UPPSALA
UNIVERSITET

UPTEC STS 21016
Examensarbete 30 hp
Maj 2021

Improving information security in the healthcare industry without interfering with patient care

Amanda Utterbäck

Civilingenjörsprogrammet i system i teknik och samhälle

UPPSALA UNIVERSITET

Improving information security in the healthcare industry without interfering with patient care

Amanda Utterbäck

Abstract

The constantly evolving digital landscape has accelerated the need for companies to implement and adopt sustainable and effective information security. This has resulted in great opportunities within the healthcare industry to improve information security in line with the increasing demand for care and nursing services. This development has, however, also created many challenges within the healthcare industry. It can be difficult for healthcare organizations to effectively manage the security risks related to employees since many healthcare organizations already are struggling to meet the needs of their clients and patients that exist due to a shortage of staff. The aim of this thesis was therefore to develop a framework for how healthcare organizations can act to manage the human factor of information security without taking time and resources from patient care. To meet this purpose, a proposed framework was developed through a literature review which was later evaluated through data collected by conducting semi-structured interviews with a variety of different healthcare organizations, where the interviewees held a range of roles within the organizations.

The results suggests that healthcare organization can improve their information security related to their employees by first establishing an information security policy that includes guidelines for all employees and ensure compliance of that policy. To ensure compliance leaders within the organization must manage and implement information security. To make this possible the organization must take action to improve management's information security awareness. When management has a high level of information security awareness, sufficient resources will be devoted to information security work. Furthermore, management will utilize strategies such as creating information security awareness, reducing perceived inconvenience, as well as developing a strong ethical climate to improve employee's information security policy compliance. Information security policy compliance will also over time lead to the development of an information security culture, which will further strengthen the information security in the organization.

Teknisk-naturvetenskapliga fakulteten

Uppsala universitet, Uppsala

Handledare: Anton Ydrefors Ämnesgranskare: Mike Hazas

Examinator: Elísabet Andrésdóttir

Acknowledgements

There are many people who have been invaluable throughout this process, without whom I would not have been able to complete this master thesis.

First, I would like to express my sincere appreciation and gratitude to my supervisor, Anton Ydrefors from Omegapoint, for his continuous support and valuable insights. His guidance has been extremly valuable during this researcher and during the writing of this thesis.

Additionally, I would like to thank my subject reader Mike Hazas at Uppsala University, for the persistent help and feedback and for consistently reviewing my work.

Lastly, I like to extend my thanks to the interviewees who participated in this study for sharing their valuable perspectives and knowledge. This research would not have been possible without their inputs.

Populärvetenskaplig sammanfattning

Den snabba digitaliseringen av hälso- och sjukvårdssektorn har resulterat i fantastiska möjligheter för vårdorganisationer att bli effektivare för att möta den ökande vårdbehovet samt förbättra tillgängligheten av vård- och omsorgstjänster (Sveriges läkarförbund n.d). Utveckling har dock också lett till ökad sårbarhet och informationssäkerhetsrisker (Stewart and Jürjens 2017). Den ökande användningen av informationssystem inom hälso- och sjukvården resulterar i högre krav på informationssäkerhet (MSB n.d.). Flera organisationer inom hälso- och sjukvårdssektorn har under de senaste åren utsatts för attacker där känslig information hämnat i fel händer. Till exempel attackerades en klinik i London år 2017 med ransomware och nu flera år senare har patienterna utpressats med foton som hackarna kom åt under intrånget. Samma sak hände också i USA år 2019 och år 2020 igen i England (Hellerud 2021). En annan attack som drabbade vårdsektorn var WannaCry som skedde år 2017. WannaCry var en ransomware-attack som krypterar all data på den infekterade enheten vilket hindrade flera sjukhus från att fungera normalt (Gisel and Olejnik 2018).

Det är uppenbart att det är viktigt för organisationer inom hälso- och sjukvårdssektorn att utveckla en hög nivå av informationssäkerhet och i detta arbete är de anställdas beteenden en viktig aspekt. Forskning har visar att människor är den svagaste länken i säkerhetskedjan och att människor ofta är grundorsaken till säkerhetsintrång. Den mänskliga faktorn i hanteringen av informationssäkerhet spelar därför en viktig roll (Connolly et al. 2016). För att hantera informationssäkerhetsrisker relaterat till anställda rekommenderar svenska myndigheter organisationer att följa en standard som kallas ISO 27001 (MSB n.d.). Enligt ISO 27001 kan en organisation effektivt hantera säkerhetsriskerna relaterade till anställda genom att se till att alla anställda har tillräcklig kompetens för att på ett säkert sätt hantera känslig information. Organisationer bör därför tillhandahålla informationssäkerhetsutbildning till alla anställda som inte har den kompetens som behövs (International Organization for Standardization 2017).

För vårdsektorn innebär detta dock stora utmaningar eftersom många vårdorganisationer har en stor personalbrist som gör det svårt att tillgodose de vårdbehov som finns (Ström 2019). Att genomföra informationssäkerhetsutbildning för alla anställda blir därför svårt. Det finns därmed ett behov av en strategi som kan förbättra informationssäkerheten relaterad till anställda utan att ta tid och resurser från vården av patienter. Syftet med denna studie var därför att utveckla en modell för hur organisationer inom hälso- och sjukvårdssektorn kan agera för att hantera den mänskliga faktorn av informationssäkerhet utan att ta tid och resurser från vården av patienter. För att uppnå detta syfte utvecklades en modell genom en litteraturstudie. Modellen utvärderades sedan med hjälp av data som samlats in genom semistrukturerade intervjuer med ett antal olika vårdorganisationer, där de som intervjuades hade en rad olika roller inom organisationerna.

Resultatet visar att organisationer inom hälso- och sjukvårdssektorn kan förbättra informationssäkerheten relaterat till sina anställda genom att först upprätta en informationssäkerhetspolicy som innehåller riktlinjer för alla anställda och sedan säkerställa att policyn följs. Om policyn följs kan organisationen säkerställa att de har den nivå av informationssäkerhet som anses nödvändig. Resultaten visade vidare att ledare inom en organisation har en viktig roll i att säkerställa att policyn följs. Det är därför viktigt att organisationer vidtar åtgärder för att förbättra ledningens kunskap kring informationssäkerhet. När ledningen har en hög nivå av informationssäkerhetsmedvetenhet kommer tillräckliga resurser att ägnas åt informationssäkerhetsarbete och ledare har bättre möjligheter att säkerställa efterlevnad av informationssäkerhetspolicyn. Ledare kan vidare framhäva efterlevnad av policyn utan att ta tid från vård av patienter genom att förbättra anställdas informationssäkerhetsmedvetenhet, minska det upplevda besväret, samt arbeta för att utveckla ett fördelaktigt etiskt klimat. När de anställda följer riktlinjerna skapas fördelaktiga informationssäkerhetsbeteenden som i längden dessutom kommer leda till en informationssäkerhetskultur, vilket ytterligare stärker informationssäkerheten i organisationen. Organisationer kan också komplettera detta arbete med att implementera tekniska säkerhetslösningar som kan lindra vissa av de säkerhetsrisker som anställda medför.

Contents

1 Introduction

The fast development of information technology has resulted in many opportunities for companies to improve their efficiency and increase overall performance. However, these rapid developments also lead to increased vulnerability and security risks (Stewart and Jürjens 2017). Information systems are constantly threatened by potential cyberattacks (Khan et al. 2020), where the confidentiality of personal and commercially sensitive data may be compromised (Connolly et al. 2016). Cybercriminals have, over the past few years, successfully managed to find ways to develop sophisticated malware specifically designed to attack their intended target (Khan et al. 2020). A critical challenge for today's organization is therefore figuring out how to reduce the risk of these attacks through improving their information security. Protecting sensitive data, now more than ever, plays a significant role within the organization. Organizations must protect their information and assets to sustain their value and reputation, as well as obeying laws and regulations (AlGhamdi, Win, and Vlahu-Gjorgievska 2020).

One of the industries which is specifically being challenged and forced to adapt due to the increasing rate of digitization is the healthcare sector. This has created great opportunities for healthcare organizations to become more efficient in order to meet the increasing demand for care and nursing services, as well as to improve the accessibility of their care (Sveriges läkarförbund n.d). The increasing use of information systems within healthcare, however, also results in higher demands for information security (MSB n.d.), in order to ensure the confidentiality, integrity, and availability of data[1] (Andress and Leary. 2017 and 2016, p. 3). Several organizations in the healthcare sector have in recent years been exposed to attacks where critical information has been compromised. For example, in 2017, a clinic in London was hacked with ransomware and now several years later, the patients have been blackmailed with photos that the hackers were able to access as a result of the attack. In 2019, a similar attack occurred in the US and in 2020 again in England (Hellerud 2021). Another notable attack that affected healthcare sector was the WannaCry ransomware attack in 2017 that encrypted all data on the infected device and prevented medical facilities from operating normally, creating a significant amount of down-time for the organization (Gisel and Olejnik 2018).

It is becoming increasingly clear that it is vital for organizations within the healthcare sector to develop an adequate level of information security. In order to achieve this level of information security, one of the most critical factors is managing employee behavior. Security issues related to employees and employee activity can be observed in many organizations (Stewart and Jürjens 2017). Recent research presents evidence that employees are the weakest link in the security chain and that employees are in fact often the root cause

[1]Confidentiality, integrity and availability creates the CIA triad which is a security model that highlights core information security objectives. The CIA triad can be used as a guide for organizations to keep their sensitive information secure (Andress and Leary. 2017 and 2016, p. 3).

of security breaches. The human factor in information security management therefore plays a critical role (Connolly et al. 2016). The International Organization for Standardization has addressed this in a standard called ISO 27001. ISO 27001, which Swedish Authorities advise organizations to implement (MSB n.d.), states that an organization can effectively manage the security risks related to employees by ensuring that all employees have adequate skills to keep information secure by providing information security training when necessary. More specifically, the organization should according to ISO 27001 first determine the necessary competence related to information security among employees. Once the necessary competence required is established within the organization, the organization must then work towards ensuring that all employees have the required competence on the basis of appropriate education, training, or experience. Furthermore, the organization should then evaluate the efficiency of these actions and maintain appropriate documentation as evidence of competence (International Organization for Standardization 2017).

For the healthcare sector, this new reality poses a tremendous challenge due to the fact that healthcare professionals in many cases work in a very stressful environment. Many modern healthcare organizations are experiencing issues related to staff shortages, which leads to challenges in meeting the care needs that exist for their patients (Ström 2019). This creates significant barriers and difficulties associated with managing employees as a strategy to reduce security threats. Providing all employees with relevant training as well as continuously making sure that all employees have adequate skills in line with ISO 27001 can present a challenge as the process of providing and maintaining training for employees in these areas is costly both in terms of time and resources. These barriers may ultimately result in increased information security risks, as healthcare organizations become less willing to take the necessary precautions to maintain their information security. There is therefore a need for a strategy that can improve information security related to employees without taking time and resources from patient care.

1.1 Purpose and research questions

The aim of this thesis is to develop a framework for how healthcare organizations can act to manage the human factor in information security without taking time and resources from patient care. This results in the following research questions:

1. How can organizations, according to the literature, act to improve their information security related to employee's behavior without taking time and resources from employee's main work tasks?
2. Can the strategies proposed in the literature be practically implemented within healthcare organizations?
3. How can technical security controls help mitigate the information security risks that the human factor contributes to?

2 Literature Review

In this section, the results from the literature review will be presented and later summarized in a proposed framework. The literature review aims to investigate how the level of information security related to employee's behaviors can be increased without taking time and resources from employee's main work tasks.

2.1 Information security policy

It is evident in the literature that the first step organizations must take in order to manage the human factor of information security is to create information security policies (ISP) that guide employees towards beneficial information security behaviors (Karlsson, Hedström, and Goldkuhl 2017). The information security policy should include guidelines, requirements and rules that are set forward by management in order to guide employees who work with information systems and by that enhance the information security within the organization. The policy will ensure that employees and other users know how they should act in order to keep information within the organization secure. The information security policy should be designed to mitigate all security risks that have been identified by the organization (Koohang, Anderson, et al. 2019;2020;). Researchers within the field of information security agree that establishing an information security policy that includes information security guidelines for all employees is critical in order to effectively protect information systems (Sohrabi Safa, Solms, and Furnell 2016; Koohang, Anderson, et al. 2019;2020; Yazdanmehr, Wang, and Yang 2020). Research carried out by Stefaniuk (2020) shows that the observed information security behavior among employees improved by 12% through employee awareness of a security management system. After the document "Information security policy" was published by the organization, Stefaniuk (2020) observed improvement increased to 18%.

As stated above, many articles emphasize that information security policies are necessary in order to achieve an adequate level of information security related to the employees of an organization (Koohang, Nowak, et al. 2020). However, previous research has shown that many employees do not comply with the organization's policy even though guidelines and rules are in place (Sohrabi Safa, Solms, and Furnell 2016). Chen, Ramamurthy, and Wen (2015) argue that *"merely having security policies in place without making sure that they are fully understood and favorably perceived by employees cannot instill the purpose of such policies among employees, and consequently, the effect of policies would be marginalized."* It is hence clear that organizations can not only rely on the existence of information security policies, they must also make sure that the employees comply with set polices. The importance of information security policy compliance in organizations is evident in the literature and several studies have investigated the underlying factors contributing to employee's information security compliance. The most prominent factors in the literature will be presented in the following section.

2.2 Information security policy compliance

2.2.1 Information security awareness

There is a consensus among researchers within the field of information security regarding the positive effect that awareness has on employees information security compliance (Koohang, Nowak, et al. 2020; Koohang, Anderson, et al. 2019;2020;). When employees are aware of potential threats against information systems and understand the importance of information security, they will to a greater extent comply with the organizations information security policies. Stefaniuk (2020) identifies two general definitions of information security awareness in the literature. The first definition is that information security awareness is the same as having knowledge about information security threats and ways to prevent them. The second involves the employee understanding the importance of information security, how to act, and knowing their individual security-related responsibilities. Stefaniuk (2020) explains that *"this approach grades awareness levels making it possible to create models of measuring information security more precisely. Having information security knowledge is the initial (lowest) degree of awareness."* The author emphasizes that knowledge is only beneficial when it leads to a positive attitude towards information security. It also requires a belief that certain actions must be taken to protect the organization's information systems. This will lead to the final stage of security awareness which is adequate employee behavior. The different stages of awareness can be seen in Figure 3 below.

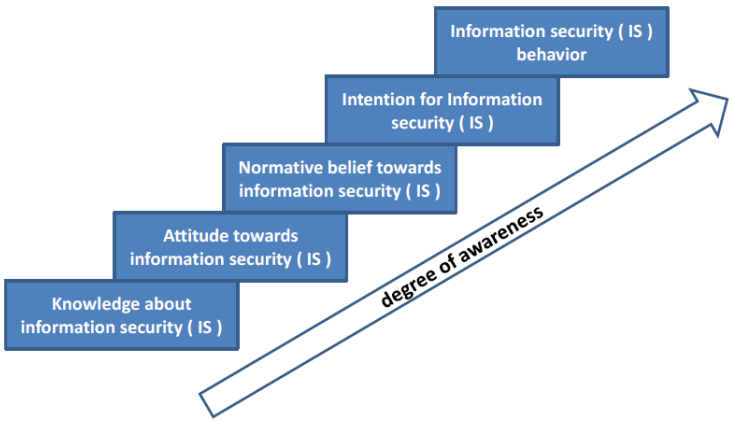

Figure 1: Degree of information security awareness [Image from: (Stefaniuk 2020)].

The most common and prominent strategy to create security awareness among employees is to implement security education and training (SETA programs) (Koohang, Nowak, et al. 2020; Gangire, Veiga, and Herselman. 2019; Koohang, Anderson, et al. 2019;2020;). *Research results show significant effectiveness of training as a method not only of information security knowledge extension but also, and most importantly, one that has a significant impact on actual behaviors of employees in the studied area* (Stefaniuk 2020).

This literature review will however focus mainly on other strategies to enhance the security awareness

among employees since training will take time from employees main work tasks. Hwang, Wakefield, et al. (2019) explore how information security experiences and observations in the workplace leads to increased security awareness through the principles of social learning theory, which is a theory of behavior replication. The social learning theory describes how an individual obtains knowledge, learns, and reproduces behavior by observing others performing a certain behavior. Through their research, Hwang, Wakefield, et al. (2019) concluded that information security awareness occurs when employees are, in addition to education, exposed to security policy, security visibility and management security participation. Security policies will contribute to awareness since they will, when clear and concretely presented, raise security knowledge and skill levels for favorable compliance behavior. Security visibility is the extent to which employees observe information security processes, information security activities and security incidents in the organization. This will create awareness since memory of the phenomenon will contribute to the learning process. Finally, management participation in security will positively influence employees' security awareness since managers possess greater social status and their involvement in security programs, procedures and protocols will capture the attention of subordinates (Hwang, Wakefield, et al. 2019).

In addition, Sohrabi Safa, Solms, and Furnell (2016) explain the importance of social interaction. Through social interaction knowledge-sharing will take place and increase the information security awareness among employees. The values of the social group that the individual interacts with have an impact on the user's view on awareness. Employees can gain information security awareness through conversations with friends (Haeussinger and Kranz 2017).

2.2.2 Perceived inconvenience

Perceived inconvenience is another important factor related to information security compliance (Ahmad et al. 2019; Hwang, Wakefield, et al. 2019; Sharma and Warkentin 2019). Ahmad et al. (2019) stress that when the desired security behavior is perceived as inconvenient by the employees, they tend to abandon it. The authors further explain that: *"Security assurance behavior involves additional steps taken by employees in ensuring information security. These steps may slow down their work and thus pose an inconvenience to the employees."* In line with this, Hwang, D. Kim, et al. (2017) explain that restriction on working procedures and actions due to the compliance of security policies is found to be a major cause of non-compliance. The restrictions that security policies may cause is referred to as work impediments. If complying with information security causes work impediments, employees may adopt non-compliance behaviors. However, Han, Y. J. Kim, and Kim. (2017) explain that once employees understand the benefits with ISP compliance, they are more likely to adopt security behaviors in line with the organization's information security policy. Therefore, managers need to find a way to communicate the benefits and importance of information security that outweigh the perceived inconvenience (Han, Y. J. Kim, and Kim. 2017).

Sharma and Warkentin (2019) argue that the perceived response cost, which is the personal costs of performing the suggested adaptive behavior, has a significant impact on the intention to comply with security policies. Response cost can appear in a number of forms, including time, money, and effort. This suggests that *"when an employee believes that there are costs of performing an activity or complying with a policy, he may decide against it, whereas in the absence of any response cost, he would have complied"*. This phenomenon seems to have weaker effect on permanent employees since they are more invested in the company. The results of the study also reveal that higher level of commitment from employees to the organization will reduce the effect of response cost since employees are more committed to the organization's policy. In addition D'Arcy and Lowry (2017 and 2019) found that an employee's daily compliance attitude is determined by evaluating the benefits of compliance and the costs/risks of non-compliance (D'Arcy and Lowry 2017 and 2019).

2.2.3 Organizational commitment

As previously shown, the literature describes that commitment is another important factor influencing employee's information security policy compliance (Change, Liu, and Jang 2017; Sohrabi Safa, Solms, and Furnell 2016; Sharma and Warkentin 2019). Change, Liu, and Jang (2017) defines commitment as a *"psychological state that binds employees toward a particular course of action, and conducting such action reflects employees' affective connection with the organization"*. Organizational commitment among the employees means that there exists a high level of congruence between employees and organization's goals and values, as well as a willingness of employees to devote extra effort to the organization's benefit. Overall, committed employees have a strong desire to maintain membership in the organization (Change, Liu, and Jang 2017). Sharma and Warkentin (2019) argues that organizational commitment is a mindset that motivates employees in contributing to an organization's competitive advantage.

Sohrabi Safa, Solms, and Furnell (2016) further explain that committed individuals value personal achievement and reputation. These employees spend more time and energy in order to achieve success in their careers. *"Committed persons would therefore not take the risk of breaking rules that could thereby jeopardize or destroy their career aspirations."* Consequently, employees with more commitment to the organization are less likely to ignore the security policies (Sohrabi Safa, Solms, and Furnell 2016). Feng, Zhu, and Nengmin Wang (2019) explain that a high level of commitment to organizational success indicates that employees have put a lot of effort into their work. Highly committed employees would therefore avoid engaging in deviant behaviors, such as non-compliance as this may diminish their personal image or affect their career success. Sharma and Warkentin (2019) also argue that organizational commitment positively impacts the employees' intention to comply with security policies. *"Employees with higher organizational*

commitment would have higher intention to comply with security policy as they are less likely to engage in counterproductive behaviors."

2.2.4 Personal and social norm

Moral beliefs and personal norms have also been found to significantly affect employees daily compliance behaviors. Moral beliefs refer to the degree to which the individual perceives that it is morally wrong to violate the organization's information security policy. Furthermore, moral beliefs are positively related to employee's information security policy compliance (D'Arcy and Lowry 2017 and 2019). Personal norms refer to the values and views an individual has on compliance with information security policies (Sohrabi Safa, Solms, and Furnell 2016). The same authors argue that personal norms affect employees attitudes towards engaging information security non-compliance. Yazdanmehr and Wang (2016) explain that personal norms are an important factor influencing employee's information security policy compliance. Personal norms are, in turn, influenced by the awareness of consequences and the ascription of personal responsibility. Moreover, Yazdanmehr and Wang (2016) show that social norms related to information security policy compliance contribute to personal norms. *"Social norms and cost of deviance in the group encourages members to act in ways that they consider other members think they "should". ... Through internalization, social norms become personal norms"* (Yazdanmehr and Wang 2016).

In addition, empirical evidence shows that information security policy compliant behavior and the norms of peers positively influence the information security behavior of others in the organization. *"The motivating effects of peer behavior can largely be ascribed to a human's desire for approval from significant others, but also because interactions with peers enable knowledge transfer"* (Haeussinger and Kranz 2017). The effect of social influence on employee compliance is determined by the extent to which they are open to social influence and their perception of what colleagues think about compliance (Yazdanmehr, Wang, and Yang 2020). Several studies have also confirmed that subjective norms have an influence on employee's information security policy compliance (Ahmad et al. 2019; Yazdanmehr and Wang 2016). Subjective norms are an employee's perceived social pressure about compliance with information security policies. This social pressure is caused by behavioral expectations of important people such as executives, colleagues, and managers. Subjective norms will influence employee's opinion about information security measures (Ahmad et al. 2019).

Yazdanmehr and Wang (2016) argue that social norms related to the information security policy, including injunctive and subjective norms, shape personal norms which lead to compliance behavior. Injunctive norms are the perceptions of the moral rules in a group, and what "should" be done. This involves an individual's perception of approval and disapproval of certain behaviors. *The desire to follow injunctive*

norms is rooted in an individual's social nature and the tendency to build, develop, and maintain social relationships with others to gain resources and social support (Yazdanmehr and Wang 2016). Wiafe et al. (2020) found, similarly, that descriptive and subjective norms are significant predictors of personal norms. Descriptive norms help individuals to determine the right behavior in similar situations. An individual perceives sufficient social support for a particular behavior when they have noted and observed what others do in a similar situation (Wiafe et al. 2020). To summarize personal beliefs and expectations from relevant other's as well as colleagues acting in accordance with the security policy will form positive feelings towards information security policy compliance.

2.3 Information security management

Researchers within the field of information security have confirmed that leadership is a critical element that positively influences employee's compliance with information security policies and in turn protects the organizational resources (Koohang, Nowak, et al. 2020; Koohang, Anderson, et al. 2019;2020; Haeussinger and Kranz 2017). In their literature review, Haeussinger and Kranz (2017) conclude that management support will increase the preventive efforts and increase the effectiveness related to information security in the organization. A high level of management commitment to information security will also result in an improved information security culture within the organization. Koohang, Nowak, et al. (2020) argue that information security *"should be viewed as a top strategic priority in organizations and that commitment from top management supports the effective enforcement of ISP requirements"*. Management should communicate a clear vision, formulate a clear strategy and establish clear goals and objectives for the organization's information security. Clear and effective information security policies will lead to increased compliance and protection of the organization's assets against security threats (Koohang, Nowak, et al. 2020).

The literature review thus showed that management plays a vital role in influencing employee's information security policy compliance. Management can use strategies such as creating information security awareness, enhancing organizational commitment, reducing perceived inconvenience, as well as developing a beneficial ethical climate that will positively influence employee's personal values and beliefs.

2.3.1 Create information security awareness

In order for management to contribute to the information security work, it is important that they first develop a high level of information security awareness. If management have a high level of information security awareness it is more likely that they will formulate effective information security policies. Moreover, higher levels of information security awareness among management will contribute to an enhanced information security within the organization since it will lead to more resources and more managerial actions towards information security. High levels of management information security awareness will also enhance employ-

ees' levels of information security awareness (Haeussinger and Kranz 2017). Furthermore, Haeussinger and Kranz (2017) explain that before employees can obtain a high information security awareness, it is essential that management itself obtain a broad knowledge about the risks and threats of information security.

Hwang, Wakefield, et al. (2019) argue that security policies, security visibility and management participation will increase employee's information security awareness. Management should hence create and communicate clear and concrete security policies, making all information security activities and security processes visible to employees, as well as actively participating hands-on in these processes. Active participation is likely to capture the attention from the workforce (Hwang, Wakefield, et al. 2019). Management can also improve information security awareness by inspiring and encouraging information security knowledge-sharing within the organization. Knowledge-sharing in organizations will not only increases the awareness among employees, but it will also show the importance of complying with organizational information security policies (Sohrabi Safa, Solms, and Furnell 2016).

2.3.2 Reduce the perceived inconvenience

Organizations must find ways to reduce the perceived inconvenience related to information security measures. Reducing the perceived inconvenience is an important challenge that information security experts face (Ahmad et al. 2019). Hwang, D. Kim, et al. (2017) explain that employees often view the completion of their own particular tasks as a more important goal than complying with information security policies. Employees may therefore understand the need for compliance but still demonstrate non-compliant behavior. The risk of this happening increases when information security activities conflict with or obstruct their daily work. *"Therefore, organizations should convince employees that positive security behavior is one of their performance factors"* (Hwang, D. Kim, et al. 2017). Han, Y. J. Kim, and Kim. (2017) explain that once employees understand why information security is important, they are more likely to behave in accordance with information security policies. Consequently, managers need to find a way to communicate this importance from an organizational perspective.

Karlsson, Hedström, and Goldkuhl (2017) stress that there will be less needs for workarounds if information security policies are designed to fit employee's work practices. Employees should not have to prioritize between information security and their work. Well-designed policies will make it easier for employees to be compliant with information security policies. *"An information security policy that is of a high communicative quality has the potential to be a practical and useful tool for information security management."* Based on a practice-based discourse analysis that included high-level and low-level information security policy documents, Karlsson, Hedström, and Goldkuhl (2017) suggests eight quality criteria for the design of information security policies in healthcare which can be seen in figure 2. These criteria are created

with a practice-based perspective, which means that they enforce information security policies as useful tools for employees, in contrast to the management perspective. However, when designing information security policies, both a management perspective and a practice-based perspective should be considered in order to create a balanced solution.

No	Quality criteria	Theme
1	External policies should be translated and transformed to the current work practice when such parts are included in the information security policy.	External congruence
2	The information security policy should contain congruent guidelines for actions that are well adapted to the current work practice.	Internal congruence
3	The information security policy should have a clear and congruent conceptual framework adapted to the current work practice.	
4	The information security policy (in whole and parts) should have a clear structure; employees need to know that they have covered all information concerning a specific topic.	
5	The information security policy (in whole and parts) should have clear communicative objectives, implying clear communicative functions of the document.	
6	The information security policy should not introduce goal conflicts.	Goal conflict
7	The information security policy (or explicit parts thereof) should have clear and uniformed target groups.	Target group
8	The information security policy should be constitutively clear, clarifying responsibilities, social commitments and expectations.	

Figure 2: Eight quality criteria for the design of information security policies [Image from: (Karlsson, Hedström, and Goldkuhl 2017)].

2.3.3 Enhance organizational commitment

Previous studies show that organizational commitment positively impacts employee's information security policy compliance. Past research also shows that employees commitment to the organization are influenced by leader's activities and behavioral styles (Feng, Zhu, and Nengmin Wang 2019). The same authors explain that factors such as management receptiveness, supervisory mentoring, leader-member exchange and supervisory support have all been found to have significant effects on organizational commitment. In addition, organizational factors such as general working conditions, performance and reward system as well as training and career development have also been identified by researchers to affect employees' commitment to the organization (Feng, Zhu, and Nengmin Wang 2019).

Sohrabi Safa, Solms, and Furnell (2016) also stress that employees will be more motivated to remain committed to the organization if they believe that the organization supports them. Feng, Zhu, and Nengmin Wang (2019) argue that leaders can influence several organizational factors since they serve as policy makers and possess the power to determine overall working conditions. Therefore, leaders have an important role in shaping the work environment in a way that will motivate employees to become committed to organizational success and protect organizational resources (Feng, Zhu, and Nengmin Wang 2019).

2.3.4 Developing a beneficial ethical climate

Several literature sources confirm that employee's attitudes towards information security are influenced by personal values and moral beliefs, expectations from relevant others and colleagues acting in accordance with the security policy. Yazdanmehr and Wang (2016) propose two strategies to adjust and influence the employee's personal norms and the general social norm toward information security policy compliance. First, organizations can implement campaigns that communicate social norms towards information security policy. The authors suggest that such messages could be framed as follows: *"Join your fellow coworkers in helping to keep information assets secure."* Secondly, management can shape the organizational environment toward rule-following in general, and specifically information security policy compliance. It is important that leadership try to create consistency regarding ethics, and establish training and socialization programs in order to establish a beneficial ethical climate across the organization. More specifically, the literature suggests that organizations can implement intervention programs to communicate that rules and standards are values emphasised by the organization, and these values should be cherished and respected by all employees. *Such interventions may eventually build the employees' shared perception toward rule-following and hence shape social norms toward ISP compliance* (Yazdanmehr and Wang 2016).

In accordance with this, Feng, Zhu, and Nengmin Wang (2019) stress that leaders can influence the formation of personal beliefs regarding compliance of organizational rules. Leaders are the norm advocators or rule makers and the behavior and norms they exhibit will influence employees. Employee's beliefs about the norms will be affected by whether or not leaders are considered trustworthy, fair, and competent (Feng, Zhu, and Nengmin Wang 2019). Wiafe et al. (2020) emphasize that *"ISP compliance behavior of managers and leaders within the organization is crucial. Organizational leadership must ensure that they conform to ISPs to serve as good examples in the organization."* Furthermore, it is important that their security behaviors are overt since this will promote the formation of advantageous norms towards compliance. It is also favorable if the environment supports information flow in order for employees to be aware of how well their colleagues are complying to the information security policy (Wiafe et al. 2020). In addition, the authors argue that subordinates are more likely to consider behaviors in line with information security as a

norm when management communicate it as ideal for organizational progress.

2.4 Information security culture

Many researchers stress the importance of not only improving employee's information security policy compliance, but also establishing an information security culture within the organization (Parsons et al. 2015; Chen, Ramamurthy, and Wen 2015; Da Veiga and Eloff 2010). This culture impacts employee understanding and security behavior in a way that can guard against many information security threats caused by employees (AlHogail 2015). Information security culture can be defined as: *"The collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organization with the aim of influencing employees' security behavior to preserve information security"* (AlHogail and Mirza 2014).

Da Veiga and Eloff (2010) explain that an information security culture is created *"due to the information security behavior of employees, in the same manner that an organizational culture develops due to the behavior of employees in the organization."* An information security culture is created through the interaction employees have with information assets, and the security behavior they develop. This happens within the context of the organizational culture within the organization. The implementation of information security components such as a policy and the resulting behavior of employees has an impact on the resulting information security culture as seen in figure 3 (Da Veiga and Eloff 2010). In line with this AlHogail (2015) argues that changes in behavior will be accomplished through the implementation of new procedures within the culture of the organization. The change in behavior will result in a set of artifacts, values, assumptions, and knowledge to enhance information security (AlHogail 2015).

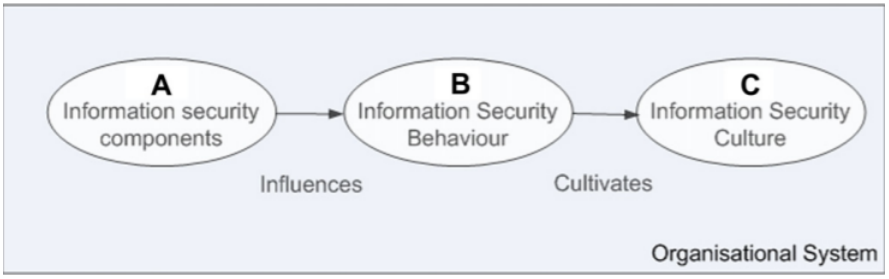

Figure 3: How an information security component influences information security behavior and an information security culture is formed [Image from: (Da Veiga and Eloff 2010)].

Fig. 3 illustrates how information security component (A) is implemented in the organization. The component can be viewed as an input that will influence the information security behavior among employees in the organization (B). Implementing the information security component affects how employees interact with information assets, and employees consequently develop certain behavior referred to as information

security behavior. *"The objective is to instill information security behavior that is conducive to the protection of information assets based on the organization's information security policies and code of ethics. Such behavior could involve the reporting of security incidents, adherence to a clear desk policy or the secure disposal of confidential documents"* (Da Veiga and Eloff 2010). The literature suggests that with time this behavior around security will become second-nature to the employees and eventually become the status-quo for how security threats are dealt with in the organization. When this happens an information security culture has been established (C). This suggests that an information security culture will be developed if employees comply with an organization's information security policies and develop beneficial information security behaviors.

AlHogail (2015) emphasize that *"an information security culture that promotes good security-related human behavior through knowledge, artifacts, values, and assumptions is far more effective than regulations that simply mandate employees' behavior."* It is necessary that employees know, understand, and accept the necessary precautions involved with information security. An established culture will contribute to this by making information security a natural aspect of employee's daily activities. An information security culture will lead to security-related ideas, beliefs, and values of the group, which shape and guide employees to beneficial security behaviors (AlHogail 2015). Parsons et al. (2015) demonstrate that an information security culture will affect how employees think, believe, and behave in relation to information security policies and procedures. Employees are more likely to have knowledge, attitudes, and behaviors in accordance with information security policy and procedures if the organization has an strong information security culture (Parsons et al. 2015). An information security culture will influence employees mindsets and behavior in a way so that information security becomes natural and taken-for granted. Employees may, for example, develop a strong security mindset of using strong passwords without thinking about that extra effort is needed (Chen, Ramamurthy, and Wen 2015).

2.5 Technical security controls

There is a consensus among researchers within the field of information security that technical measures are not sufficient to achieve an adequate level of information security related to the employees. Researchers have, however, suggested a number of technical security controls that can mitigate the insider threat that employees non-compliance and poor information security behavior results in (Fatima and Colomo-Palacios 2018; Fernández-Alemán et al. 2015). Standard information security measures like virus and malware protection software, firewalls and access control are important measures to mitigate security breaches caused by inadequate user behavior. In addition to these standard measures, a number of technical security controls related to password security, secure use of the internet, secure use of email and secure use of portable equipment were identified in the literature .

2.5.1 Password security

Fernández-Alemán et al. (2015) argue that weak passwords is a major security problems in healthcare caused by inadequate security and privacy practices in healthcare employees. In line with this, The European Union Agency for Cybersecurity present that weak or reused passwords is one of the biggest vulnerability in the case of unintentional insider threats (ENISA 2020). The Swedish Civil Contingencies Agency in addition emphasizes that password attacks are frequently used by attackers to obtain unauthorized access to a system (MSB 2020). Some measures which can be adopted by health staff and healthcare organizations to enhance the password security is to employ a strong authentication mechanism and use software for reminder to change password after one year (Fatima and Colomo-Palacios 2018; Fernández-Alemán et al. 2015).

More robust identification methods that will improve security is an important measure (Fatima and Colomo-Palacios 2018; Fernández-Alemán et al. 2015). Multi factor authentication should be used, where the authentication methods is based on a combination of at least two of the following factors: a users knowledge (e.g. a password or a PIN), a users possession (e.g. key or an identification card) and a users inherence (e.g. biometrics such as face and voice pattern) (Fernández-Alemán et al. 2015). Another security measure that can be used to protect the system against password hacking is to change passwords frequently (Fatima and Colomo-Palacios 2018; Fernández-Alemán et al. 2015). The organizations' IT departments can set up a mechanism to send reminder emails to staff from time to time and even to force them to change password on an ongoing basis. However, it may be challenging for the user to remember the new password when they have to change it frequently, but an easy solution is for the user to use software to manage all of their passwords (Fernández-Alemán et al. 2015).

2.5.2 Secure use of the internet

Secure use of the internet is another important security aspect in healthcare organizations related to the employees (Fatima and Colomo-Palacios 2018; Fernández-Alemán et al. 2015). File-download is one of the major penetration channels utilized by malware. Users without technical knowledge needed to detect suspicious files download may execute files that are embedded with malicious codes (Fernández-Alemán et al. 2015). Web browsing may also result in that employees unintentionally leak sensitive information. Browsing of suspicious sites is one of the biggest vulnerability in the case of unintentional insider threats according to cybersecurity experts (ENISA 2020). The organizations' IT departments can block unwanted websites so that staff for example can not use personal e-mail accounts and file storage accounts, download files and access games, on-line newspapers and magazines (Fernández-Alemán et al. 2015; Fatima and Colomo-Palacios 2018). Another measure is to deploy data loss prevention software to recognize potentially harmful sites, as well as identify harmful email practices (Greitzer et al. 2014; Abdelsadeq et al. 2019). Data loss prevention software will monitor the movement, usage and storage of data to ensure that no sensitive

information is lost or misused (Mohanta, Hahad, and Velmurugan 2018).

2.5.3 Secure use of e-mail

Secure use of e-mail is another important aspect for many organizations (Fernández-Alemán et al. 2015; Fatima and Colomo-Palacios 2018). Incidents which involve the interception of e-mails containing personal data or e-mails to the wrong recipients who are not authorized to receive that information is a common and concerning scenario in healthcare and other organizations. Another concern is spam which not only affects the network resources, but also becomes a source of virus attacks (Fernández-Alemán et al. 2015). Greitzer et al. (2014) explain that an outsider's electronic entry acquired through phishing email that enables an attack carried out via software, such as malware and spyware is a common incident. Furthermore, cybersecurity experts argue that phishing and spear phishing are the biggest vulnerabilites in the case of unintentional insider threats (ENISA 2020). MSB (2020) stress that phishing and spear phishing are successful because it makes extensive use of human qualities, such as curiosity.

Implementing data loss prevention software as explained above and e-mail security software should be considered to mitigate these security and privacy threats (Greitzer et al. 2014; Fernández-Alemán et al. 2015). Fernández-Alemán et al. (2015) argue that e-mail security software can be used to reduce unsolicited email messages. e-mail security software effectively filter out the volumes of e-mails sent to receivers' mailbox without their permission. A number of anti-spam solutions have been proposed in the literature. Although anti-spam solutions have had success, new types of spamming techniques can appear which should be watched by health organizations' IT departments (Fernández-Alemán et al. 2015).

2.5.4 Secure use of portable equipment

Greitzer et al. (2014) explain that portable equipment, such as laptop, smart phone, portable memory device, or hard drive, no longer in possession (lost, discarded, or stolen) poses a major information security risk caused by insiders. In line with this Fatima and Colomo-Palacios (2018) argue that discard equipment without removing the information is a common unintentional insider threat. It is therefore important to enable remote memory wipe for lost equipment to mitigate this security threat (Abdelsadeq et al. 2019; Greitzer et al. 2014). Another important measure is to encrypt data stored on removable memory devices (Fatima and Colomo-Palacios 2018).

2.6 Summary of the key findings from the literature

In the table below the key findings from the literature review are presented. These findings will later be used to develop a framework for improving information security related to employees without taking time and resources from employees main work tasks.

Table 1: Key findings of the literature review

Section	Key findings
Information security policy compliance	The fist step an organization must take in order to manage the human factor of information security is to formulate a comprehensive policy that mitigates all the information security risks related to employees that the organization can identify. When a policy is in place, the organization must ensure that all employees comply with the set policy. The literature highlights several factors that affect employees' information security policy compliance: information security awareness, perceived inconvenience, organizational commitment and personal and social norm.
Information security management	Leader within an organization must manage and implement information security in order to ensure information security policy compliance. It is therefore important that management has a high level of information security awareness. It is also important that management devote sufficient resources to information security work. Management can, with the help of various strategies, influence the previously identified factors to improve employee's information security policy compliance. Management can use strategies such as creating information security awareness, enhancing organizational commitment, reducing perceived inconvenience, as well as developing a beneficial ethical climate.
Information security culture	Information security policy compliance will lead to the development of an information security culture, which will further strengthen the information security in the organization.
Technical security controls	Technical measures are not sufficient to achieve an adequate level of information security related to employees. Technical security controls can, however, mitigate the security risks that employees non-compliance may result in, technical measures may therefore be implemented together with other measures in order to improve the level of information security.

2.7 Proposed framework - Improving information security related to employees

The findings from the literature review suggest that there are several measures that an organization can adopt to improve their information security related to employees without taking time and resources from employee's main work tasks. These measures are summarized in the proposed framework below (Figure 4). The framework suggest that organizations can develop an adequate level of information security related to the employees by first establishing an information security policy that includes guidelines for all employees and then ensure compliance of that policy. Leader within an organization can ensure compliance by man-

aging and implementing information security. This means that management devotes sufficient resources to information security work. Furthermore management will utilize strategies such as creating information security awareness, enhancing organizational commitment, reducing perceived inconvenience, as well as developing a beneficial ethical climate to improve employee's information security policy compliance. A prerequisite for managing and implementing information security successfully is that management has a high level of information security awareness. Information security policy compliance will also over time lead to the development of an information security culture, which will improve the information security further.

If all employees follow the established policy, the organization can ensure that they have the level of information security related to employees that they desire. However, if not all employees comply with the information security policy, technical security controls can mitigate the insider threat that non-compliance may result in and it may therefore be beneficial to implemented technical measures together with other measures in order to create an adequate level of information security.

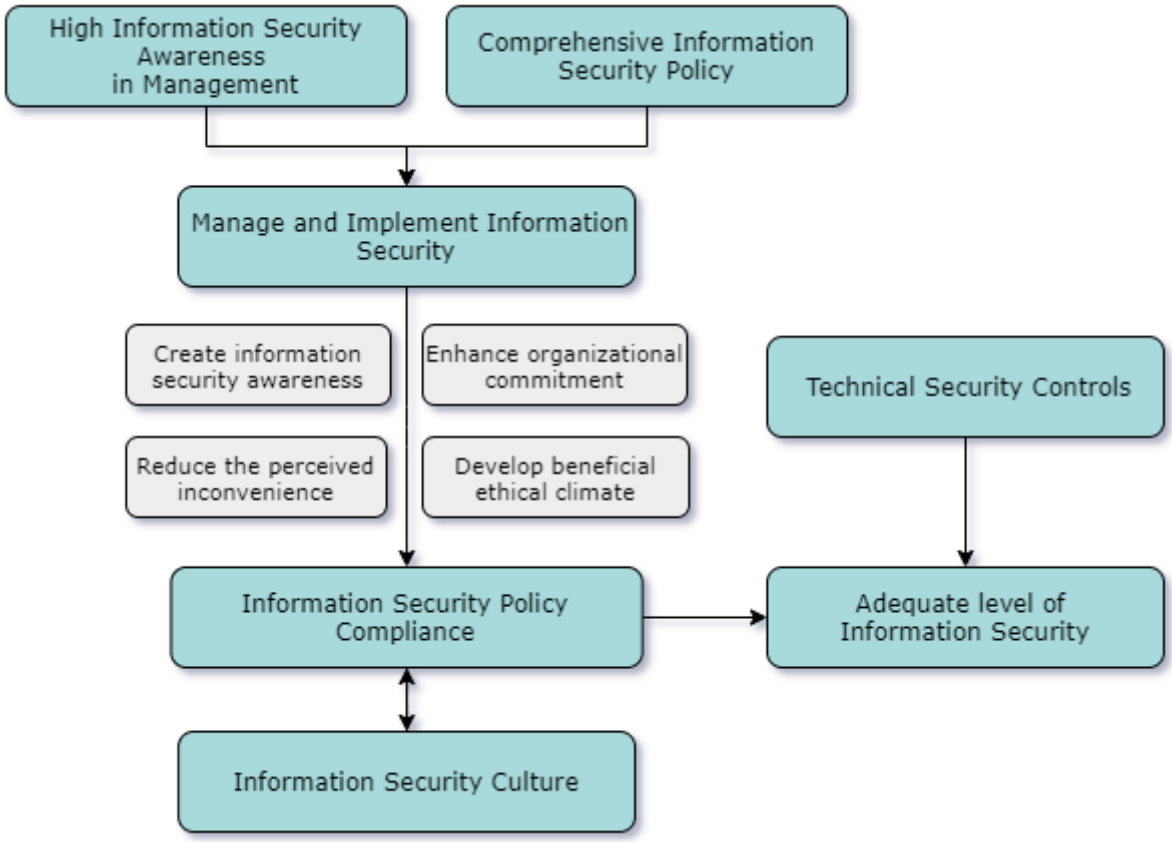

Figure 4: Proposed model to improve information security related to employees

3 Method

In this section, the research approach taken and the methods used will be explained and justified. First the research method will be explained in detail and then the validity and reliability of the chosen method will be discussed.

3.1 Research approach

3.1.1 Qualitative method

Qualitative methods focus on enabling a deeper understanding of phenomenon based on what people tell and do (Gillham 2000, p. 10). A qualitative research approach was therefore taken for this study in order to gain a deeper understanding for healthcare organizations information security work. One of the advantages of a qualitative method is that it creates opportunities to investigate something that can be considered uncontrollable and informal (Gillham 2000, p. 10), which employees' behaviors regarding information security can be considered to be. Furthermore, it also creates the opportunity to gain perspectives from those involved in what is being analyzed (Gillham 2000, p. 10-11). Qualitative research is often used when the researcher is more interested in describing and understanding complexity than measuring something (Arksey and Knight 1999, Ch. 1). It was considered essential to use a qualitative method in the data collection for this study since it was important to understand the problem in depth.

3.1.2 Deductive reasoning

The research approach taken was mainly of deductive nature since the purpose of the data collection was to test whether the framework developed from the literature review would work in practice. Deductive method means that you direct your analysis towards a specific area and adopt a clear theoretical position. This theoretical position is then tested through the collection of data (Saunders, Lewis, and Thornhill 2012, p. 48). Deductive method is hence often used to prove or disprove something (Saldaña 2011, p. 93), which was the main purpose of the data collection for this study. However, since semi-structured interviews open up for unexpected information to emerge, this study also had elements of an inductive approach. An inductive approach means that a specific topic is explored without a clear theoretical position. Instead a theoretical explanation is developed as the data is collected and analyzed (Saunders, Lewis, and Thornhill 2012, p. 48). Induction is to explore and infer from the collected data (Saldaña 2011, p. 93). Saunders, Lewis, and Thornhill (2012, p. 148) claims that it is often beneficial to combine deduction and induction within the same piece of research even though one approach is often dominant.

3.2 Research design

3.2.1 Semi-structured interviews

Interviews are one of the most common methods for qualitative research. This type of data collection method is an effective way of requesting, collecting and documenting individual's or group's perspectives, opinions, attitudes, and beliefs in their own words (Saldaña 2011, p.32). Interviews were therefore used in this study both to obtain a deeper understanding of the problem being investigated and to review how possible solutions might work in practice. Representatives from several different organizations experiencing the presented problem participated in the interview study, which made it possible to obtain different perspectives and opinions.

There are, according to Arksey and Knight (1999, Ch. 1) three major formats of interviews, namely structured, semi-structured and unstructured interviews. What sets them apart is the degree of structure and formality. Semi-structured interviews are perhaps the most common and most diverse of the three formats. Semi-structured interviews fall between the structured and unstructured format, since this type of interview contains both open and more theoretically driven questions. This is beneficial since the structure will allow all relevant topics to be addressed, but at the same time the interviewers are free to follow up ideas and ask for clarifications (Arksey and Knight 1999, Ch. 1). Since the goal of this interview study was to gather different perspectives and opinions on the problem and possible solutions, semi-structured interviews seemed advantageous. This method made it possible to ask questions related to the problem and the possible solutions, but at the same time leave room for unexpected information.

3.2.2 Selecting participants to interview

To obtain valuable insights about the problem, it was necessary to interview participants with experience within the field of information security related to employees. It was however also considered valuable to interview employees who work more directly with healthcare to understand how they experience information security measures. Therefore, one employee with direct responsibility for information security, and one employee working more closely with healthcare were interviewed from each participating organization. It was considered advantageous to interview participants from different organizations since this most likely would contribute to a more holistic view of the problem and possible solutions. Therefore, 5 different organizations participated in the study, which meant that 10 interviews were conducted in total.

The participants in the study were recruited through email. At the beginning of the study, a number of emails were sent out to organizations that were considered to be suitable for the study. At the first contact, the organizations were asked if any of their employees who work with information security wanted

to participate in an interview. Thereafter, the information security experts were asked if they knew of any healthcare employees who could be contacted for another interview. Through this strategy, a satisfactory number of participants were recruited, that contributed to a broad view of the problem and possible solutions.

Table 1 below provides an overview of the participants of the interview study; the pseudonym used to refer to them in the report, the organization they belong to, their current position at the organization and the interview date.

Table 2: Overview of the participants of the interview study.

Pseudonym	Organization	Position	Date
John	A	Information Security Officer	2020-12-03
Anna	B	Information Security Coordinator	2020-12-14
´ Dan	C	Head of Finance (Responsible for information security)	2021-01-18
Lisa	D	IT Coordinator	2021-01-20
Hanna	E	Information Security Coordinator	2021-02-01
Ellen	C	Site Manager	2021-02-12
Ian	A	Logistics Manager	2021-02-17
Elsa	B	Care Assistant	2021-02-22
Nora	D	Site Manager	2021-02-24
Mia	E	Nurse	2021-04-04

3.3 Conducting the interviews

The interviews were conducted through video calls and lasted between 25-45 minutes. All calls were, after the participant's consent, recorded and transcribed to facilitate the analysis. Moreover, the interviews were conducted with a predetermined framework of questions. According to Gillham (2000, p. 69) it is important to have a clear idea of what is considered valuable to get answers to and that the theoretical framework is well thought out before before conducting a semi-structured interview. The literature review was therefore completed before the interview questions were formulated. The interview questions were designed on the basis of the proposed framework by dealing with questions about each parameter. This was important since the objective of the data collection was to validate if the framework would work in practice for healthcare organizations.

Two different types of interview questions were formulated since it was considered beneficial to ask the employees who work with information security different questions than those who worked with healthcare. However, all employees who work with information security were asked the same questions and those who

worked with healthcare were asked another set of questions. It is important to keep in mind when using qualitative data for analysis that qualitative data is more arbitrary because it is based on human impressions and observations. It is therefore important to standardize data collection in order to be able to analyze it (Saunders, Lewis, and Thornhill 2012, p. 546). It was therefore considered important to use the same set of questions for each group of participants. The interview questions used for employees who work with information security can be seen in Appendix A and the interview questions for employees who worked with healthcare can be seen in Appendix B.

3.4 Data analysis

As mention above, all interviews were recorded and transcribed to ensure that no information from the interviews were lost. Thereafter, the empirical data could be analyzed by coding. Coding means that data is broken down and named through different themes or categories (Saunders, Lewis, and Thornhill 2012, p. 572). For this study, a type of coding called template analysis was used to analyze the data. Template analysis is procedure to analyze qualitative data where a template or a list of the codes or categories are used to categorize the data. Template analysis combines a deductive and an inductive approach since some codes can be predetermined and other codes can be added to the template as data is collected (Saunders, Lewis, and Thornhill 2012, p. 572). Different themes were, for this study, identified based on the collected data that could be linked to the proposed framework. Template Analysis was considered advantageous for this study because the objective of the data collection was to validate the framework. It was therefore important that codes related to the framework were used, but it also left the opportunity to identify other interesting factors.

During the data analysis it became clear that organization C has a quite different approach to information security than the other organizations. At present, the organization does nothing to influence employee's information security behaviors. However, according to them, they have a strong information security culture and powerful technical security controls that ensure a high level of information security. As they have a very different focus, the organization will, in the discussion, only be analyzed under the sections information security culture and technical security controls because the data collected does not relate to the other areas.

3.5 Validity and reliability

In qualitative research, it is important to ensure validity and reliability when collecting data. Reliability refers to the consistency of a measure, and validity is about the accuracy of a measure. In semi-structured interviews, problems related to these quality indicators may arise. However, the researcher can avoid these quality problems in different ways (Saunders, Lewis, and Thornhill 2012; Arksey and Knight 1999).

Problems with validity can arise if the researcher interprets answers in a different way than what the participant tried to convey. To ensure validity during interviews it is important that the researcher gains access to a participant's knowledge and experience, and is able to infer the same meanings as the participant thought to convey (Saunders, Lewis, and Thornhill 2012, p. 381). In order to create and ensure a high degree of validity, it is important that the interviewer asks questions and explores the respondent's opinions or knowledge of the subject from many angles (Saunders, Lewis, and Thornhill 2012, p. 384) and that the questions asked during the interview is drawn from the literature (Arksey and Knight 1999, Ch. 4). Therefore, the questions asked during the semi-structured interviews were from different angles and themes, based on the designed framework. To gain different perspectives and strengthen the validity of the study, 5 different organizations participated in the study and from each organization both an information security one employee with direct responsibility for information security, and one employee working more closely with healthcare were interviewed. It is according to Arksey and Knight (1999, Ch. 4) important to select a group of participants that fits the purpose of the research, therefore the participants in the empirical study were carefully selected.

Problems with reliability can arise during semi-structured interviews due to the lack of standardization and the fact that bias can arise unknowingly from the person conducting the interview. This means that the interviewer through comments, tone or non-verbal behaviors reveals what he or she wants to hear and thus affects how the participant responds. There is also a risk that the interviewer is biased in her way of interpreting the response she receives, which results in misleading data (Saunders, Lewis, and Thornhill 2012, p. 381). To ensure reality, it is important that researchers reflect on the ways in which their background, personality, mind set, and actions may affect the data collection Arksey and Knight (1999, Ch. 4). To improve the reliability, the researcher tried to pay attention to and reduce this during the interviews and data analysis.

4 Empirical study

In this section, the empirical data from the interviews will be presented. Firstly, the current state of information security of the participating organizations are described and thereafter the remaining empirical data will be introduced in accordance to the parameters of the proposed framework.

4.1 Information security within the participating organizations

The current state of information security varies between the participating organizations. John, an Information Security Officer at organization A, states that his organization has a lot of work ahead of them before they achieve their desired level of information security. They have performed a large gap analysis and much of the information security work is based on closing gaps as well as continuously handling the issues that, according to John, comes from all possible directions. John also mentions that it is difficult to keep up with current demands as he is working alone with information security in the organization. On the other hand, Ian who is a Logistics Manager at organization A, believes that the organization has a satisfying level of information security. His main argument is that the organization has improved since the General Data Protection Regulation went into effect.

Organization B has a relatively high level of information security according to both Anna who is an Information Security Coordinator and Elsa who is a Care Assistant at the organization. Anna explains that one of the owners started with information security work fairly early, with governing documents and policies around it, and they have collaborated extensively with their shareholders to develop a satisfying level of information security in the organization. It is according to Anna essential for everyone within the organization to work towards a common goal. She places emphasis on the fact that they are a large organization with 2000+ employees, and therefore the focus lies on education and training. This presents a challenge due to the amount of employees who require training. Moreover, Anna says that it is very difficult to keep up with training in information security because the business is under time pressure. However, especially during the last few years, she has seen a positive change in the organization in the belief that it is important to work more systematically with information security.

Organization C, has facilities for people who have suffered from honor-related violence and they have many clients with protected identity. Dan, who is Head of Finance explains that it is extremely important that they do not reveal any information about these clients or the facilities. This has according to both Dan and Ellen, who is a Site Manger, made the organization very careful with information in general and both believe that they have a very high level of information security throughout the organization. The organization has an external company which is responsible for the IT environment and the security within

this environment. Dan has meetings with the IT supplier each month, where information security is one of the main discussion points.

Nora, who is a Site Manager at organization D, believes that the organization has a satisfying level of information security. She explains that they have worked on information security and it has subsequently improved over the years. Lisa, who is the IT Coordinator at the organization agrees, however she emphasizes that there are areas of improvement. Due to the current pandemic information security has not been prioritized within the organization. Lisa explains that there has not been enough resources, time or energy to work with information security in the past year.

Hanna, Information security Coordinator at Organization E explains that information security is a rather neglected area in the healthcare sector. The organization has a lot of work left to do in order to achieve an adequate level of information security, but there has been a noticeable increase in interest. She believes that the increased attention that information security receives in media helps. She further explains that management has realized that information security is an important area that they must take into account in order to be able to take care of their patients in the best possible way. However, she expresses that there is a lack of resources and that it is difficult for her to reach out to the entire organization when she works alone to increase the level of information security related to human behavior in an organization with 14 000 employees. Mia who is a Nurse at organization E explains that they work with information security in organizations, but there are room for improvements. She believes that it is unclear whether it is important to follow the the information security policy and guidelines that are set or not. Mia further explains that she and her colleagues in some cases receive different directives when they talk to their manager compared to the patient safety officer.

4.2 Information security leadership

Information security is an important question for management in all of the participating organizations. John (Information Security Officer, A) explains that he has regular meetings with the organization's CFO where they discuss information security strategies. He believes that the commitment from management is sufficient in order for the organization to keep improving. In line with this, Anna (Information Security Coordinator, B) believes she has had the support of the organization's CEO from the beginning. She also has regular meetings with the company board where they receive regular updates in order to understand the importance of information security. Lisa (IT Coordinator, D) points out that management has the ultimate responsibility for the organizations information security. She believes that management therefore need to be committed to information security. It has however not been prioritized in their organization during the ongoing pandemic, which she thinks is reasonable. Hanna (Information Security Coordinator, E) has a similar observation,

explaining that although management thinks that information security is important, this year has brought many other challenges due to the pandemic. Furthermore, she does not believe that the management fully understands what is actually required to create a solid information security. Dan (Head of Finance, C) emphasizes that information security is a very important issue for everyone in the organization. He further explains that leaked information would damage the trust for the organization.

Managers are in general involved in the information security work and communicate these issues to the employees for most of the participating organizations. This does not only include senior management, but should exist throughout the organization. Dan (Head of Finance, C) explains that site managers have a great responsibility in ensuring that all employees follow guidelines regarding information security. They also have a responsibility to ensure that the employees have the right access levels within the IT systems. For organization D, both site managers and group leader are responsible for communicating information security issues to the employees. Lisa (IT Coordinator, D) explains that she sends out information to site managers and group leader so that they are able to communicate these messages to their employees.

Similarly, Hanna (Information Security Coordinator, E) believes that management in general are committed to information security and they try to communicate these issues to the employees, but time presents the greatest challenge. She believes that if management felt less stressed and had more knowledge on information security, they could pass the knowledge on to the employees and motivate employees to follow information security guidelines. However, she points out that managers need to focus on the core business and it may therefore be beneficial for the organization to employ additional information security experts who have information security as their main focus. Anna (Information Security Coordinator, B) explains that management are involved in the information security work. They have follow-up meetings every month with all site managers where they, among other things, discuss information security. They clear up what shortcomings there are and what measures need to be taken. Anna emphasizes that it is important to include information security in other topics that are already being covered in order to make it easier for the managers:

We do not have our own risk analysis for information security, but it may be included in the risk analysis that the managers still do for patient safety and other things. To make it easy for managers to do the right thing.

(Anna, Information Security Coordinator, B)

Furthermore, Anna believes that managers could take on a bigger responsibility in communicating and educating employees in information security issues, but in order for the managers to feel comfortable in doing so, they need a certain level of information security knowledge. Anna explains that managers may

feel uncomfortable in discussing information security due to apparent knowledge gaps. The organization is therefore taking steps in order to further educate their managers. Organization A are also working on improving managers information security awareness. Right now, site managers are not involved in the information security work, but it is one of their focus areas to give managers more responsibility in communicating information security issues. In order to make that possible, managers needs to develop an adequate level of information security awareness (John, Information Security Officer, A). John believes that developing a top down strategy for information security would be beneficial, although he is aware of the time this will take to establish.

4.3 Information security policy

Most of the participating organizations have an information security policy which includes guidelines for how employees should act in order to keep information secure. However, the quality and detail within these guidelines varies. Organization B has several governing documents related to information security which they have attempted to simplify. This has resulted in written guidelines for how to behave in relation to information systems (Anna, Information security Coordinator, B). In addition, Elsa (Care Assistant, B) explains that they have clear guidelines for how to act in order to keep information secure and she believes that the guidelines are followed to a great extent by her and her colleagues. Similarly to Organization B, Organization E claim that they have clear information security guidelines for the employees. Hanna (Information Security Coordinator, E) explains that all policies and guidelines are set by the local authority which the organization is a part of, which in turn all connected organizations are obligate to follow. The development of policies and guidelines are not something they work directly with. However, the organization takes responsibility in the adherence of set policies as they are included in the employment contract that employees in turn must follow. Hanna believes that a potential issue with this is that employees are not specifically asked to read these guidelines before signing the contract. This suggest the guidelines are in place, however the details required for them to be followed, are not. In line with this, Mia explains that they have clear information security guidelines, but for various reasons these are not always followed by the employees (Mia, Nurse, E)

Organization A and Organization D, on the other hand, rely on dated policies which due to complexity and increased importance require an update. The Information Security Officer at Organization A explains that the organizations policies and guidelines on information security have not been updated for some time. They are in the process of creating new policies, but this is time-consuming and requires a lot of work. John (Information Security Officer, A) further explains that the information security guidelines should differ between different levels of the organization, since they must be adapted to different roles within the organization and what responsibilities the employees have. The organization needs to update the existing policies by segmenting them based on the different levels in the organization they relate to. However, Ian (Logistics

Manager, A) believes the guidelines currently in place are generally followed by the employees, but human error can lead to making mistakes and thus violating the set policy.

Organization D has just undergone an acquisition process and a holistic information security policy that covers the entire organization as a result of the merger has not yet been established. However, the policies and guidelines that was set in collaboration with the previous corporate group are to some extent still in use (Lisa, IT Coordinator, D). Nora (Site Manager, D) believes that there is a clear structure for information security and what rules apply to ensure patient safety. When you start working, you sign a confidentiality agreement so that you know what applies.

Organization C has lots of guidelines and routines integrated into the IT systems they use (Dan, Head of Finance, C). Ellen (Site Manager, C) explains that the system is so well designed and user friendly that it is impossible to use it wrong or insecurely. She further explains that confidentiality is very important for them and that they have clear guidelines around it. However, she is unaware of whether or not these guidelines are written down or if it is just a natural part of the work process.

4.4 Information security training and awareness

Most of the participating organizations have some form of information security training for their employees. Organization B has a mandatory security training called DISA that all employees are required to take. The training addresses basic information security needs within the organization that every employee in the organization is required to be aware of according to Anna (Information Security Coordinator, B). Elsa (Care Assistant, B) explains that she and her colleagues go through security training once per year where they take an online course which takes about half an hour. She believes that all of the full time employees have a high level of information security awareness. However, one of the weaknesses in the information security awareness of the organization is that part time employees do not have the same requirements and thus do not possess the same level of knowledge about information security. Similarly to Organization B, Organization E also receive virtual training session which, according to Hanna (Information Security Coordinator, E), are comprehensive and useful for the employees. However, the level to which these trainings are mandatory is vague and the rules around the requirements for the employees are highly informal. For organization E, these virtual sessions are a new method, and the organization has not yet implemented a routine to make it possible to check whether or not employees are actually attending the training. This ambiguity surrounding these new trainings is confirmed by Mia (Nurse, E). She claims that she and her colleagues have not received any training in information security from the organization, and instead points to the fact that certain education in information security is included in a nurse's degree. She therefore believes that most of her colleagues know how to act to keep information secure but may not always behave accordingly.

Organization A and Organization D are communicating short training sessions or information campaigns to their employees via email, but they have encountered challenges in reaching out to employees this way. Organization A use a learning tool called nano learning, where they can send out courses via email every few weeks. The courses entail very short information campaigns that consist of a couple of pages you go through with a couple of sentences on each. The organization has recently realized that the majority of the users do not use these courses. The organization is therefore now reviewing this strategy. Whether or not this is due to the brevity of the trainings, or the way in which the information is communicated via email, are two of the factors the organization aims to review (John, Information Security Coordinator, A). During the interview, Ian (Logistics Manager, A) confirms John's concerns about the training not reaching out to the employees. Ian claims that he does not currently receive any information security training, but he is confident that employees have the necessary knowledge about risks and routines around information security. He places emphasis on the fact that when the General Data Protection Regulation went into effect, that was when the employees received the training regarding information security and as a result of these trainings employees now have an adequate level of knowledge.

Organization D has recently since the merger integrated all areas of the organization into the same emailing communication. This has enabled trainings in information security to be sent via the same channels to the entire organization. This training consists of emails every three or four weeks with information and interactive questions that may take two or three minutes to perform. Prior to the acquisition the level of education and training was more detailed-oriented and the variety and quantity of training was more extensive (Lisa, IT Coordinator, D). Lisa explains the problem prior to merger was that the training was hosted on the administration system which not all employees had accounts for. The new corporate group have the same structure, but now they have decided that everyone should have accounts. This means that although not as detail-oriented, the amount of employees receiving the trainings has greatly increased. Nora (Site Manager, D) believes that she and her colleagues have not gone through any specific information security training, but she mentions that they are receiving short information campaigns related to IT use. Although she does not consider these to be specific trainings, Nora thinks that these campaigns will improve the employees information security awareness.

Lisa further emphasizes that as an IT Coordinator at Organization D she visits the different facilities within the organization on a regular basis and during these visits attempts to raise information security awareness when she interacts with the employees. One example of this interaction Lisa gives is reminding people to log out when they leave the computer. Lisa claims that her in-person presence and visibility to other employees reminds staff of information security and the routines around it. During these visits

employees are also able to have discussions with Lisa and raise their questions and concerns regarding information security policy. She goes on to say that employee awareness increased greatly when the General Data Protection Regulation was introduced, as it led to a lot of discussions and the company began to work more actively with information security.

Organization C applies a differing approach. The employees officially do not go through any information security training. However, the employees receive training in how to use the organization's IT system (Dan, Head of Finance, C). Ellen emphasis that the technical security controls that the organization use is providing the security, thus information security is embedded within the systems and therefor the human factor to information security is not prioritized.

4.5 Inconvenience related to information security

The empirical study revealed that lack of time is a major challenge related to information security for healthcare organizations. Anna (Information Security Coordinator, B) explains that time is the biggest obstacle in her work pertaining to information security and prevents her from achieving the level of information security that she desires. Due to the challenges related to time as a resource, the organization is forced to prioritize. The training directly related to healthcare will according to Anna, always come first within the organization. Hygiene training is an example of a training which will always take precedence over IT related issues and policies. In line with this, Hanna (Information Security Coordinator, E) emphasis that time is always a critical factor. Hanna explains that completing all necessary day-to-day tasks within regular hours is always a struggle, and as long as information security is not the key part of your work it will not be prioritized. She states that the goal is that information security will be a natural part of everyone's work, but for her organization they are only at the start of that journey. Lisa (IT Coordinator, D) stresses that it is not appropriate to add extra work for the employees or to point out that guidelines on information security are not followed when employees are putting all their available energy into providing patients with the care they need. John (Information Security Officer, A) believes that the lack of prioritization of information security stems from the fact that organizations must weigh benefit against risk when working with information security. One of these risks would be employees not being able to spend that time on other critical tasks.

Employees who do not work with information security, on the other hand, have a different view of the challenges in implementing more security measures as mentioned above. Nora (Site Manager, D) believes that she in fact does have time to actively participate if more security measures were implemented and she does not think it would affect the daily work. In line with this, Mia (Nurse, E) does not believe that information security measures affect her work. She thinks it would be useful to the organization if more measures were implemented, especially if the directives regarding what is expected became more clear.

Ian (Logistics Manager, A) suggests that an increased level of security within the organization can only be beneficial. He argues that although new processes may affect work in the beginning, that after some time information security practices would hopefully be naturally integrated into the rest of his day-to-day tasks. Elsa (Care Assistant, B) would not mind if more security measures were implemented, however she does not believe it is necessary. In contrast to the other interviewees, she confirms that security measure does affect her work by making it a bit more complicated, but she understands why it is necessary. She also claims that employees would in fact have time to prioritize information security to a larger extent.

4.6 Commitment and motivation

To give patients the best possible help seems to be one of the biggest motivations driving healthcare employees in their daily work. Nora (Site Manager, D) believes that the ability to help people that they meet when they need it the most is the greatest motivation for her and her colleagues. In line with this, Elsa (Care Assistant, B) is motivated by seeing her clients lives improved though her daily work. She enjoys seeing the people she works with develop and achieve the belief that they are able to obtain the life they wish for. In line with this, Ian (Logistics Manager, A) explains how motivating it is to see changes for the better and that your work contributes to that. Mia (Nurse, E) is also finds motivation through giving patients the best possible care and she believes that this is the case for most of her colleagues as well.

Ellen (Site Manager, C) explains, in line with the other healthcare employees interviewed, that what motivates her and her colleagues in their work is to be able to help people who need support and to be able to make a difference for people in vulnerable situations.

4.7 The ethical climate

Moral issues are discussed daily in most of the participating organizations. Elsa (Care Assistant, B) believes it is necessary to discuss moral issues in her role as a care assistant. She further emphasizes the importance of treating patients correctly. In line with this, Nora (Site Manager, D) points out that her and her colleagues evaluate and discuss what practices are right and wrong on a daily basis. She explains that it is extremely important to ensure the patients integrity and that they receive the best possible care. Moreover, Mia (Nurse, E) explains that she, together with her colleagues, often discuss moral issues in their daily work. Ian (Logistics Manager, A) explains that moral issues arise from time to time, in situations where it is not always apparent what is the right thing to do.

Moral issues related more specifically related to information security are also discussed in many of the participating organizations. Elsa (Care Assistant, B) explains that in the organization a frequent discussion point is what information should be stored in medical records. It is only the most necessary that should be

stored there, which presents the question as to what information should in fact be considered “necessary”. Ian (Logistics Manager, A) states that what information may be sent via email is discussed frequently in the organization. In the case of a colleague sending confidential information via email, there is is likely to be swift action and repercussions for that colleague. Ian highlights that the discussion often presents itself in the case of a mistake being made in communication, and thereafter the organization evaluates how this communication could have been handled differently. Nora (Site Manager, D) also mentions that she and her colleagues discuss the use of email and what information may be shared in that way. Moreover, they discuss the handling of medical records within the organization, due to patient confidentiality and not all employees are entitled to the same medical records. She emphasizes that it is incredibly important that these rules regarding medical records are followed so that patients feel safe and that the trust between the patient and the organization is maintained.

Ellen (Site Manager, C) explains that she and her colleagues discuss and analyze associated risks for their residents on a daily basis, due primarily to many of them living under protected identity. Ellen highlights the importance of discussion how various information is handled as it can be life threatening for many of the residents if information is accessed by the wrong people.

4.8 Information security culture

The empirical study reveals that building a strong information security culture is the ultimate goal of the information security work in all of the participating organizations. However, the extent to which organizations have come to establish an information security culture varies. According to the empirical study, Organization A and Organization E have not come as far as the other organizations in developing an information security culture. John (Information Security Officer, A) states that they are actively working towards establishing an information security culture. However, he points out that establishing a culture within the organization takes time, especially when evaluating what areas to invest in. Hanna (Information Security Coordinator, E) has a similar view stating that the organization has a long way to go before an information security culture is established, but they are working towards it.

Organization B and Organization D, however, believe they have come further in establishing an information security culture. Anna (Information Security Coordinator, B) whose primary focus and objective in her role is creating an information security culture, is positive that her organization is making substantial progress in establishing this culture. They work towards integrating information security into everything that they do, but she emphasizes the time taken to build and create a new culture within a large organization. Lisa (IT Coordinator, D) believes that information security is already a part of their culture. She believes that although there still are areas of improvement, frequent discussions on information security as well as

employees being involved in the information security work, point to the fact that a culture exists.

Organization C has a very strong information security culture according to Dan, Head of Finance. Ellen (Site Manager, C) confirms this belief within the organization, stating that information security is a part of their organizational culture. Dan, suggests that due to the nature of their work, where the organization deals with confidential information related to honor-related violence, has forced the organization to make it a priority to build a culture involving strong information security.

4.9 Technical security controls

Some of the participating organizations have invested in security solutions in order to mitigate the risks involved with poor information security behavior. Anna (Information Security Coordinator, B) collaborates with another colleague who is responsible for IT security to enhance the level of information security. Together they have decided to invest in a number of technical security controls in order to achieve this. However, Anna emphasizes that despite the adoption of new technical security controls, it is still important to work with awareness. She believes that in order for information security to be successful within the organization, both awareness and technical security controls are needed. Lisa (IT Coordinator, D) explains that Organization D has implemented a number of technical security controls to mitigate the security threat that employees implicates. Some of these solutions have worked very well, while in other cases the solution disturbs the daily work, and thus the organization has been forced to reevaluate what technical security controls to adopt and implement. Lisa says, for example, that they have tried to implement privacy filters for computer screens so that only the person directly in front of the monitor can see the screen, but it did not work since they often sit two people in front of the same computer in their daily work. She believes that although the intended use of a security solution is positive, that does not necessarily mean that it will work within the infrastructure of their organization:

It is difficult to make certain security solutions work in reality and in everyday work.

(Lisa, IT Coordinator, D)

Organization A, however, provides an example of an organization wherein no specific technical security controls to reduce security risks related to the human factor have been implemented. John (Information Security Officer, A) explains that they are currently at the stage of evaluating whether they should invest in more security controls in the future. In line with the findings at Organization D, he emphasizes that it is important that the technical security controls are able to function efficiently without interfering in the employees daily work.

Organization E is another organization within the empirical study that has not yet invested in specific

technical security controls to promote and enable information security. Hanna (Information Security Co-ordinator, E) explains that they have not implemented any security controls to specifically mitigate the security threat that employees implicates. The organization has a department that focuses specifically on IT security, and she states that collaboration between different departments would benefit and facilitate further investment in information security. She again highlights that it is necessary to combine technical security controls with information security awareness, and this would be further enabled by collaboration between different departments.

Johan and Hanna, at Organization A and D respectively, agree that it is not possible nor effective to implement security controls if the employees do not know why it is necessary. John explains that if employees do not understand why security controls are implemented, it often leads to employees finding workarounds to facilitate their work. For example, they may start using their private email or send information outside the organizations system. This is an example of one of the more devastating consequences of unsuccessfully implementing new, unwanted security controls according to John. In line with this, Hanna explains that if employees do not have the awareness needed to implement compelling security controls, employees will find other creative approaches to do their work that may create new major security risks as a result. Moreover, Hanna, emphasizes that the potentially increased complexity that security controls can bring to the work of their employees make it even more necessary for employees to be aware of why they are asked to implement these security controls.

Sometimes security makes things more complicated and a little more difficult and you have to understand why, otherwise, you take shortcuts and find other ways to get past these safety aspects anyway. People are quite inventive.

(Hanna, Information Security Coordinator, E)

Organization C has invested a lot in their networking infrastructure and seems to have a different view of the extent to which technical security controls can mitigate the security threat that employees implicate. Dan (Head of Finance, C) believes that the IT systems that employees use in their work have clear guidelines so that it is difficult to make mistakes, the system is in itself very secure. It is therefore not necessary to implement other security measures.

5 Discussion

In the following sections, the results from the empirical study and the literature review will be analyzed in order to answer the research questions for this study. The analysis will be presented in accordance to the parameters of the proposed framework.

5.1 Information security leadership

Researchers within the field of information security have confirmed that leadership is an important factor that positively influence employees compliance with information security policies and in turn increases the level of information security within the organization. The empirical results show that leaders within healthcare organizations believe in the importance of information security to their organizations as a whole. All of the participants who worked directly with information security confirmed that management within their organization are actively involved in the information security work and believe it is an important issue to some extent. However, Koohang, Nowak, et al. (2020) emphasized that information security should be viewed as a top strategic priority by management and in some of the participating organizations it did not appear to be a top priority to that extent.

The empirical study suggests that one of the main issues involved with information security not being prioritized is that it leads to a lack of investment in resources. Many of the participating organizations do not devote sufficient resources to developing and improving information security within their organizations. Hanna (Information Security Coordinator, E) expresses that there is a lack of resources and that it is difficult for her to reach out to the entire organization on her own. In line with this, John (Information Security Officer, A) mentions that delivering the necessary communication surrounding information security policies and keeping these up to date becomes increasingly difficult as he is the only dedicated resource in the field within the organization. Additionally, Lisa (IT Coordinator, D) explains that due to the ongoing pandemic of the past year, combined with the recent merger of the organization has pushed information security further down the list of priorities within the organization. This suggest that information security is not viewed as a top strategic priority by management of these organizations.

Haeussinger and Kranz (2017) concludes that management support will increase the preventive efforts and increase the effectiveness related to information security in the organizations. This suggests that management needs to be more involved in the information security work in these organizations, and that the attitudes and culture within management is a key driver in increasing the investment of resources within information security. This is likely to contribute to more preventive efforts and more effective information security work. It is according to the proposed framework important that leaders within an organization

manage and implementing information security in order to improve employee's information security behavior. The empirical results supports the framework since an increased involvement and commitment to information security among leaders would result in an improved information security for the participating healthcare organizations.

5.2 Information security awareness in management

According to the proposed framework, one of the key areas in which managers must improve in order to make information security a strategic priority is to develop their overall awareness of information security and how it affects their organization. Haeussinger and Kranz (2017) explain that an increased level of awareness within management results directly in further action towards information security and more effective information security work. The empirical study revealed that management in most participating organizations do not have adequate awareness of the issue which leads to little or no action towards an improved information security. None of Organization A, D or E currently have an awareness training program for leaders within the organization and management are hence not receiving any specialized training aimed directly towards management. The empirical study suggests that most of the participating organizations could improve information security through implementing a information security awareness training program for leaders within the organization. This is generally due to the fact that management has a broader view of the organization and are more aware of its challenges as a whole. Another reason that management plays a crucial role in improving information security is that management is generally the part of the organization which has the most power to create change.

The empirical study shows that in many of the organizations managers are to some extent attempting to communicate information security issues to the employees. However, employees at Organization A, B and E all stated in the empirical study that managers in their organization could take on a bigger responsibility in communicating and educating employees in information security issues. The findings suggest that information security is not something that is completely neglected by management, but rather it is an area which requires more attention than it is already given.

Several of the information security professionals interviewed pointed out that before managers can take on a bigger responsibility they need do not only need an increased awareness, but also they must possess a certain amount of knowledge in the subject. For example, Anna (Information Security Coordinator, B) believes that managers are not necessarily comfortable communication information security policies, and this may be caused due to a lack of knowledge in the subject. This Organization has taken steps to educate management by focusing on training in the subject. Organization A are also working on improving the information security awareness among managers. John (Information Security Officer, A) believes in devel-

oping awareness and knowledge around information security in the organization from the top down. Both organization A and B are hence adopting a similar strategy as the framework developed from the literature review.

5.3 Information security policy

The proposed framework suggests that when leaders have a high level of information security awareness, they will have better abilities to improve the information security behavior among employees. Management will then be able to influence employees to comply with the organizations information security policy. However, in order to ensure compliance of the given policy within the organization, management must first establish clear guidelines for how employees should act in order to keep information secure. Researchers within the field of information security agree that establishing an information security policy that includes information security guidelines for all employees is critical in order to effectively protect information systems.

The empirical study revealed that Organizations B and E have an information security policy which includes guidelines for employees. However, once theses guidelines have been put in place it is questionable whether or not these guidelines are effective in producing the desired results. The empirical study revealed that for Organization E, although guidelines are in place, the employees do not seem to follow the policy. An important factor for guidelines to be effective is for these to be up to date, as information security is an issue that is inherently changing to the rapid acceleration of technology. Organizations A and D admitted that the policies surrounding information security are dated and need to be upgraded to be successful. Despite this, both mentioned organizations emphasized that there are processes put in place to work on updating these policies. It does hence seem like most of the participating organizations believes that guidelines for the employees are important, but that they need to work further for the guidelines to contribute to an improved information security. This goes in line with the findings in the literature and it seems like the proposed framework could apply to the organizations examined in the empirical study. If these organization make sure that they have clear guidelines for employees and ensure compliance of these guidelines, their information security will be significantly improved.

5.4 Information security policy compliance

5.4.1 Creating overall awareness in the organization

The literature review reveled that many researchers within the field of information security highlight education and training as a key strategy to create security awareness among employees and hence increase the information security policy compliance. However, there are challenges surrounding these strategies for healthcare organizations as training programs can be very time consuming and resource intensive. It is clear

that all participating organizations except Organization C have some form of information security training for their employees. However, Organizations A, D and E are encountering challenges with communicating information security guidelines and trainings to all employees within the organization. In addition, the organizations are having difficulties in continuously keeping up to date with these trainings due to time constraints. For example, Anna (Information Security Coordinator, B) explained that in the healthcare industry, many employees are required to have specific skills in the field of healthcare itself. This means that time allocated for training is more likely to be prioritized within healthcare itself, and not information security. The proposed research framework suggests other strategies that leaders can adopt to create information security awareness and these strategies may be better suited for healthcare organizations.

When it comes to creating information security awareness within an organization, the role of management is undoubtably linked. Management can facilitate information security by creating and communicating clear and concrete security policies, making all information security activities and security processes visible to employees, encouraging information security knowledge-sharing, as well as actively participating hands-on in the information security work. These are the main pillars which would ensure that all members of the organization have an adequate level of knowledge and awareness regarding information security. However, the results from the empirical study imply that information security visibility and knowledge-sharing may be an important yet neglected factor to create information security awareness.

Many of the information security experts interviewed give examples that indicate that visibility and knowledge-sharing have contributed to awareness. This may not be due to specific actions and processes implemented directly in the organization, but awareness may also be raised through outside factors. For example, Hanna (Information Security Coordinator, E) explained that the increased attention that information security receives in media creates awareness. Furthermore, Lisa (IT Coordinator, D) explained that employee awareness increased when the General Data Protection Regulation was introduced, which in turn led to increased discussions and more active work towards information security within the organizations.

There are also examples in the empirical study of more direct approaches to enhance visibility and knowledge-sharing within the organization. Lisa (IT Coordinator, D) is one example of an employee who believes that visibility and knowledge-sharing will increase the information security awareness among employees. Examples of direct actions she has taken to manipulate these factors is regular visits to the various facilities in her organization. Through reminding people to log out when they leave the computer and encouraging discussion regarding information security issues, she is not only making employees aware, but she is making them evaluate their own behavior. She believes that it is an advantage that she is visible so that the staff is reminded of information security and the routines around it. This also suggests that communication

regarding information security can be direct, and does not necessarily have to involve management in order to spread the message.

In conclusion, the empirical results seem to support the proposed framework that knowledge-sharing and visibility can increase information security awareness within organizations. The participating organizations may be able improve employee's information security awareness by creating and communicating more clear and concrete security policies. Other key potential areas of improvement include increased managerial involvement, making information security activities more visible, and encouraging information security knowledge-sharing. The empirical study suggests that the organizations interviewed are aware of the benefits of these changes, thus organizations have taken the steps towards action in these areas.

5.4.2 Reduce the perceived inconvenience

The literature and hence the proposed framework suggests that management must find ways to reduce the perceived inconvenience related to information security measures. The perceived inconvenience often relates to these measures being time-consuming, and the perceived opportunity cost of working towards these measures. This seems to be particularly prevalent within healthcare organizations, due to it being a highly stressful and intensive environment. This is confirmed by the information security experts interviewed in this study. The empirical study revealed that lack of time is a major challenge related to information security for healthcare organizations. The participants from organization A, B, D and E working directly with information security all emphasized that the stressful work environment that many healthcare employees experience prevent them from achieving the level of information security that the they desire. It is also important to keep in mind that the opportunity cost for training or education could possibly be saving a human life, which makes the industry extremely careful to prioritize information security. Several organizations expressed that it was unreasonable to add to an employees workload by implementing information security trainings, when this is taking away time not only from the employees, but also the patients they serve.

The literature suggests two key strategies to reducing the perceived inconvenience related to information security measures. Both of these strategies are likely to, if implemented correctly, help healthcare organizations increase information security policy compliance. It will not only contribute to compliance of existing policies, but it will also enable implementation of further security measures. The first strategy is for managers to find a way to communicate to employees that behave in accordance with information security policies is a part of their daily work. This stems from the fact that many employees may not understand the importance of information security, or believe that it plays a part in their specific role within the organization. If employees believe that it is in fact a part of their job, employees are more likely to understand to not prioritize the completion of other tasks over complying with information security policies. This strategy

could most likely be useful for healthcare organizations. As previously mentioned, several interviewees in the empirical study believe that managers in their organization could take on a bigger responsibility in communicating and educating employees in information security issues. In line with the literature, managers could probably more specifically communicate to employees that information security must be taken into account in order to be able to take care of their patients in the best possible way. This would create a shift in the mind-set from information security being something that takes time away from patients, to that of something that is critical for employees to properly take care of their patients.

The other strategy involves finding a way to implement information security activities without them conflicting with or obstructing employees daily work. Karlsson, Hedström, and Goldkuhl (2017) stress that employees should not have to prioritize between information security and their work. Well-designed policies will make it easier for employees to be compliant with information security policies. Furthermore, Karlsson, Hedström, and Goldkuhl (2017) suggests how beneficial policies should be designed by proposing eight quality criteria for the design of information security policies in healthcare. The empirical study suggests that those who work with information security in healthcare do not seem to aspire to implement enough measures because it would obstruct employees daily work in an already stressful environment. It is clear that many organizations sees focusing on information security as a choice, which in turn will have an opportunity cost on other areas within the organization. There could be several reasons why employees may feel that investing or spending time on information security will obstruct their daily work. One reason is the lack of support from management. If managers are not sufficiently committed, this makes it harder for employees to understand that information security should be embedded and integrated within their daily work. Secondly, some of the existing guidelines that organizations have chosen to implement may in fact be too time consuming or complex, which leads to information security becoming an obstruction or add-on to other tasks. If management and the information security experts work together to formulate an information security policy in accordance with the quality criteria that Karlsson, Hedström, and Goldkuhl (2017) propose, these policies and guidelines would most likely be more efficient and this not interfere with other tasks or job roles within the organization.

Through the empirical study, it was apparent that there was a difference in the way that employees who did not directly work with information security viewed the challenges related to perceived inconvenience. This may be due to a lack of implemented and adopted information security measures, which means the employees have not been able to obtain an understanding of the issues. In the empirical study these employees seemed positive to change in information security measures, suggesting that employees would be open to investing time in their current roles to create more awareness and knowledge within information security.

5.4.3 Enhance organizational commitment

The findings from the literature review suggests that organizational commitment positively impacts employee compliance with information security policies. Committed employees often, according to the literature, want to achieve success in their careers. Highly committed employees would therefore avoid engaging in deviant behaviors, such as non-compliance as this may diminish their personal image or affect their career success. Leaders can, hence, enhance organizational commitment by improving organizational factors such as the performance and reward system, as well as the training and career development system. However, healthcare employees do not seem to value personal achievement and career success in the same way, being motivated through moral factors rather than performance or financial rewards. The empirical results showed that the biggest motivations for healthcare employees is to give their patients the best possible help. To enhance organizational commitment by improving career opportunities within the organization does, therefore, not seem to be appropriate for healthcare organizations. However, if management made it clear that complying with information security was crucial for the patients in care, this would create a level of organizational commitment relevant for the health care sector.

5.4.4 Developing a beneficial ethical climate

The proposed framework suggests that leaders can enhance the ethical climate in the organization to improve the information security compliance. Employees attitudes towards information security are influenced by personal values and moral beliefs. Behavior can also be effected through the expectations of relevant others and colleagues acting in accordance with the security policy. Leaders are thus able to adjust and influence the employee's personal norms and the general social norm toward information security policy compliance. The empirical study suggests that ethics and moral are important for healthcare employees. Moral issues are discussed daily in most of the participating organizations. This suggests that leaders could improve the information security in these organizations by adjusting the ethical climate and the social norm so that information security becomes an important moral issue. If leaders were to communicate that obstructing information security would be considered a moral violation, this would likely motivate and incentivize healthcare workers.

The literature suggests several strategies to influence social and personal norms. Firstly, organizations can implement campaigns that announce social norms towards information security policy compliance. This would likely be an effective strategy for healthcare organizations as employee's behavior is often guided by social norms. Through campaigns, management can convey that information security is important to the organization and that all employees are responsible for the information security related to their patients. The empirical study revealed that issues related to information security are often discussed amongst employees in the participating organizations. There is thus an opportunity for management to shape

this discussion to improve the information security behavior among employees. Secondly, management can shape the organizational environment toward rule-following in general and specifically information security policy compliance. The empirical results show that healthcare organizations have high moral standards, however due to dated policies or lack of support from management, employees do not necessarily see the guidelines as strict rules. Creating this framework would likely make the employees more compliant.

Finally, leaders can influence the personal and moral beliefs within the organization through leading by example and creating the behavior and norms though their own actions. In the empirical study, no participant pointed to specific behaviors and actions taken by individual members of management. This suggests that leaders within healthcare organizations can take more responsibility in publicly displaying acts or behaviors that would possibly affect the organizations information security.

5.5 Information security culture

The proposed framework suggest that if management influence their employees to better information security behaviors through the proposed strategies, an information security culture will develop over time. This is because an information security culture is, according to the literature, created through the interaction employees have with information assets and the security behavior they develop. The empirical study revealed that building a strong information security culture is the ultimate goal of the information security work in all of the participating organizations. As culture is not something created on its own, it is important that organizations work on the mentioned strategies to improve information security, and a culture will be created as a result. Building a culture ensure continuity, as when a strong culture is developed, it is more likely that information security will continue to be a priority. If information security is part of an organizations culture, this would lead to it becoming increasingly embedded within the organization, and not a choice with a specific opportunity cost. This confirms that the framework can be used by healthcare organizations to improve their information security culture.

Organization C has a very strong information security culture according to Dan, Head of Finance and Ellen, Site Manger. This is interesting since they have not implemented any of the proposed strategies to enhance employee's information security behavior. Dan believes the inherent role of confidentiality and private information within the company, has lead to information security being embedded within the organization. This is interesting as it can be argued that confidentiality is crucial in most if not all healthcare organization, however not all of the organizations in the empirical study were as confident regarding their own culture. Even though employees understand that information security is very important, it can be difficult for them to know how to behave if there are no clear guidelines. Thus a culture is not enough, if the guidelines are not clear. Researchers within the field of information security agree that information security guidelines

are important. Ellen also mentioned patient confidentiality, and expressed that the guidelines were clear. However, she questioned whether or not the guidelines are distributed or communicated in a way that all employees are aware. Thus, it can be argued that an organization is only successful handling information security when a strong culture is also combined with efficient actions.

5.6 Technical security controls

There is a consensus among researchers within the field of information security that technical measures and controls are not sufficient to achieve an adequate level of information security without the correct behavior of employees. The empirical study showed this to be true according to the interviewees. Employees at Organization A, B and E agreed implementing security controls will not have the desired effect if employees do not know the purpose or how they should work with these tools. The empirical study suggested that if employees were to not understand these tools, they would eventually find ways to work around them. For example, Anna (Information Security Coordinator, B) explains that if employees do not have the awareness and you implement compelling security controls, employees will find other creative approaches to do their work that may involve major security risks. This emphasizes the importance of the employees in the handling of information security. Technical security controls are a tool, but if these tools are not used correctly they will eventually become irrelevant.

Technical security controls can, however, mitigate the security threat that employees non-compliance may result in. Technical measures may therefore be implemented together with other measures, but it is important that the technical security controls that are implemented do not disturb the work too much. Lisa (IT Coordinator, D) believes that many security controls are beneficial in theory but do not work in practice. For example, Organization D has implemented a number of technical security controls and some of these controls have worked very well, while in other cases the solution disturbs the daily work too much. In line with this, John, emphasizes that it is important that the technical security controls purchased must work in employees daily work. The literature suggests a number of technical solution that can mitigate the insider threat that employees information security behavior may result in and if these are implemented with employees work practices in mind, like discussed in section 5.4.2 (Reduce the perceived inconvenience), they may be a helpful to improve the level of information security in these organizations.

Unlike the other organizations, Organization C, does not seem to agree with the literature saying that technical measures are not sufficient to achieve an adequate level of information security related to the employees. The organization has invested a lot in their IT solutions and seems to believe that the system is providing the security. Dan (Head of Finance, C) believes that the IT systems that employees use in their work have clear guidelines so that it is difficult to make mistakes, the system is in itself very secure.

Moreover, Ellen, Site Manager, emphasis that the technical solutions that the organization use is providing the security. This goes against the literature and further research is probably necessary to understand whether it is possible to achieve a adequate level of information security with only technical solutions. Organization C has a different focus in their information security work than what the proposed framework suggest, the results from the study of Organization C can thus neither reject nor confirm whether the framework would work in practice for healthcare organizations.

6 Conclusions

The aim of this thesis was to develop a framework for how healthcare organizations can act to manage the human factor in information security without taking time and resources away from patient care. To achieve this purpose, three separate research questions were examined.

The first research question addressed the literature's view on how organizations can act to develop an adequate the level of information security related to employee behavior. The literature review suggests that organizations can develop an adequate level of information security related to the employees by first establishing an information security policy that includes guidelines for all employees, and then continue to work on ensuring compliance of that policy. If all employees follow the established policy, the organization can ensure that they have the level of information security related to employees that they require to avoid or manage security threats. Information security policy compliance will also over time lead to the development of an information security culture, which according to the literature will further strengthen the information security in the organization. It is hence important to improve the compliance of information security policies within the organization. The results suggest that leaders can positively influence employee's information security policy compliance without taking time and resources from patient care if they themselves manage and implement information security. This suggests that if management devotes sufficient resources to information security work, this can improve information security without the opportunity cost being time and resources taken away from patients. Furthermore, management will utilize strategies such as creating information security awareness, enhancing organizational commitment, reducing perceived inconvenience, as well as developing a beneficial ethical climate to improve employee's information security policy compliance. However, it is necessary that management has a high level of information security awareness, in order to manage and implement information security successfully.

The second research question asked if the suggested strategies in the literature review to increase the level of information security related to employees would work in practice when implemented in healthcare organizations. The findings from the empirical study suggests that the framework developed in the literature review would, to a great extent, work in practice for healthcare organizations. Four out of the five participating organizations stated that they would significantly increase the level of information security if they established clear guidelines for all employees and ensured compliance of said guidelines through improving the information security leadership in the organization. The participating organizations were generally open and positive to changes that would improve information security. If management improved the overall information security awareness in the organization, reduced the perceived inconvenience, and influenced the ethical climate toward information security, many of their information security deficiencies would be

addressed. Implementing these strategies would lead to an improved information security culture, which was the ultimate goal for all organizations that participated in the study. However, one strategy to improve employee's information security policy compliance that did not seem to apply to healthcare organizations was to enhance organizational commitment. The framework should therefore be revised to not include this strategy.

The final research question addressed how technical security controls can help mitigate the information security risks that the human factor contributes to. The results from the literature review suggest that technical security controls can help mitigate the insider threat that employee's non-compliance and poor information security behavior results in. There is, however, a consistent view expressed in the literature that technical measures alone are not sufficient to achieve an adequate level of information security related to the employees. It is therefore important to combine technical security controls with other information security measures. One of these measures, as mentioned above, is to ensure that all employees comply with the information security policy. This goes in line with the majority of the data gathered from the empirical study, as most of the participating organizations do not believe that technical security controls are sufficient to achieve the level of information security they desire. However, Organization C has implemented a strategy where they rely entirely on technical security solutions. The organization believes that they have an adequate level of information security, which is not in line with the remaining results from the empirical study or what has been said in the literature. A deeper analysis of this individual organization is needed to be able to answer whether this strategy is sufficient. However, the results of this study suggest that technical security controls should be implemented together with other measures in order to create an adequate level of information security.

In conclusion, the results suggests that healthcare organization can improve their information security related to their employees without taking time and resources from patient care if they implement the final framework which can be seen in figure 5 below.

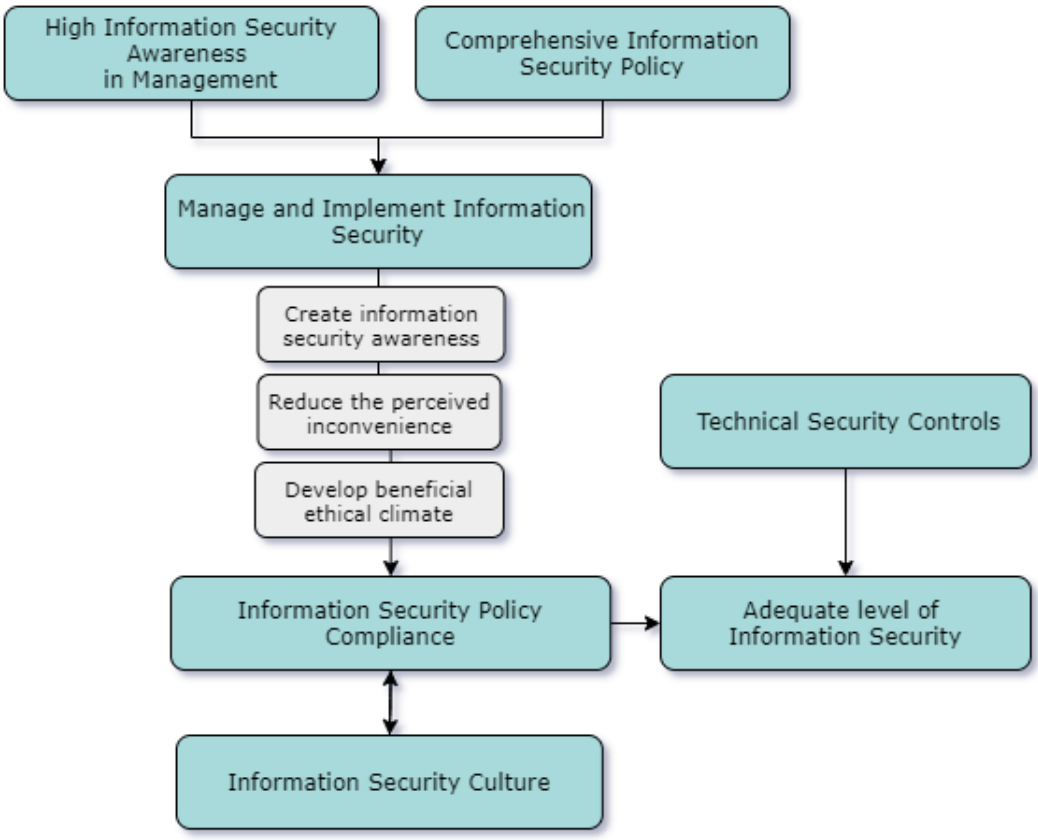

Figure 5: Final framework to improve information security related to employees

References

[1] Z. A. A. Abdelsadeq et al. “Unintentional Insider Threats Countermeasures Model (UITCM)”. In: *2019 International Conference on Cybersecurity (ICoCSec)*. 2019, pp. 53–58.

[2] Zauwiyah Ahmad et al. “Security Monitoring and Information Security Assurance Behaviour among Employees.” In: *Information Management & Computer Security* 27.2 (2019), pp. 165–188.

[3] Sultan AlGhamdi, Khin T. Win, and Elena Vlahu-Gjorgievska. “Information security governance challenges and critical success factors: Systematic review.” In: *Computers & Security* 99 (2020), p. 102030.

[4] A. AlHogail. “Design and Validation of Information Security Culture Framework”. In: *Computers in Human Behavior* 49 (2015), pp. 567–575.

[5] A. AlHogail and A. Mirza. “Information security culture: A definition and a literature review”. In: *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. 2014, pp. 1–7.

[6] Jason Andress and Mark Leary. *Building a Practical Information Security Program*. Amsterdam, [Netherlands]: Syngress, 2017 and 2016.

[7] Hilary Arksey and Pete T Knight. *Interviewing for social scientists an introductory resource with examples*. Sage Publications, 1999.

[8] Shuchih Ernest Change, Anne Yenching Liu, and Yu-Teng Jacky Jang. “Exploring Trust and Information Monitoring for Information Security Management”. In: *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*. IEEE, 2017, pp. 1–5.

[9] Yan Chen, K. (Ram) Ramamurthy, and Kuang-Wei Wen. “Impacts of Comprehensive Information Security Programs on Information Security Culture”. In: *Journal of Computer Information Systems* 55.3 (2015), pp. 11–19.

[10] Alena Yuryna Connolly et al. “The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study.” In: *10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*. Frankfurt, Germany: Plymouth University, 2016, pp. 34–44.

[11] John D’Arcy and Paul B. Lowry. “Cognitive-affective Drivers of Employees’ Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study”. In: *Information Systems Journal (Oxford, England)* 29.1 (2017 and 2019), pp. 43–69.

[12] A. Da Veiga and J.H.P. Eloff. “A framework and assessment instrument for information security culture”. In: *Computers & security* 29.2 (2010), pp. 196–207.

[13] ENISA. *Insider threat - ENISA Threat Landscape*. 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat.

[14] Aqsa Fatima and Ricardo Colomo-Palacios. "Security Aspects in Healthcare Information Systems: A Systematic Mapping." In: *Procedia Computer Science* 138 (2018), pp. 12–19.

[15] Gengzhong Feng, Jiawen Zhu, and et al. Nengmin Wang. "How Paternalistic Leadership Influences IT Security Policy Compliance: The Mediating Role of the Social Bond', Journal of the Association for Information Systems". In: *Journal of the Association for Information Systems* 20.11 (2019), pp. 1650–1691.

[16] J. L. Fernández-Alemán et al. "Technical solutions for mitigating security threats caused by health professionals in clinical settings". In: *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 2015, pp. 1389–1392.

[17] Yotamu Gangire, Adele Da Veiga, and Marlien Herselman. "A Conceptual Model of Information Security Compliant Behaviour Based on the Self-Determination Theory." In: *2019 Conference on Information Communications Technology and Society, ICTAS 2019*. Durban, South Africa, South Africa: IEEE, 2019, pp. 1–6.

[18] Bill Gillham. *Case study research methods*. London: Continuum, 2000.

[19] Laurent Gisel and Lukasz Olejnik. *The potential human cost of cyber operations*. International Committee of the Red Cross, 2018.

[20] F. L. Greitzer et al. "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies". In: *2014 47th Hawaii International Conference on System Sciences*. 2014, pp. 2025–2034.

[21] Felix Haeussinger and Johann Kranz. "ANTECEDENTS OF EMPLOYEES' INFORMATION SECURITY AWARENESS - REVIEW, SYNTHESIS, AND DIRECTIONS FOR FUTURE RESEARCH". In: *In Proceedings of the 25th European Conference on Information Systems (ECIS), June 5-10, 2017*. Guimarães, Portugal, 2017.

[22] JinYoung Han, Yoo J. Kim, and Hyungjin Kim. "An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective." In: *Computers & Security* 66 (2017), pp. 52–65.

[23] Emil Hellerud. *Allt vanligare att privatpersoner utpressas med stulna uppgifter*. 2021. URL: https://www.tv4.se/artikel/4X9UbYNQRQ324PYv16X6O0/allt-vanligare-att-privatpersoner-utpressas-med-stulna-uppgifter (visited on 04/11/2021).

[24] Inho Hwang, Daejin Kim, et al. "Why Not Comply with Information Security? an Empirical Approach for the Causes of Non-Compliance". In: *Online Information Review* 41.1 (2017), pp. 2–18.

[25] Inho Hwang, Robin Wakefield, et al. “Security Awareness: The First Step in Information Security Compliance Behavior”. In: *The Journal of Computer Information Systems* (2019), pp. 1–12.

[26] International Organization for Standardization. *Information technology - Security techniques -Information security management systems – Requirement*. 2017.

[27] Fredrik Karlsson, Karin Hedström, and Göran Goldkuhl. “Practice-Based Discourse Analysis of Information Security Policies.” In: *Computers & Security* 67 (2017), pp. 267–279.

[28] Aamir Hussain Khan et al. “SartCyber Security Awareness Measurement Model (APAT)”. In: *IEEE* (2020), p. 298.

[29] Alex Koohang, Jonathan Anderson, et al. “Building an awareness-centered information security policy compliance model”. In: *Industrial Management & Data Systems* 120.1 (2019;2020;), pp. 231–247.

[30] Alex Koohang, Alojzy Nowak, et al. “Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness”. In: *Journal of Computer Information Systems* 60.1 (2020), pp. 1–8.

[31] Abhijit Mohanta, Mounir Hahad, and Kumaraguru Velmurugan. *Preventing Ransomware: Understand, Prevent, and Remediate Ransomware Attacks*. Birmingham, England;Mumbai, India;: Packt Publishing, 2018.

[32] MSB. *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden*. 2020. URL: https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf.

[33] MSB. *Metodstöd för systematiskt informationssäkerhetsarbete*. n.d. URL: https://www.https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/metodstod-for-systematiskt-informationssakerhetsarbete (visited on 04/11/2021).

[34] Kathryn Marie Parsons et al. “The Influence of Organizational Information Security Culture on Information Security Decision Making”. In: *Journal of Cognitive Engineering and Decision Making* 9.2 (2015), pp. 117–129.

[35] Johnny Saldaña. *Fundamentals of Qualitative Research*. Oxford University Press, 2011.

[36] M. N. K. Saunders, Philip Lewis, and Adrian Thornhill. *Research Methods for Business Students*. Pearson: New York;Harlow, England, 2012.

[37] Shwadhin Sharma and Merrill Warkentin. “Do I really Belong?: Impact of Employment Status on Information Security Policy Compliance.” In: *Computers & Security* 87 (2019), p. 101397.

[38] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. “Information security policy compliance model in organizations”. In: *Computers & security* 56 (2016), pp. 70–82.

[39] Tomasz Stefaniuk. “Training in shaping employee information security awareness”. In: *Entrepreneurship and Sustainability Issues* 7.3 (2020), pp. 1832–1846.

[40] H. Stewart and J. Jürjens. “Information security management and the human aspect in organizations”. In: *Information management computer security* 25.5 (2017), pp. 494–534.

[41] Marie Ström. *IVO: Personalbristen i vården måste upp på högsta ledningsnivå*. 2019. URL: https://lakartidningen.se/aktuellt/nyheter/2019/03/ivo-om-risker-och-brister-2018/ (visited on 04/11/2021).

[42] Sveriges läkarförbund. *Digitalisering i vården*. n.d. URL: https://slf.se/var-politik/digitalisering-i-varden/ (visited on 04/11/2021).

[43] Isaac Wiafe et al. “The Role of Norms in Information Security Policy Compliance”. In: *Information & Computer Security* 28.5 (2020), pp. 743–761.

[44] Adel Yazdanmehr and Jingguo Wang. “Employees’ Information Security Policy Compliance: A Norm Activation Perspective”. In: *Decision Support Systems* 92 (2016), pp. 36–46.

[45] Adel Yazdanmehr, Jingguo Wang, and Zhiyong Yang. “Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance”. In: *Information Systems Journal (Oxford, England)* 30.5 (2020), pp. 791–844.

Appendix

Appendix A: Interview questions for employees responsible for information security

Background

- Can you please tell me a bit about the company in terms of what you mainly focus on and what your core objectives are?
- What is your role at (Company name) and can you please provide a brief job description?
- How long have you been working at (Company name)?

Information security in general

- Are there any processes in place at (Company Name) to improve information security and if so what are they?
- What do you perceive are the main challenges that (Company Name) are facing when it comes to achieving a desired level of information security?

Leadership

- In what ways is management working on a leadership level to improve and maintain information security within the company?
- What role does management play in motivating employees to follow guidelines on information security and do you believe it is possible for management to take more responsibility within this area?

Technical security controls

- In what ways is (Company Name) innovating and/or implementing technical security controls in order to reduce the risk of security threats caused by human factors?
- What do you beleive are the benefits of investing in new technical security controls in order to reduce the security risks that employees are exposed to? Could there be any potential disadvantages to investments in this area?

Information security culture

- Can you think of an example were employees have expressed information security awareness?
- What role do you think information security plays in your company culture?

Appendix B: Interview questions for employees not responsible for information security

Background

- Can you please tell me a bit about the company in terms of what you mainly focus on and what your core objectives are?
- What is your role at (Company name) and can you please provide a brief job description?
- How long have you been working at (Company name)?

Information security in general

- Are there any processes in place at (Company Name) to improve information security and if so what are they?
- What do you perceive are the main challenges that (Company Name) are facing when it comes to achieving a desired level of information security?

Information security awareness

- Have you and your colleagues received any form of information security training?
- Would you say that you and your colleagues have an adequate knowledge about information security?

Inconvenience

- Do you feel that information security measures affect your or your colleagues' work?
- How would you feel if more information security measures were implemented?

Motivation and commitment

- What is the biggest motivation for you and your colleagues in your work?

The ethical climate

- Can you come up with a scenario where you and your colleagues discuss information security issues?
- Are there times when it is necessary not to follow information security guidelines?
- Do you discuss moral issues in general?

Information security culture

- What role do you think information security plays in your company culture?