. The process model was proven to work well in this kind of investigation, as it offered clearly defined phases covering the whole life cycle of ISP development. The results showed covered and uncovered phases on the literature that can be used to plan and conduct future research on the subject. In addition, the process model could be used in the same way to study the phases of ISP management, besides healthcare, also in other sectors in future studies.

ISPs in healthcare. Prior studies had shown the importance of ISP for organizations (Doherty & Fulford, 2006; Höne et al., 2002) and establishing an ISP has been seen to improve cybersecurity (NIST 2022a). Even so, the literature related to healthcare ISPs was limited. One reason for this was that studying an

organization's security practices can be difficult because organizations might not simply want to provide data on their security practices to outsiders (Kotulic & Clark, 2004). This study was one of the first studies that investigated ISPs from several different healthcare organizations. Furthermore, this study used an internationally recognized information security standard to analyze the content of the obtained ISPs and provided quantitative information about the policy documents. Besides introducing the use of ISO27002 standard on analyzing ISPs for research purposes, this study showed that information security related material can be found from the internet and can encourage future researchers to search and gain research permits from organizations to provide new information on this important topic in all sectors.

Patient safety incident reports and cybersecurity. Systematic reporting of incidents was known to be an important factor in preventing adverse patient safety incidents and to increase patient safety (Kohn et al., 2002). The prior literature reviews had concentrated on studies about patient safety incident reporting systems in general (Brunsveld-Reinders et al., 2016) or to their effects on patient safety (Stavropoulou et al., 2015). It was also known that healthcare had suffered from cyberattacks (Ghafur et al., 2019; Choi et al., 2019) and that the sector has been targeted by adverse cyber actors (Jalali et al., 2020). This study provided an analysis of the literature on patient safety incident reports and cybersecurity. Only a few patient safety incident reports and IS related studies were found but no studies were found studying cybersecurity related patient safety incident reports. This was one of the first studies to address this issue. A future research agenda with example research questions were presented by utilizing the the Socio-technical approach from Kayworth and Whitten (2010).

Information security incident reports in healthcare. This was one of the first studies to study information security incident reports in healthcare. Beforehand it was known that gathering information security related data from organizations for research purposes can be difficult and that organization may not be willing to give such information to researchers (Kotulic & Clark, 2004). In addition, the previous literature review revealed a gap of knowledge in information security incident reports reported via the HaiPro system in healthcare. In this study, these two gaps of knowledge were considered, and information security incident reports reported via HaiPro in one healthcare organization were studied. As seen in the literature review, access to the incident reports reported via HaiPro system was easier to get directly from a healthcare organization using the system, compared to the organization controlling the research on the national HaiPro database. As a result, new knowledge was provided about incidents that employees working in a healthcare organization had reported related to information security. The results

provided not only information about the reported incidents, but new knowledge related to problems on reporting information security incidents. The results showed that information security incidents have affected directly patient safety, and this was the first time the link between the two incident reporting types, information security incident reports and patient safety incident reports has been studied. This study showed the potential of information security incident reports in healthcare and the HaiPro system for research purposes and can encourage researchers to consider them in future studies.

10.4 Reliability and validity

In their article "*A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems*" Klein and Myers (1999) list seven principles for evaluating an interpretive study. From these seven principles, the researchers are encouraged to use the appropriate principles for evaluating their interpretive study. The most fundamental principle is the first principle called *The Fundamental Principle of the Hermeneutic Circle* which the other six principles expand. The evaluation of this study against the selected principles is shown in Table 20.

Table 20. Evaluation of the study

Principle	Evaluation
1. The Fundamental Principle of the Hermeneutic Circle All human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form	This study iterated between the ISPs, awareness, and incident reporting in a healthcare context to interpret the relationship between the areas that forms the PAR model as a whole
2. The Principle of Contextualization Requires critical reflection of the social and historical background of the research setting, so that the intended audience can see how the current situation under investigation emerge	Digitalization of healthcare has been rapid. Digitalization has improved the sector but at the same time exposed it to serious cybersecurity risks such as cyberattacks. Now, healthcare sector needs cybersecurity more than ever.
4. The Principle of Abstraction and Generalization Requires relating the idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action.	The PAR model aimed at simplifying the findings of this study and the rules for the PAR model set common properties for these abstractions.

As seen in the main research question, the scope of this study was limited to three areas of cybersecurity that were chosen based on a framework published by NIST for improving critical infrastructure cybersecurity (NIST, 2022d). The main weakness of this study lies in the fact that other areas of the chosen framework were not studied, or that other frameworks for improving cybersecurity were not used. In addition, the generalizability of these results is limited because of the other frameworks used such as the ISO 27001 and ISO27002 standards and the socio-technical approach by Kayworth & Whitten (2010). During the research, several frameworks such as NIST CSF, ISO27001, ISO27002 and PRISMA were updated, and the current versions are different than the versions used in this study.

The literature reviews conducted followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al., 2009). As mentioned, the PRISMA framework has been updated during the research and the current version differs from the version used in this study. However, the literature searches were limited regarding the used search engines and search strings. There are several different search engines and databases for academic papers that were not used, and only papers written in English were included in the synthesis. What is more, the used search strings may have not captured all relevant publications even with the search engines that were used.

As discussed in more detail in chapter 4.7, the study on cybersecurity awareness among healthcare employees had several limitations. Overall, cybersecurity awareness was studied via surveys where the respondents could estimate his or her own personal level of awareness. In this study, cybersecurity awareness was not tested in practice.

The information security policies studied in this study were analyzed with content analysis, and compared to the ISO27002 standard's guidelines. Therefore, the analyzation of the ISPs was limited to the used method and standard. Different research methods and standards would have likely produced different results with the same data.

Studying information security incident reports was limited to incidents reported via one system in one healthcare organization. Even though the information security incident reports were stored in the national database, the research data sample covered reports from one organization only. Different organizations with different and probably more advanced systems and processes for incident reporting could have provided different results.

Another limitation of this study was related to the research data that was obtained from healthcare organizations operating in one single country. If repeated, the

results could differ if data would be obtained from organizations operating in other countries. Furthermore, the used research data consisted mainly of information gathered from public healthcare organizations. Using research data gathered from private healthcare organizations especially operating in several countries could provide different results compared to this study.

During the research, the healthcare sector in the target country was under major changes due to a health and social services reform. Starting from the beginning of 2023, all public healthcare organizations in Finland were reorganized into wellbeing services regions together with social welfare, and rescue services. In practice, public healthcare organizations whom the data to this dissertation was gathered do not technically exist anymore. In the reform, the responsibilities for cybersecurity including cybersecurity awareness, security policies and incident reporting will be likely reorganized as well into the new wellbeing services regions and therefore reproducing this study with these organizations will not be possible.

10.5 Recommendations for further research

Further studies are needed on cybersecurity in healthcare and this study provides them with several recommendations. Future studies should take into consideration both the results that revealed gaps of knowledge and the limitations of this study. Future research could try to repeat this study or a part of it with data from healthcare organizations operating in other countries to see if the results are different compared to the results shown in this study. In addition, the future studies could cover private healthcare organizations to expand the view from this study that mainly covered public healthcare organizations. Presumably data from private healthcare organizations would provide different results compared to this study.

Future studies should test the PAR model and study the effectiveness of the model in cybersecurity management. The PAR model could be tested by implementing the model into cybersecurity management processes in a healthcare organization, and observing and gathering data on how changes in one phase such as improved user's cybersecurity awareness affects other phases. With these kinds of settings, the model could be tested in practice and further developed. It is also possible to expand the PAR model with areas of cybersecurity that were left out of the scope of this study. In the improved model shown in this study, the reporting phase contained both reporting of incidents, processing, and handling of the incident reports. In future studies, these could be studied separately to expand the model and to provide new knowledge. As mentioned, the PAR model can be used in other

sectors as well, and therefore future studies could also test the model outside the healthcare sector.

Considering the health and social services reform and the fact that the organizations used in this study have been reorganized into new wellbeing services regions, future research should study the cybersecurity in these wellbeing services regions that are responsible for healthcare, social welfare, and rescue services. These new organizations are bigger, have more resources, and they are even more critical for society compared to the previous smaller organizations studied in this dissertation.

The link between patient safety and cybersecurity needs more investigation. Reported patient safety incidents and information security incidents in healthcare organizations offer interesting possibilities to study this connection. However, the future studies should seek also other ways such as connecting the reported incidents to other data when studying this area. As this was the first research to study information security incident reports reported via the HaiPro system, and taking into account that there is a national database for these reports, future studies should consider trying to find a way to study these reports more even though the research permit application process can be difficult and require time and effort. Future studies could for example use information security incident reports reported via the HaiPro system to study what was the root cause behind the incident, or if these incidents were connected to known data breaches, computer virus infections, or unpatched systems.

Even though the analyzation of information security incident reports in this study provided new knowledge about reported information security incidents in healthcare, and the connection between information security incidents and patient safety incidents, the research data did not contain patient safety incident reports that were linked to the information security incidents. Based on the literature review seen in chapter 7, it was known that there is a gap of knowledge considering cybersecurity related patient safety incident reports, as well. Therefore, patient safety incident reports that have been linked to information security incident reports should be studied in future.

This information could be used to improve cybersecurity in healthcare organizations and to increase patient safety by targeting cybersecurity resources to services and processes linked to patient safety incident reports. Furthermore, studying patient safety incidents that have been related to cybersecurity will provide information about healthcare services and practices that can be prone to cybersecurity related incidents. These studies could help to improve processes and practices in healthcare organizations and in the whole sector by increasing their

resilience against possible cybersecurity incidents and making the recovery process faster. A more detailed research agenda for studying cybersecurity related patient safety incident reports was provided in chapter 7.9.

As shown in this study, previous studies related to cybersecurity and healthcare had often focused on ensuring compliance in practice. Nevertheless, it can be questioned if, for example, the current level of cybersecurity awareness and education comply with laws and regulations for personnel security and could be studied in more detail in future studies. There is room for new studies focusing on ensuring compliance in the future and considering that the studied healthcare organizations had difficulties to ensure the compliance, future studies should investigate the other two objectives of the socio-technical approach. In other words, future studies on cybersecurity in healthcare should aim to study Maintaining cultural fit and Balancing information security and business needs, aspects that were often not included in the previous literature.

References

ACSC. 2022. Data security. Retrieved from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-terminology

Agency for Healthcare Research and Quality. 2015. National scorecard on rates of hospital-acquired conditions 2010 to 2015. Interim data from national efforts to make health care safer. Retrieved from https://www.ahrq.gov/hai/pfp/2015-interim.html

Angst CM, Block ES, D'Arcy J, Kelley K. 2017. When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. MIS Q. 2017;41, 893-916.

Alanazi, S., Anbar, M., Ebad, S.A., Karuppayah, S., & Al-Ani, H.A. 2020. Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. Symmetry, 12, 1544.

Alder, S. 2015. Improper Dumping of Patient Medical Records Continues. HIPAA Journal. Retrieved from https://www.hipaajournal.com/improper-dumping-of-patient-medical-records-continues-8241/

Alemzadeh, H., Iyer, R. K., Kalbarczyk, Z. and Raman, J. 2013. Analysis of Safety-Critical Computer Failures in Medical Devices. IEEE Security & Privacy, vol. 11, no. 4, pp. 14-26, July-Aug. 2013.

Alexandrou, A., & Chen, L. 2019. A security risk perception model for the adoption of mobile devices in the healthcare industry. Security Journal, 1-25.

Awanic. 2015. Handling of a patient safety incident report in the HaiPro system. Retrieved from https://awanic.fi/haipro/eng/wordpress/wp-content/uploads/2015/06/HaiPro_prosessikuva_eng3.pdf

Awanic. 2020. HaiPro: Reporting System for Safety Incidents in Health Care Organizations. Retrieved from http://awanic.com/haipro/eng/

Awanic. 2022a. Front page. Retrieved from https://awanic.fi/eng/

Awanic. 2022b. HaiPro – Patient safety incident report. Retrieved from http://83.150.87.4/haipro/20/lomake.asp?kieli=ENG

Awanic. 2020b. Ohje potilasturvallisuusilmoituksen käsittelijälle instructions for handling the patient safety incident report. Retrieved from https://awanic.fi/haipro/wordpress/wp-content/uploads/2022/02/pt-kasittelijan_ohje_12102020.pdf

Basu, S., Andrews, J., Kishore, S., Panjabi, R., & Stuckler, D. 2012. Comparative performance of private and public healthcare systems in low- and middle-income countries: a systematic review. *PLoS medicine*, *9*(6), e1001244. https://doi.org/10.1371/journal.pmed.1001244

Bhattacherjee, A. 2012. Social Science Research: Principles, Methods, and Practices. Global Text Project. Retrieved from https://open.umn.edu/opentextbooks/textbooks/79

Björck, F. Henkel, M. Stirna, J. and Zdravkovic, J. 2015. Cyber Resilience – Fundamentals for a Definition, In New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham, pp. 311, 2015.

Blanke SJ, McGrady E. 2016. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. J Healthc Risk Manag. 2016;36(1):14-24. https://doi.org/10.1002/jhrm.21230

Brown K, V. 2018. Hospitals Are Throwing Sensitive Patient Information Out With the Recycling. Gizmodo. Retrieved from https://gizmodo.com/hospitals-are-throwing-sensitive-patient-information-ou-1823960276

Brunsveld-Reinders AH, Arbous MS, De Vos R, De Jonge E. 2016. Incident and error reporting systems in intensive care: a systematic review of the literature. Int J Qual Health Care. 2016;28(1):2-13. https://doi.org/10.1093/intqhc/mzv100

Bulgurcu, B., Cavusoglu, H., & Benbasat, Izak. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 34. 523-548. https://doi.org/10.2307/25750690

Cambridge Dictionary. 2023. Healthcare. Retrieved from https://dictionary.cambridge.org/dictionary/english/health-care

Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. Health Serv Res. 2019;54(5):971-980. https://doi.org/10.1111/1475-6773.13203

Church, R. L., Scaparra M. P., Middleton R. S. (2003). Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems. Annals of the Association of American Geographers, 94(3), 491-502.

Cox, L.A., & Babayev, D.A. 2005. Some Limitations of Qualitative Risk Rating Systems. Wiley-Blackwell: Risk Analysis (Archive).

CISA. 2021. Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

CISA. 2022. Ransomware 101. Retrieved from https://www.cisa.gov/stopransomware/ransomware-101

CISA. 2023. What is Cybersecurity? Retrieved from https://www.cisa.gov/uscert/ncas/tips/ST04-001

DeSouza, E., & Valverde, R. 2016. Reducing Security Incidents in a Canadian PHIPA Regulated Environment with an Employee-Based Risk Management Strategy. Journal of Theoretical and Applied Information Technology. 90. 197.

Doherty NF, Fulford H. 2006. Aligning the information security policy with the strategic information systems plan. Computer Security 2006;25(1):55–63.

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. http://doi.org/10.22215/timreview/835

Dunn, M. 2005. The socio-political dimensions of critical information infrastructure protection (CIIP). IJCIS, 1, 258-268.

Eikey EV, Murphy AR, Reddy MC, Xu H. 2015. Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings. Int J Med Inform. 2015;84(12):1065-1075. https://doi.org/10.1016/j.ijmedinf.2015.09.006

Endsley, M.R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors: The Journal of Human Factors and Ergonomics Society, 37, 32 - 64.

ESET. 2017. Cybersecurity training in the work. Retrieved from https://cdn1.esetstatic.com/ESET/US/docs/business/ESET-Cybersecurity-Training-Survey-Data.pdf

European Commission. 2017. Raising awareness and developing training schemes on cybersecurity in hospitals. Retrieved from https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-tds-03-2018.html

European Commission. 2019. Critical Infrastructure. Retrieved from https://ec.europa.eu/home-affairs/what-wedo/policies/crisis-and-terrorism/critical-infrastructure_en

European Data Protection Board. 2022. Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations. Retrieved from https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en

EU-healthcare.fi. 2021. Hospital districts. Retrieved from https://www.eu-healthcare.fi/contact-information/public-healthcare/hospital-districts/

Evans MG, He Y, Luo C, Yevseyeva I, Janicke H, Maglaras LA. Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form. IEEE Access, 2019;7, 102087-102101. https://doi.org/10.1109/ACCESS.2019.2927195

Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. 2015. Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inform. 2015;84(6):454-467. https://doi.org/10.1016/j.ijmedinf.2015.01.010

Fernando JI, Dawson LL. 2009. The health information system security threat lifecycle: an informatics theory. Int J Med Inform. 2009;78(12):815-826. https://doi.org/10.1016/j.ijmedinf.2009.08.006

Fisher, M., & Marshall, A. 2009. Understanding descriptive statistics. Australian critical care: official journal of the Confederation of Australian Critical Care Nurses, 22 2, 93-7 .

Finlex. 1999. Laki viranomaisten toiminnan julkisuudesta, Publicity act. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Finnish institute for health and welfare. 2021. Health and social services reform. Retrieved from https://soteuudistus.fi/en/health-and-social-services-reform

Flaumenhaft, Y., & Ben-Assuli, O. 2018. Personal health records, global policy and regulation review. Health policy, 122 8, 815-826.

Fortune. 2022. Companies are desperate for cybersecurity workers—more than 700K positions need to be filled. Retrieved from https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/

Gartner. 2023. Cybersecurity. Retrieved from https://www.gartner.com/en/information-technology/glossary/cybersecurity

GDPR. 2021. What is GDPR, the EU's new data protection law? Retrieved from: https://gdpr.eu/what-is-gdpr/

GDPR. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med. 2019;2:98. https://doi.org/10.1038/s41746-019-0161-6

Gomes R & Lapão LV. 2008. The adoption of IT security standards in a healthcare environment. Stud Health Technol Inform. 2008;136:765-770. PMID:18487824

Gregor S. 2006. The Nature of Theory in Information Systems. MIS Quarterly, 30(3), 611–642. https://doi.org/10.2307/25148742

HaiPro.fi. 2015. Potilasturvallisuusilmoituksen täyttöohje. Retrieved from http://www.haipro.fi/ohjeet/pt-ilmoittajan_ohje_07032015.pdf

Hajar, R. 2015. History of medicine timeline. *Heart views: the official journal of the Gulf Heart Association*, *16*(1), 43–45. https://doi.org/10.4103/1995-705x.153008

Harvard University. 2022. Data Classification - Administrative Examples. Retrieved from https://security.harvard.edu/data-classification-table

Hautamäki, E., Kinnunen, U., & Palojoki, S. 2017. Health information systems´ usability-related use errors in patient safety incidents. Finnish Journal of eHealth and eWelfare, 9, 6-17.

He Y, Johnson C. 2017. Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. Inform Health Soc Care. 2017;42(4):393-408. https://doi.org/10.1080/17538157.2016.1255629

Hedström, K., Karlsson, F., & Kolkowska, E. 2013. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. Information Management & Computer Security, 21, 266-287.

Hegarty FJ, MacMahon ST, Byrne P, McCaffery F. 2014. Assessing a hospital's medical IT network risk management practice with 80001-1. Biomed Instrum Technol. 2014;48(1):64-71. https://doi.org/10.2345/0899-8205-48.1.64

Hemme, K. 2015. Critical Infrastructure Protection: Maintenance Is National Security. Journal of Strategic Security, 8(3), 25–39.

HHS. 2023. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS. 2022. Hive ransomware analyst note. Retrieved from https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note.pdf

HIPAA journal. 2021. HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems. Retrieved from https://www.hipaajournal.com/hvac-vendor-allegedly-hacked-access-gained-to-hospital-systems/

Hoffman, L., Burley, D. and Toregas, C. 2012. Holistically Building the Cybersecurity Workforce. IEEE Security & Privacy, vol. 10, no. 2, pp. 33-39, March-April 2012.

Hsieh, H. F., & Shannon, S. E. 2005. Three approaches to qualitative content analysis. *Qualitative health research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Hubbard, D. W. 2020. The failure of risk management: Why it's broken and how to fix it (2nd Edition). Hoboken, N.J: Wiley.

Humaidi N, Balakrishnan V. 2018. Indirect effect of management support on users' compliance behaviour towards information security policies. Health Inf Manag. 2018;47(1):17-27. https://doi.org/10.1177/1833358317700255

Höne, Karin & Eloff, J.H.P. 2002. Information security policy - What do international information security standards say? Computers & Security. 21. 402-409. https://doi.org/10.1016/S0167-4048(02)00504-7

IBM. 2022. Cost of a data breach 2022 - A million-dollar race to detect and respond. Retrieved from https://www.ibm.com/reports/data-breach

Independent security evaluators. 2017. Securing hospitals. Retrieved from https://securityevaluators.com/hospitalhack/

ISO. 2013. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html

ISO. 2015. ISO/IEC/IEEE 15288:2015. Systems and software engineering — System life cycle processes. Retrieved from https://www.iso.org/standard/63711.html

ISO. 2020. ISO/IEC 27001 information security management. Retreived from https://www.iso.org/isoiec-27001-information-security.html

IT Governance. 2022. What is ISO 27001 Information Classification? Retrieved from https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001

Jahanbakhsh M, Sharifi M, Ayat M. 2014. The status of hospital information systems in Iranian hospitals. Acta Inform Med. 2014;22(4):268-275. https://doi.org/10.5455/aim.2014.22.268-275

Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. J Med Internet Res. 2020;22(1):e16775. https://doi.org/ 10.2196/16775

Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res 2018;20(5):e10059. https://doi.org/10.2196/10059

Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S Health Care and Cybersecurity: Bibliometric Analysis of the Literature. J Med Internet Res 2019;21(2):e12644. https://doi.org/10.2196/12644 PMID: 30767908

Jylhä, V., Bates, D.W., & Saranto, K. 2016. Adverse events and near misses relating to information management in a hospital. Health information management: journal of the Health Information Management Association of Australia, 45 2, 55-63.

Karlsson, F., Hedström, K. & Goldkuhl, G. 2017. Practice-based discourse analysis of information security policies. Computers & Security. 67. 267-279. 10.1016/j.cose.2016.12.012.

Katina, P.F., Pinto, C.A., Bradley, J.M., & Hester, P.T. 2014. Interdependency-induced risk with applications to healthcare. Int. J. Crit. Infrastructure Prot., 7, 12-26

Kayworth TR, Whitten D. 2010. Effective Information Security Requires a Balance of Social and Technology Factors. MIS Q. Executive. 2010;9(3). Retrieved from https://ssrn.com/abstract=2058035

Kisekka V, Giboney JS. The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. J Med Internet Res 2018;20(4):e107 https://doi.org/10.2196/jmir.9014

Kim, K., McGraw, D., Mamo, L., & Ohno-Machado, L. 2013. Development of a Privacy and Security Policy Framework for a Multistate Comparative Effectiveness Research Network. Medical Care, 51, S66–S72.

Klein, H.K., & Myers, M.D. 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Q., 23, 67-94.

Knapp, K.J., Morris, R.F., Marshall, T., & Byrd, T. 2009. Information security policy: An organizational-level process model. Comput. Secur., 28, 493-508.

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (Eds.). 2000. To Err is Human: Building a Safer Health System. Washington (DC): National Academies Press (US); 2000. PMID: 25077248.

Kotulic, A. J., & Clark, J. G. 2004. Why there aren't more information security research studies. Information and Management, 41(5), 597–607.

KPMG. 2018. The healthy approach to cybersecurity. Retrieved from https://www.kpmg-institutes.com/content/dam/kpmg/healthcarelifesciencesinstitute/pdf/2017/cyber-report-healthcare.pdf

Kruse CS, Frederick B, Jacobson T, Monticone DK. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1-10. https://doi.org/10.3233/THC-161263

Kumar S, Henseler A, Haukaas D. 2007. HIPAA's effects on US healthcare. Int J Health Care Qual Assur. 2009;22(2):183-197. https://doi.org/10.1108/09526860910944665

Kwon J, Johnson ME. 2013. Security practices and regulatory compliance in the healthcare industry. J Am Med Inform Assoc. 2013;20(1):44-51. https://doi.org/10.1136/amiajnl-2012-000906

Leape L. 2002. Reporting of adverse events. *The New England journal of medicine*, *347*(20), 1633–1638. https://doi.org/10.1056/NEJMNEJMhpr011493

Lederman R. 2004. The Implications of Data Privacy Legislation for the Development of Hospital Information Systems. Health Inf Manag. 2004;33(1):12-17. https://doi.org/10.1177/183335830403300104

Lee, A. S., & Baskerville, R. L. 2003. Generalizing Generalizability in Information Systems Research. Information Systems Research, 14(3), 221–243. https://doi.org/10.1287/isre.14.3.221.16560

Lehto, M, & Limnéll, J. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Finland's cybersecurity: the

present state, vision and the actions needed to achieve the vision. https://urn.fi/URN:ISBN:978-952-287-368-2

Limnéll, J., Majewski, K. and Salminen, M. 2014. Kyberturvallisuus, Cybersecurity. Jyväskylä: Docendo, 2014, pp. 107.

Lowry, S., Quinn, M.T., Ramaiah, M., Schumacher, R.M., Patterson, E.S., North, R., Zhang, J., Gibbons, M.C., & Abbott, P.A. 2012. (NISTIR 7804) Technical Evaluation, Testing and Validation of the Usability of Electronic Health Records.

Magrabi, F., Ong, M. S., Runciman, W., & Coiera, E. 2010. An analysis of computer-related patient safety incidents to inform the development of a classification. Journal of the American Medical Informatics Association: JAMIA, 17(6), 663–670. https://doi.org/10.1136/jamia.2009.002444

McCumber, J. 2005. Assessing and Managing Security Risk in IT Systems: A Structured Methodology, Auerbach Publications, 2005, pp 99.

Mehrizi, M.H., Nicolini, D., & Rodon, J. 2022. How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future. MIS Q., 46, 531-590.

Merriam-Webster. 2023a. Cyber. Retrieved from https://www.merriam-webster.com/dictionary/cyber

Merriam-Webster. 2023b. Cybersecurity. Retrieved from https://www.merriam-webster.com/dictionary/cybersecurity

Ministry of Finance. 2008. Tärkein tekijä on ihminen, The most important factor is human. Retrieved from https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229

Ministry of Finance. 2009. *5 Henkilöstöturvallisuus*, 5 Personnel security. Retrieved from https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus

Ministry of Social Affairs and Health. 2008. Introduction of a reporting system for dangerous situations in health care. https://urn.fi/URN:NBN:fi-fe201504223648

Moher D, Liberati A, Tetzlaff J, Altman DG, PRISMA Group. 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med. 2009;6(7):e1000097. https://doi.org/10.1371/journal.pmed.1000097

National Academies of Sciences, Engineering, and Medicine. 2018. Improving health care worldwide: Retrieved from https://www.nap.edu/catalog/25152/crossing-theglobal-quality-chasm-improving-health-care-worldwide

National Audit Office. 2017. Investigation: WannaCry cyber attack and the NHS. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

National Health Executive. 2018. WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled. Retrieved from https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

National Cyber Security Centre of Finland. 2022. Information security. Retrieved from https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/information-security

National Cyber Security Centre of United Kingdom. 2022a. Phishing: Spot and report scam emails, texts, websites and calls. Retrieved from https://www.ncsc.gov.uk/collection/phishing-scams

National Cyber Security Centre of United Kingdom. 2022b. Advice & guidance. Retrieved from https://www.ncsc.gov.uk/section/advice-guidance/all-topics

NIST. 2012. CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model (Second Draft). Retrieved from https://csrc.nist.gov/CSRC/media/Publications/nistir/7756/draft/documents/Draft-NISTIR-7756_second-public-draft.pdf

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. 2022a. Glossary: Security. Retrieved from https://csrc.nist.gov/glossary/term/security

NIST. 2022b. Glossary: Usability. Retrieved from https://csrc.nist.gov/glossary/term/usability

NIST. 2022c. Glossary: Availability. Retrieved from https://csrc.nist.gov/glossary/term/availability

NIST. 2022d. Glossary: Confidentiality. Retrieved from https://csrc.nist.gov/glossary/term/confidentiality

NIST. 2022e. Cybersecurity framework, Inforgraphic. Retrieved from https://www.nist.gov/cyberframework/framework

NIST. 2022f. Cybersecurity framework, Questions and answers. Retrieved from https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework

NIST. 2023. Glossary: attack surface. Retrieved from https://csrc.nist.gov/glossary/term/attack_surface

Natsiavas P, Rasmussen J, Voss-Knude M, et al. 2018. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Med Inform Decis Mak. 2018;18(1):85. https://doi.org/10.1186/s12911-018-0664-0

Wiener, Norbert. 1948. Cybernetics: Or Control and Communication in the Animal and the Machine. Cambridge, Massachusetts: MIT Press.

O'Brien D, Yasnoff WA. 1999. Privacy, confidentiality, and security in information systems of state health agencies. American journal of preventive medicine, 1999;16(4), 351-358. https://doi.org/10.1016/S0749-3797(99)00024-0

OECD. 2019. Health in the 21st Century: Putting Data to Work for Stronger Health Systems, OECD Health Policy Studies, OECD Publishing, Paris, https://doi.org/10.1787/e3b23f8e-en.

OECD. 2021. Health at a Glance 2021. Retrieved from https://www.oecd.org/health/health-at-a-glance/

Office of the Data Protection Ombudsman. 2021. Scientific research and data protection. Retrieved from https://tietosuoja.fi/en/scientific-research-and-data-protection

Office of the Data Protection Ombudsman. 2022. Data breach notification. Retrieved from https://tietosuoja.fi/en/data-breach-notification

Ontrack. 2022. Hard Drive Recovery. Retrieved from https://www.ontrack.com/en-ca/data-recovery/hard-drive

Ourworldindata. 2023. Life Expectancy. Retrieved from https://ourworldindata.org/life-expectancy

Paananen, H., Lapke, M. & Siponen, M. 2019. State of the Art in Information Security Policy Development. Computers & Security. 88. 101608. 10.1016/j.cose.2019.101608.

Palojoki, S., Mäkelä, M., Lehtonen, L., & Saranto, K. 2017. An analysis of electronic health record-related patient safety incidents. Health informatics journal, 23 2, 134-145.

Park WS, Seo SW, Son SS. 2010. Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. Healthc Inform Res. 2010;16(2):89-99. https://doi.org/10.4258/hir.2010.16.2.89

Peikari HR, T R, Shah MH, Lo MC. 2018. Patients' perception of the information security management in health centers: the role of organizational and human factors. BMC Med Inform Decis Mak. 2018;18(1):102. https://doi.org/10.1186/s12911-018-0681-z

Pixabay. 2023. Medical-operation-surgery-doctor. Retrieved from https://pixabay.com/photos/medical-operation-surgery-doctor-5051148/

Päijät-Hämeen Sosiaali- ja terveydenhuollon kuntayhtymä. 2015. Tasekirja_2015. Retrieved from https://www.phhyky.fi/assets/files/2015/12/Tasekirja_2015_Phsotey-ja-liikelaitokset_valmis_9.5.2016.pdf

Renaud, K. 2012. Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches? IEEE Security & Privacy, 10, 57-63.

Renaud, K., & Goucher, W. 2012. Health service employees and information security policies: an uneasy partnership? Information Management & Computer Security, 20, 296-311.

Rousku, K., Kuivalainen, M. 2016. Information security barometer for personnel and management. https://urn.fi/URN:ISBN:978-952-251-812-5

Rousku, K., Mellin, L. Data security barometer for personnel and management. 2017. https://urn.fi/URN:ISBN:978-952-251-952-8

Said, M.B., Robel, L., Golse, B., & Jais, J.P. 2017. Security Policy and Infrastructure in the Context of a Multi-Centeric Information System Dedicated to Autism Spectrum Disorder. Studies in health technology and informatics, 235, 328-332.

Samadbeik M, Gorzin Z, Khoshkam M, Roudbari M. 2015. Managing the security of nursing data in the electronic health record. Acta Inform Med. 2015;23(1):39-43. https://doi.org/10.5455/aim.2015.23.39-43

Samhan, B. 2020. Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? International Journal of Healthcare Management, 13, 12 - 21.

Samonas, S., & Coss, D.L. 2014. The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information Security, 10.

Saranto, K., Kivekäs, E., Kinnunen, U., & Palojoki, S. 2018. Lack of Patient Data Privacy Challenges Patient Safety. Studies in health technology and informatics, 251, 163-166.

Schattner P, Pleteshner C, Bhend H, Brouns J. 2007. Guidelines for computer security in general practice. Inform Prim Care. 2007;15(2):73-82. https://doi.org/10.14236/jhi.v15i2.645

Slawomirski, L., Auraaen, A., Klazinga N. 2017. The economics of patient safety: Strengthening a value-based approach to reducing patient harm at national level. Retrieved from http://www.oecd.org/els/health-systems/The-economics-of-patient-safety-March-2017.pdf

Smet M. 2002. Cost characteristics of hospitals. *Social science & medicine (1982)*, *55*(6), 895–906. https://doi.org/10.1016/s0277-9536(01)00237-4

Sohn D. H. 2013. Negligence, genuine error, and litigation. International journal of general medicine, 6, 49–56. https://doi.org/10.2147/IJGM.S24256

SPTY. 2020. Lisätietoa HaiPro järjestelmästä ja aineistosta. Retrieved from http://spty.fi/wp-content/uploads/2020/03/Lisatietoa-HaiPro-jarjestelmasta-ja-aineistosta_paiv260419.pdf

Stahl, B., Doherty, N., & Shaw, M.C. 2012. Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal, 22.

Stachel, R.D., Morris, R., & Delahaye, M. 2015. Security breaches in healthcare data: an application of the actor-network theory.

Stakes. 2006. Potilas- ja lääkehoidon turvallisuussanasto, Patient and medical care safety vocabulary. Stakesin työpapereita 28/2006. https://urn.fi/URN:NBN:fi-fe201204193972

Stavropoulou C, Doherty C, Tosey P. 2015. How Effective Are Incident-Reporting Systems for Improving Patient Safety? A Systematic Literature Review. Milbank Q. 2015;93(4):826-866. https://doi.org/10.1111/1468-0009.12166

Schwandt, T. A. 1994. Constructivist, interpretivist approaches to human inquiry. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (pp. 118-137). Thousand Oaks, CA: Sage.

Syyrilä, T., Vehviläinen-Julkunen, K., & Härkänen, M. 2020. Communication issues contributing to medication incidents: Mixed method analysis of hospitals´ incident reports using indicator phrases based on literature. Journal of clinical nursing.

Takai-Igarashi, T., Kinoshita, K., Nagasaki, M., Ogishima, S., Nakamura, N., Nagase, S., Nagaie, S., Saito, T., Nagami, F., Minegishi, N., Suzuki, Y., Suzuki, K., Hashizume, H., Kuriyama, S., Hozawa, A., Yaegashi, N., Kure, S., Tamiya, G., Kawaguchi, Y., Tanaka, H., & Yamamoto, M. 2017. Security controls in an integrated Biobank to protect privacy in data sharing: rationale and study design. BMC Medical Informatics and Decision Making, 17.

The Security Committee. 2018. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma vuosille 2017 -2020, Implementation program for Finland's cyber strategy for 2017 – 2020. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

TEPA Term Bank. 2022. Tietoturva, Information security. Retrieved from https://termipankki.fi/tepa/fi/haku/tietoturva

Trendmicro. 2017a. Cybercrime and Other Threats Faced by the Healthcare Industry. Retrieved from https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf

Trendmicro. 2017b. The Price of Health Records: Electronic Healthcare Data In the Underground. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/electronic-healthcare-data-in-the-underground

TSK. 2017. Vocabulary of Comprehensive Security. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

TSK. 2018. Vocabulary of Cyber Security. Retrieved from https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf&file=pdf/Kyberturvallisuuden_sanasto.pdf

TSK. 2022. Comprehensive security. Retrieved from https://turvallisuuskomitea.fi/en/comprehensive-security/

Tuttle, D., Holloway, R., Baird, T., Sheehan, B., & Skelton, W. K. 2004. Electronic reporting to improve patient safety. *Quality & safety in health care*, *13*(4), 281–286. https://doi.org/10.1136/qhc.13.4.281

U.S. Department of Health & Human Services. 2017. HIPAA for Professionals Retreived from https://www.hhs.gov/hipaa/for-professionals/index.html

Vaasa central hospital. 2018. Laaturaportti 2018. Retrieved from https://www.vaasankeskussairaala.fi/globalassets/hallinnon-tiedostot/forvaltning_hallinto/hallituksen-poytakirjat/2019/29032019-hallitus-liite-laaturaportti-2018.pdf

VAHTI. 2004. Information security and performance management. Retrieved from https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2004.pdf

Vrhovec, S., & Markelj, B. 2018. Relating Mobile Device Use and Adherence to Information Security Policy with Data Breach Consequences in Hospitals. J. Univers. Comput. Sci., 24, 634-645.

Walsham, G. 1993. Interpreting Information Systems in Organizations, Chichester, New York: Wiley. 269 pages. (1994). Organization Studies, 15(6), 937–937. https://doi.org/10.1177/017084069401500614

Walsham, G. 1995. Interpretive case studies in IS research: nature and method. Eur J Inf Syst 4, 74–81 (1995). https://doi.org/10.1057/ejis.1995.9

Walsham, G. 2006. Doing Interpretive Research. EJIS. 15. https://doi.org/320-330. 10.1057/palgrave.ejis.3000589

Webster J, Watson RT. 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 2002;26(2). https://doi.org/10.2307/4132319

Weir, C. S., Douglas, G., Carruthers, M. and Jack, M. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens, Computers & Security, 28, 1-2, pp. 47-62.

White, R., Bamber, F., Bowyer, A., Leung, N., Lopes, F., Mills, L. and Williams D. 2017. Investigation: WannaCry cyber attack and the NHS. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Whitman, M. E., Townsend, A. M., and Aalberts, R. J. 2001. "Information Systems Security and the Need for Policy," in Information Security Management – Global Challenges in the Next Millennium, G. Dhillon, London: Idea Group, pp. 9-18

Whitten, D. 2008. The Chief Information Security Officer: An Analysis of the Skills Required for Success, Journal of Computer Information Systems, 48:3, 15-19, https://doi.org/10.1080/08874417.2008.11646017

Wikipedia. 2021a. Kuntayhtymä, list of municipalities in Finland. Retrieved from https://fi.wikipedia.org/wiki/Kuntayhtym%C3%A4

Wikipedia. 2021. Hippocratic Oath. Retrieved from https://en.wikipedia.org/wiki/Hippocratic_Oath

Wikipedia. 2023a. All pages with prefix: Cyber. Retrieved from https://en.wikipedia.org/wiki/Special:PrefixIndex?prefix=Cyber&namespace=0

Wikipedia. 2023b. Cybernetics. Retrieved from https://en.wikipedia.org/wiki/Cybernetics

Wikipedia. 2023c. Healthcare. Retrieved from https://en.wikipedia.org/wiki/Health_care

Wikimedia Commons. 2023. Medical institution, iron bed Fortepan 77082.jpg. Retrieved from https://commons.wikimedia.org/wiki/File:Medical_institution,_iron_bed_Fortepan_77082.jpg#file

Wired. 2021. They told their therapists everything, hackers leaked it all. Retrieved from https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

WHO. 2002. Quality of care: patient safety. Retrieved from https://www.who.int/patientsafety/worldalliance/ea5513.pdf?ua=1&ua=1

WHO. 2009. Global priorities for patient safety research. Retrieved from https://iris.who.int/handle/10665/44205

WHO. 2019. Patient safety-Global action on patient safety. Retrieved from https://apps.who.int/gb/ebwha/pdf_files/WHA72/A72_26-en.pdf

WHO. 2020. Patient safety. Retrieved from https://www.who.int/patientsafety/en/

WHO. 2022a. Universal health coverage (UHC). Retrieved from https://www.who.int/news-room/fact-sheets/detail/universal-health-coverage-(uhc)

WHO. 2022b. Global spending on health: rising to the pandemic's challenges. Retrieved from https://www.who.int/publications/i/item/9789240064911

Yee, K. 2004. Aligning Security and Usability. IEEE Secur. Priv., 2, 48-55.

Zarei J, Sadoughi F. 2016. Information security risk management for computerized health information systems in hospitals: a case study of Iran. Risk management and healthcare policy, 2016;27(9), 75-85. https://doi.org/10.2147/RMHP.S99908

Zeng X, Reynolds R, Sharp M. 2009. Redefining the roles of health information management professionals in health information technology. Perspect Health Inf Manag. 2009;6:1f. PMID:20052321

Appendices

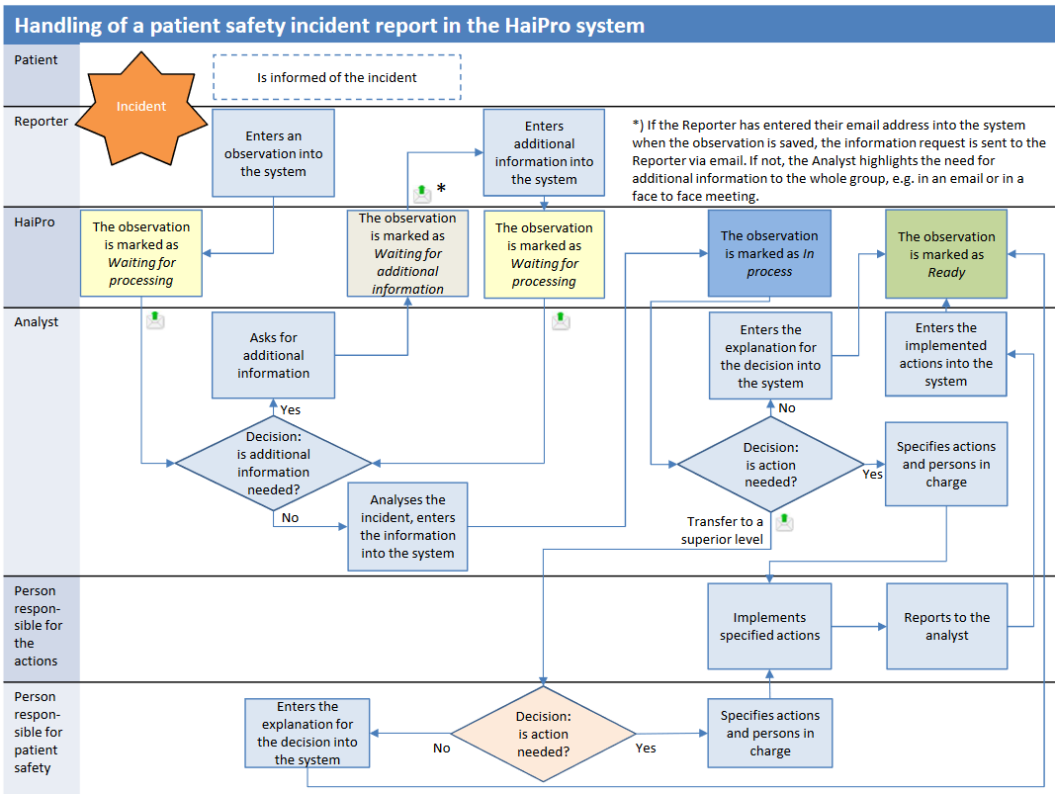

Figure 35. Handling of a patient safety incident report in the HaiPro system (Awanic, 2015)

	Harm severity				
Probability	Neglible	Minor	Moderate	Significant	Serious
Rare	Level I Insignificant risk	Level II Minor risk	Level II Minor risk	Level III Moderate risk	Level III Moderate risk
Unlikely	Level II Minor risk	Level II Minor risk	Level III Moderate risk	Level III Moderate risk	Level IV Significant risk
Possible	Level II Minor risk	Level III Moderate risk	Level III Moderate risk	Level IV Significant risk	Level IV Significant risk
Likely	Level III Moderate risk	Level III Moderate risk	Level IV Significant risk	Level IV Significant risk	Level V Severe
Almost certain	Level III Moderate risk	Level IV Significant risk	Level IV Significant risk	Level V Severe	Level V Severe

Figure 36. 5x5 Risk matrix.

Table 21. Cybersecurity management – literature review: Papers included in the synthesis.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
1999	Privacy, Confidentiality, and Security in Information Systems of State Health Agencies	O'Brien, Yasnoff	Survey questionnaire with 33 questions distributed to 52 state health agencies and the health departments in U.S., District of Columbia, and Puerto Rico.	Lack of written policies and inadequacies in policies that existed were noted. Key personnel should be educated and trained about security and technical security measures should be funded. Internal threat was ranked as number one threat to both confidentiality and security.
2004	The implications of data privacy legislation for the development of hospital information systems	Lederman	In-depth interviews of 8 total Health information managers and Managers of Health Information Services in five public and three private hospitals in Australia.	National laws and regulations for data privacy and information systems in healthcare domain can be demanding and difficult to comply with in practice. Such actions can require completely new information systems and procedures that need resources and support from regulating authorities.
2007	HIPAA's effects on US healthcare	Kumar et al.	No empirical data.	Health Insurance Portability and Accountability Act (HIPAA) was intended to improve the patient and information security in US healthcare. However, it was already outdated, confusing and difficult to comply with resulting negative effects to the healthcare sector.
2007	Guidelines for computer security in general practice	Schattner et al.	14 Semi-structured interviews with representatives from several different actors from medical software industry to government responsible for health IT, and member of health information consumer group.	The general practice guidelines for computer security included steps from getting the information from prior studies and local issues and then discussing with the IT-experts how to overcome these issues. Checklist for computer security started with making sure that there is a proper role and person working as coordinator for IT-security and security policies and procedures in place.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2008	The Adoption of IT Security Standards in a Healthcare Environment	Gomes, Lapão	Interviews and risk-level rating of ISO 27002 domains by employees in public hospital in Portugal	Although information security standards such as ISO 27002 are important to secure the cyber environment in healthcare domain, there should be more attention to put to development of practical guidelines to achieve these requirements. Responsibilities in cybersecurity management should be clearly defined in healthcare organizations.
2009	Redefining the Roles of Health Information Management Professionals in Health Information Technology	Zeng et al.	No empirical data	Roles of health information management professionals in health information technology should be clearly defined including responsibilities for cybersecurity.
2009	The health information system security threat lifecycle: an informatics theory	Fernando, Dawson	Field observations and inferences, 26 recorded interviews including standardized questions and questionnaires to clinicians in 3 large teaching hospitals in Australia. Publicly available documents such as annual reports about the hospitals.	The operation of hospitals is not supporting the regulatory environment in practice. More resources in hospitals supporting privacy and security are needed. Governments, health authorities and hospital managements should work together to improve the situation.
2010	Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds	Park et al.	Check-list type questionnaire prior interviews to two public hospitals and three private hospitals in South Korea. Interviewing responsible personnel according to the checklists.	The level of current Information security management system in the hospitals evaluated was determined to be insufficient. Legal regulations and international standards should be followed, and compliance level should be reviewed regularly.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2012	Assessing and Comparing Information Security in Swiss Hospitals	Landolt et al.	Data were collected by online questionnaire from 51 Chief Information Officers working in hospitals in German-speaking Switzerland.	Lack of patient data protection were noted. According to the survey asking 24 from 133 parameters defined in ISO/IES 27002 standard the security basics should be improved. The suggested improvement method for cybersecurity management included many administrative steps from business continuity plan and risk management process following standards and policies, security supporting management with clear security related roles and responsibilities, and information classification.
2012	Security practices and regulatory compliance in the healthcare industry	Kwon, Johnson	Telephone survey to privacy and security responsible in 204 randomly selected healthcare facilities in US (one respondent per organization).	In the organizations with highest level of compliance, audit practices and third parties breach management and training were seen as important. Cybersecurity was seen as technical issue and technical safety measures were prioritized whereas non-technical practices such as security management processes had wide differences between the organizations.
2014	Assessing a Hospital's Medical IT Network Risk Management Practice with 80001-1	Hegarty et al.	Semi-structured interviews to staff members working in a multidisciplinary team in a public hospital in Ireland.	Healthcare organizations can benefit from using 80001-1 standard in their risk management. Different stakeholders working together to comply with the standard can raise awareness and improve the safety culture in the organization.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2014	The Status of Hospital Information Systems in Iranian Hospitals	Jahanbakhsh et al.	Interviews with IT staff with several years of working experience in 7 public instructional hospitals in city of Isfahan in Iran.	Several insufficiencies and problems from unprotected servers to unclear management roles were found from the hospital's IT environment. Clear National IT strategy and the use of standardization (such as ISO 27000 family) are suggested. Even the target hospitals were under the administration of the same medical university, the systems and procedures were not standardized. Traditional ways can have an effect to the management.
2015	Analysis of health professional security behaviors in a real clinical setting: An empirical study	Fernández-Alemán et al.	Data were collected by questionnaire with 180 health professional respondents working in a public hospital in Spain.	The security behavior of healthcare professional did not meet the security standards, guidelines, or best practices. Security education, security policy and risk assessment should be improved.
2015	Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings.	Eikey et al.	Semi-structured interviews with 20 hospital IT staff members. Field observations in the same hospital.	IT staff should have more knowledge of clinical user needs and practices. The communication between the two should be improved to ensure that the patient information is protected.
2015	Managing the Security of Nursing Data in the Electronic Health Record	Samadbeik et al.	Data were collected by questionnaire with 20 respondents; 11 IT experts from computer companies and 9 IT experts from Tehran University of Medical Science's hospitals in Iran.	Both hospital information system vendors and hospital information technology specialists shared the view of information security protection and requirements. Yet, the guidelines and requirements should be improved.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2016	When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist.	Blanke, McGrady	No empirical data.	Risk assessment should be a vital part of organization's operation to prepare and avoid adverse cyber events such as data breaches. Even several stakeholders are needed to secure the cyber environment in healthcare domain, the main responsible for maintaining the risks related to adverse cyber events are the management personnel.
2016	Information security risk management for computerized health information systems in hospitals: a case study of Iran.	Zarei, Sadoughi	Questionnaire with respondents from 549 hospitals in Iran.	Only few hospitals had implemented standards such as ISO / IEC 27001 in their information security management even they had framework for information security management. Risk management process should be improved thoroughly in target hospitals from identification to treating the risks. Problems in risk management should be noted by authorities to create new practical policies to be used in the process.
2017	Indirect effect of management support on users' compliance behavior towards information security policies	Humaidi, Balakrishnan	Survey with self-administered questionnaires from 454 healthcare professionals (Health administrators, doctors, and support staff) in three public hospitals in Malaysia.	The management support had positive impact to the health professional's security compliance behavior and on the trust in organizational security policies. The organizational policies and guidelines should be written in clear language and easy to understand.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2017	Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization.	He, Johnson	A demographic background questionnaire. 15 semi-structured interviews to IT and healthcare professionals working in a Chinese healthcare organization.	Lack in gathering and distributing the knowledge about security incidents can lead into a situation where lessons are not learned, and the cybersecurity management is not improved. Reporting about the incidents to several stakeholders with different technical backgrounds were found challenging.
2018	Comprehensive user requirements engineering methodology for secure and interoperable health data exchange.	Natsiavas et al.	Definition of user scenarios, analyzing the user scenarios for user requirements, assets, threats, and business processes, Two surveys: 1. Survey with 35 respondents from healthcare providers and workers 2. Survey with 437 patients / citizen, Workshop with end-users.	The lack of cybersecurity culture in healthcare organizations was identified. Information security standards were not met. More resources should be addressed to comply with the standards and regulations and to implement cybersecurity technologies and measures and to improve the cybersecurity culture in healthcare that would eventually help exchanging the data between healthcare organizations in different countries.
2018	Cybersecurity in Hospitals: A Systematic, Organizational Perspective	Jalali, Kaiser	19 semi-structured interviews with hospital chief information officers, chief information security officers and healthcare cybersecurity experts in US.	Chief information officers and Chief information security officers should work to reduce end point complexity and improve internal stakeholder alignment. The healthcare sector should be made less attractive and vulnerable to cybercriminals ensuring that every hospital has proper resources for cybersecurity. Compliance does not guarantee security and healthcare organizations should aim higher in cybersecurity than the current regulations and policies that often tend to note data privacy but not data security.

Year of publication	Title	Authors	Research settings and data collection method	Summary of findings
2018	Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues	Jabeen, et al.	No empirical data.	In healthcare domain there are several cybersecurity related issues related to the trust and reputation management. Cybersecurity in healthcare can be improved with both soft and hard trust mechanisms.
2018	Patients' perception of the information security management in health centers: the role of organizational and human factors	Peikari et al.	Data were collected by questionnaire with 382 patients in 9 educational hospitals in Iran.	When studying the relationship of the organizational and human factors, the research concluded that technical and physical protection, staff training and monitoring can have positive impact for the patient's trust and the perceived security in hospital. Yet, no clear connection between perceived information security and physical protection mechanisms was found.
2018	EARS to cyber incidents in health care	Jalali et al.	No empirical data.	Response plans with prevention and detection capabilities are essential for healthcare organizations.
2019	Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form	Evans et al.	Survey with 485 respondents working in a private healthcare organization.	From employee perspective the cybersecurity can be improved, and risk of cybersecurity incidents caused by human errors decreased by organizational focus on its employees and their environmental factors.

Table 22. ISPs compared to ISO27002 guidelines

ISP guidelines	**Organization**																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
ISP contains a note that it has been pproved by the management	x	x	x	x	x	x	x	x	x	x		x		x	x	x		x	x	x	x
Published and communicated to employees	x	x			x	x	x	x		x	x		x	x		x	x	x			
Published and communicated to relevant external parties	x	x			x	x	x	x		x	x		x	x		x	x	x			
The ISP address requirements created by:																					
Business strategy										x	x			x	x		x		x		
Regulations, legislation and contracts	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
The current and projected information security threat environment																					
The ISP contains statements concerning:																					
Definition of information security	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Definition of objectives and principles to guide all activities relating to information security	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x
Assignment of general responsibilities for information security management to defined roles	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
Assignment of specific responsibilities for information security management to defined roles	x		x		x	x		x	x	x	x		x	x		x	x		x	x	x
Processes for handling deviations and exceptions	x	x		x	x	x	x	x	x	x	x		x		x	x	x	x		x	x