LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Agnes Ekfors Elvin
Fredrik Sundström
William von Heland

Supervisor: Miranda Kajtazi

Grading Teachers: Select an object.
Select an object.

Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations

AUTHORS: Agnes Ekfors Elvin, Fredrik Sundström, William von Heland

PUBLISHER: Department of Informatics, Lund School of Economics and Management, Lund University

PRESENTED: June, 2021

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Christina Keller, Professor

NUMBER OF PAGES: 128

KEY WORDS: teleworking, cyber security, threats, risks, forced, social, technical, risk tolerance

ABSTRACT (MAX. 200 WORDS): This study investigates the cyber security threats and risks that are associated with forced teleworking during the period of Covid-19, when organizations have been forced to telework. Three different main aspects from two theories have been crucial when investigating the threats and risks associated with forced teleworking, which are the Social, Technical and Risk Tolerance aspects. This study is of a qualitative nature, where five different interviews have been conducted to see similarities and differences between literature and practice of threats, practices, standards and frameworks used. From the three aspects, the findings show that cyber security threats and risks have increased during this time period, but nothing that could not be handled. It has been concluded that legislation and regulations needs to be highlighted when deciding certain practices to prevent risks and threats, and that employee training is the most important cyber security practice. Furthermore, new trends of social engineering have risen and the scaled up teleworking cannot be seen as a crisis from a cyber security perspective. Finally, it can also be noted that employees with more knowledge about threats, risks and practices might lead to a more risk taking behaviour which could harm teleworking organizations.

Content

Figures

Table

1 Introduction

Ben Fairweather (1999) defines teleworking as "using information and communications technologies (ICTs) to bring work to the worker, rather than require them to go to the work" (Fairweather, 1999, p. 40). Moreover, Kowalski and Swanson (2005) describe teleworking as remote work arrangements and define the definition by saying that all work that is done outside of its primary location is teleworking. Baruch (2001) states that teleworking is an alternative to the regular way of working and that it is enabled through the development of Information Technology and Information Systems. Teleworking has multiple benefits for employees and employers as employees can work efficiently wherever they are comfortable, whilst employers possibly can save money by removing some office space (Fairweather, 1999).

According to Belzunegui-Eraso and Erro-Garcés (2020) teleworking as a definition started in the 1970s as a result of the oil crisis. In 2001 approximately 28 million people in the United States of America teleworked in one way or another and since then the numbers have continued to grow (Kowalski & Swanson, 2005; Evangelakos, 2020). With better technical solutions on the market the availability and easiness of connecting online have improved (Dery, Sebastian & van der Meulen, 2017). Another reason for the growing numbers of teleworking is forced reasons that organizations cannot handle by nature (Krishna, Nicholson & Sahay, 2003). It is common in project teams to telework, especially as development teams often are outsourced to other countries in contrast to where the rest of the team is located (Krishna, Nicholson & Sahay, 2003). Another forced reason for teleworking is the Covid-19 pandemic. It has led to employees from all kinds of organizations working from home, in other words teleworking (European Commission, 2020). According to a report from the European Commission, released in 2020, only 5,4 percent of the employed population in the European Union worked from home in 2019 (European Commission, 2020). In contrast, the same report mentions that approximately 40 percent teleworked in the beginning of the pandemic (European Commission, 2020). As the restrictions and recommendations for the pandemic have become stricter with time, the number of people teleworking has increased (Gartner, 2020).

Teleworking results in challenges for organizations regarding security issues (Rikitake, Kikuchi, Nagata & Asami, 2001; Yang, Zheng, Zhu, Chen, Zhao & Valluri, 2013). This challenge was current before the Covid-19 pandemic but has grown as the number of teleworkers have grown with Covid-19, as earlier mentioned (Belzunegui-Eraso & Erro-Garcés, 2020). In 2001 Rikitake et. al highlighted the security issue for businesses as many models for teleworking had been developed but without a focus on security policies. The security issues they saw in 2001 are more or less the same as today meaning home networks are targets for malicious attacks as they are vulnerable, always connected and without good firewalls (Rikitake et. al, 2001). Still, employees working from home have to reach and have access to the same data and information as they would have if they worked from an office, where the networks are much more secure (Nastase & Ionescu, 2011). Nastase and Ionescu (2011) describe the biggest challenge with teleworking being to create a framework that enables an employee to get full access to internal data with maximum security and integrity. It is important for an organization to understand the risks and challenges associated with teleworking (Yang et. al, 2013). In order to handle and mitigate the security risks associated with having employees working in other places than at the office, organizations need to be sure they know the risks and have solutions for them (Yang et. al, 2013). If companies are not prepared, they do not have the

chance of handling situations like Covid-19 in advance (Evangelakos, 2020). Due to the pandemic, teleworking has become the new norm for many people and organizations and as it came as a surprise, the preparedness was difficult to predict (Evangelakos, 2020). The information and data that an organization has is valuable, as well as its critical corporate assets that they want to protect (Evangelakos, 2020). With forced teleworking many organizations cannot ensure this (Evangelakos, 2020). It is difficult to change a whole organization's information security landscape over a night as this is something that takes time to change (Evangelakos, 2020).

However, as the trend of teleworking has constantly grown since the 1970s, many organizations were prepared for this forced teleworking situation, but others were not (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020). Microsoft has released numbers showing an increase in Microsoft Teams meetings with over 500 percent and the concepts of Bring Your Own Device (BYOD) and cloud-computing has never been as relevant (Evangelakos, 2020). With a growing number of hackers and with a growing worth of data, the number of malware attacks have increased significantly (Firch, 2021). Together with this, research can already show that attackers have used the situation of Covid-19 and weak data protection with more malware- and phishing attacks (Evangelakos, 2020). This problematic situation has to be handled by organizations with speed as the consequences of cyber attacks can lead to organizational crisis and be expensive to solve afterwards (Evangelakos, 2020).

1.1 Research Problem

Teleworking for organizations has some clear potentials and possibilities, however security issues exist, especially for smaller companies in terms of expertise and resources (Pyöriä, 2011). Teleworking is environmentally friendly, has the possibility to create flexible work arrangements, it can be a way of raising a company’s corporate image, as well as it has the possibility to improve job-control, well-being at the individual level and overall efficiency of organizations (Pyöriä, 2011; Mello, 2007; Belzunegui-Eraso & Erro-Garcés, 2020). It is however stated that teleworking is best suited for jobs that necessitate peace and concentration, and away from unnecessary interruption (Pyöriä, 2011). It has also been found that it differs between managers and professionals apart from other employees (Martinez-Sanchez, Pérez-Pérez, de-Luis-Carnicer & Vela-Jiménez, 2006). Professionals and managers need to reorganize the way they work in order to allow flexibility and work capacity to continue as it should, however it is stated that when the Covid-19 crisis happened there was a lack of contingency plans that involved teleworking when companies were forced to work remotely (Belzunegui-Eraso & Erro-Garcés, 2020; Martinez-Sanchez et al., 2006). Moreover, Belzunegui-Eraso and Erro-Garcés (2020) argue that the implementation of teleworking possibilities moves slower than expected for organizations.

Teleworking risks involve security risks for disclosure, modification and destruction of data from personnel, physical and administrative security vulnerabilities (Yang et. al, 2013). However, Yang et al. (2013) present different solutions and main components to the risks previously presented. What has failed to be addressed is how to handle these issues on a larger scale, when a vast majority of employees are forced to work from home, which eventually could lead to a scaled up teleworking force as the new norm. Moreover, it has been stated that organizations should determine within the company what kind of remote access should be

permitted from which kind of client device (Souppaya & Scarfone, 2016). Another key recommendation is that organizations should reassess their policies for telework devices after a time, which involves limiting the types of devices and also the level of access that they may be granted (Souppaya & Scarfone, 2016). These recommendations imply that it is not encouraged to telework with a large amount of devices with full access to the organization, which might be needed in a time when everyone is forced to telework (Souppaya & Scarfone, 2016).

Teleworking has its growing popularity due to the Covid-19 crisis, and while some are positive to its implementation in organizations, others are not (Vrchota, Marikova & Rehor, 2020; Belzunegui-Eraso & Erro-Garcés, 2020). It also differs in what kind of industry that has been more open to teleworking before the emergence of Covid-19 and which ones that had already adopted this style of working (Vrchota et al., 2020). Nevertheless, the precautions made to protect citizens from the Covid-19 crisis, which involves the implementation of teleworking, comes with great cyber security risks for enterprises of all sizes (Vrchota et al., 2020). Nilles (1991) predicted that teleworking would become a widespread researched phenomenon. In contrast to his predictions, a research gap can be seen in the teleworking area as of today. The gap in the area of research is rather broad at the same time as there is an increasing number of users of teleworking tools used by various teams (Pearce, 2009). In the literature it seems to be a knowledge gap in security risks, threats and solutions when teleworking is forced upon an organization, which has led to a scaled up teleworking force that can be exposed to more threat actors. While the popularity of implementing telework increases, it also increases the amount of employees working from less secure locations, which means that the security risks, threats and solutions associated with it needs a more comprehensive exploration when the majority of organizations work remotely.

1.2 Research Motivation

New demands from customers are requiring companies to be more flexible in their work, this is threatening the traditional way of working and forcing organizations to use a more innovative workstyle (Gratton, 2004). Many employees in organizations have been using the teleworking tools voluntarily during history (Salomon & Salomon, 1984). Because of new demands that are requiring more remote work, some employees are now forced into starting to use the teleworking tools in their daily work (Kilpi, 2020; Bakac, Zyberaj & Barela, 2020). Teleworking is now playing a bigger part of the daily worklife in organizations than ever before (Kilpi, 2020). Because of this fact it is highly important to have more relevant research within the teleworking area itself, just as Nilles was longing for in 1991.

Despite the fact that numerous studies have been executed about collaboration through teleworking, a research gap can still be seen when it comes to what security risks and threats that exist when coworkers are being forced into working and collaborating through teleworking tools. This knowledge gap is something that this thesis aims to investigate through this research. Traditional working styles are changing as they need to be able to fulfill the market's new requirements, such as being more flexible and being able to work from home in pandemic times (Gratton, 2004; Gartner, 2020). In order to be more flexible, organizations have started to use a mixed approach containing traditional and remote work (Review & Brumma, 2016). Even if many studies have been done within the area, they still differ in their results of what benefits and issues the organizations might face when teleworking in a wider range.

Moreover, it can be argued that there still are few articles and studies covering effects of teleworking as this style of working has increased in popularity, especially in 2020 and 2021 during Covid-19.

Informatics as a research area is rather broad and this thesis will cover the areas of Social, Organization and Technology, which are the three pillars of Informatics. In this study it has been decided to focus on how organizations' cyber security are affected by teleworking when being forced to work from other places than the regular office. The authors of this thesis claim that the topic is strongly connected to the Informatics area. Furthermore, the authors of this thesis believe that the collaboration within organizations and through the teleworking tools is connected to the Social pillar (Belzunegui-Eraso & Erro-Garcés, 2020). The companies that are of focus for this thesis have a clear connection to the organizational pillar. Finally, the teleworking tools are built by and are working through technology, which makes the connection to the technological pillar present in this thesis (Belzunegui-Eraso & Erro-Garcés, 2020).

1.3 Purpose

Reflecting upon the research problem and motivating the need to conduct this study, the purpose of this thesis is to identify and gain clarity on how forced teleworking affects organizations when it comes to cyber security issues. The aim of this study is to understand and describe the risks and threats that are associated with forced teleworking for organizations. Through investigating the topic by looking into it from three main aspects, the Social aspect, the Technical aspect and the Risk Tolerance aspect, it is possible to answer the research question.

1.4 Research Question

In this study taking the focus on an organizations' cyber security threats and risks by forced teleworking emphasizes the need to better understand cyber security risks and threats in response to forced teleworking. Therefore, the following research question:

What cyber security risks and threats are there for organizations associated with forced teleworking?

1.5 Delimitation

While teleworking has been invented in the previous millenium (Qvortrup, 1998) and has become a practice for many decades (Babulak, 2009; Erro-Garcés, 2020; Harris, 2003; Kowalski & Swanson, 2005; Evangelakos, 2020) in this study we intend to tackle a particularly intense period of teleworking that has led us to identify it as forced teleworking. The focus for this study is therefore solely on organizations that have an active operation in Sweden and that were forced to telework due to Covid-19 pandemic. Moreover, this study is qualitative in nature, with five respondents from five different organizations and that it is not easy to capture the intentions of all organizations that have an active operation in Sweden during the forced

teleworking period, but that we can still identify important patterns to understand the issue better.

2 Theoretical Background

The theoretical background consists of the literature found in order to gain understanding in the research topic. 2.1 explores teleworking as a timeline, its effects and defines the meaning of forced teleworking. 2.2 focuses on cyber security and its threats, whereas 2.3 focuses more on practices inside organizations. Finally, 2.4 portrays security practices embedded in teleworking and 2.5 builds the research model for this thesis.

2.1 Teleworking

2.1.1 A Timeline of the History of Teleworking

According to Qvortrup (1998) the concept of teleworking had a negative meaning when it developed in the 1970s and 1980s in the United States of America as the work that was related to teleworking was low-paid, unskilled jobs. The most important moment in history for teleworking was the development of the internet in the 1970s (Babulak, 2009). The internet allowed for new ways of communicating and handling of information (Babulak, 2009). Moreover, electronic network accessibility together with the growing accessibility of portable computers enabled for flexible places of working (Babulak, 2009). Belzunegui-Eraso and Erro-Garcés (2020) on the other hand deem teleworking started as a result of the oil crisis. Qvortrup (1998) meant teleworking was similar to electronic homework or described low paid office work done from home. In 1985, teleworking got an updated definition, it was seen as people working from home with computers connected to offices (Qvortrup, 1998). Employees started to telework to avoid travelling to offices and offshore countries for affairs, especially entrepreneurs that were early adopters of teleworking as they could work from home and did not need access to physical offices (Qvortrup, 1998). However, organizations also saw potential in teleworking being a likely direction for organizational development in 1996 (Harris, 2003).

A historical overview of teleworking is shown below (see Figure 2.1). The figure intends to highlight key developments of the evolution of teleworking through decades, starting with the early 1970s.

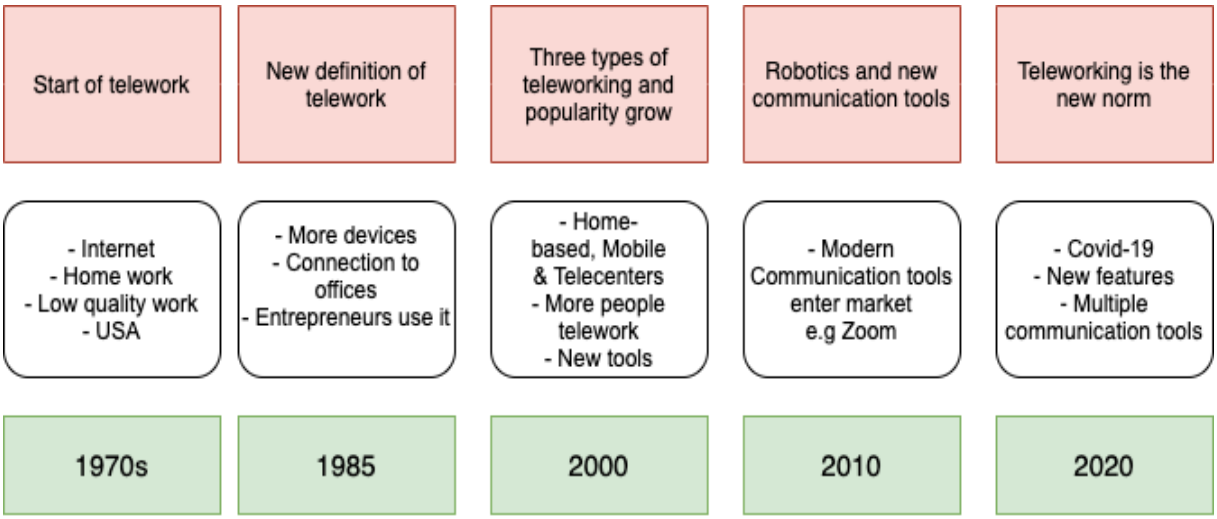


Figure 2.1: The evolution of teleworking found in literature (Qvortrup, 1998; Babulak, 2009; Erro-Garcés, 2020; Harris, 2003; Kowalski & Swanson, 2005; Evangelakos, 2020)

Since then, multiple technologies have been invented which has enabled for smoother and more efficient telework, even between different parts of the world (Babulak, 2009). In 2001 approximately 28 million people in the United States of America teleworked in one way or another (Kowalski & Swanson, 2005). The number of teleworkers in the United Kingdom was reported to be slightly over two million people the same year and between 1997 and 2001 the number increased in average with 13 percent per year (Harris, 2003). Moreover, according to Global Workplace Analytics, over five million people in the United States of America work a majority of its working hours through teleworking (Evangelakos, 2020). This is a 173 percent growth over the last 15 years (Evangelakos, 2020). According to Babulak (2009) 50 percent of US workers teleworked two out of five working days from home in 2009. Because of the long distances between american cities as well as the integration with european companies, teleworking is turning out to be a new norm (Babulak, 2009). Unlike the negative view on teleworking in the 1970s and 1980s (Qvortrup, 1998), Babulak (2009) argues for teleworking being high-qualified work with more sophisticated types of work, with higher payments in the 2000s.

With the Covid-19 pandemic that started in 2020, teleworking has grown significantly (Evangelakos, 2020). A survey from Gartner, Inc. states that 88 percent of world-wide businesses mandated or encouraged their employees to telework when the pandemic started (Gartner, 2020). The same report shows that almost 50 percent of employees in organizations will continue to telework even after Covid-19 and before the pandemic the number was 30 percent (Gartner, 2020). Microsoft has presented numbers showing the enormous growth of use regarding Microsoft Teams (Evangelakos, 2020). Since the start of the pandemic, the number of conferences, calls and meetings done through Microsoft Teams have grown 500 percent (Evangelakos, 2020). Moreover, Zoom, another video conferencing software tool, attracted more users the first six weeks of 2020 than they did during the twelve months of 2019 (Evangelakos, 2020).

2.1.2 Effects of Teleworking

Instead of having to travel to clients, manufacturers or colleagues, teleworking has enabled one to communicate and work together remotely (Qvortrup, 1998). Babulak (2009) mentions six principal advantages with teleworking: energy savings, cost savings for employees, protection of environment, facilitation of job mobility, companies reduced fees on overheads and properties and finally increase of productivity. These advantages come mainly from the development of technologies (Qvortrup, 1998). Technology makes it possible to communicate with almost all parts of the world at any time (Babulak, 2009). Examples of developments that have changed the way of working are: phones, communication tools and computers, but also robotics (Babulak, 2009). In 2002, the internet population surpassed 500 million users and in 2007 the first iPhone was released (Binchus, 2021). According to Babulak (2009) humans understand each other much better when looking at another person while speaking, than only hearing a voice. Face to face contact, eye contact and body language plays a big role in communication, with a bigger impact on the understanding than the actual words (Babulak, 2009).

Communication technologies have, in comparison to phone calls, changed the interaction while communicating (Babulak, 2009). One of the first technological communication tools that entered and revolutionized the way of communicating was Skype that was founded in 2003 with a goal of bringing people closer together when they are apart (Skype, 2012). Since then, multiple technological tools for communication have appeared and still the market is evolving (Binchus, 2021). In 2011, Zoom Video Conferencing was founded, a tool that has strived for continued development and has led its communication improvements through innovation (Binchus, 2021). Microsoft launched the first version of the video conferencing tool Microsoft Teams in 2017 when it was named Microsoft Classroom and in 2018 it was upgraded and available for everyone as Microsoft Teams (Protalinski, 2018). The same year as the first version of Microsoft Teams was released, 2017, Google Meet made its communication tool Google Hangouts Meet available for everyone (Johnston, 2017). According to Kristen Herhold (2020) most employees in the United States of America that are forced to telework due to Covid-19 use Zoom, Microsoft Teams, Skype, Google Meet or Slack to communicate. The top three most used services, according to Clutch's survey, are Zoom with 36 percent, Microsoft Teams with 19 percent and Skype with 17 percent (Herhold, 2020). Zoom Video Conferencing reached 300 million daily participants in online meetings in 2020 (Binchus, 2021).

Loneliness, irritation, worry and guilt are four mental health conditions that are effects of teleworking (Mann & Holdsworth, 2003). Even though the use of telework leads to new working patterns within an organization that can lead to reduced cost, the trade-off of risking one's mental health exists (Mann & Holdsworth, 2003). Teleworking was thought to have a positive impact on the quality of life for employees, since they got to spend more time with their family, but the findings of Mann and Holdsworth (2003) show that a paradox exists in this area. While the popularity of teleworking is growing it is also found that office workers are affected negatively when more people are working remotely (Golden, 2007).

According to Baruch (2002) teleworking has five effects on individuals, the first one claims that teleworking can have a negative effect on career aspirations, but that it does not change the conception of oneself if it is balanced with work. Furthermore, there are effects on time management when teleworking, meetings can be back to back without necessary breaks in

between and there is a reduction of distraction when working from home (Baruch, 2002). There are no indications of changes in, for instance, priorities when teleworking (Baruch, 2002). Baruch (2002) does however claim that a major satisfaction and less stress can be achieved through teleworking, which is against the thoughts of Mann and Holdsworth (2003). People's characteristics are of great importance when teleworking, and self-discipline is one of the most important ones (Baruch, 2002). Certain people are not meant to telework according to Brauch (2002), but the same research also shows that at an organizational level the performance on quality and quantity increased when doing so.

There are multiple definitions stated for teleworking. One could say there are three categories of teleworking, home-based teleworking, mobile teleworking and telecenters (Yang et. al, 2013). Home-based teleworking describes work that is being done through teleworking from a home whilst mobile teleworking describes work that is being done on movement (Yang et. al, 2013). Telecenters is work being done in a combination between home and a traditional office (Yang et. al, 2013). The two definitions we have chosen to focus on for this research is: *"Teleworking, also known as telecommuting, involves working away from the traditional office using computers and telecommunication facilities to maintain a link to the office"* (Bélanger & Allport, 2008, p. 102) and secondly, *"Work that is carried out at a distance from the core organization through the medium of ICTs"* (Greenhill & Wilson, 2006, p. 381).

2.1.3 Forced Teleworking

Forced is defined by the Cambridge Dictionary as *"an action that is forced is done because it is suddenly made necessary by a new and usually unexpected situation"* (Cambridge Dictionary, n.d). Covid-19 was a new and unexpected situation that organizations and societies worldwide were not prepared for, and necessary actions were taken to ensure the possibility to keep on working (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020). Teleworking was one of these actions that were taken by organizations to ensure the possibility to work in relation to employees health (Belzunegui-Eraso & Erro-Garcés, 2020). Therefore, teleworking could be seen as a forced action due to Covid-19 (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020). With Covid-19 there has been a push for organizations and employees to telework world wide (Evangelakos, 2020). Regulations and recommendations in different countries of the world have affected the situation of where people work from, for instance were all active organizations in Sweden forced to telework to some extent due to the recommendations from the government (Krisinformation, 2021). In other parts of the world the regulations have forced employees of organizations to telework whilst others have had the possibility to mix teleworking with office work (Belzunegui-Eraso & Erro-Garcés, 2020). During the last couple of years a growing number of employees telework and the scale up has continued to grow with the development of technology (Evangelakos, 2020). What has been found in literature is the scale up of teleworking due to Covid-19 (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020). Due to the changes with a scaled up teleworking, many organizations will continue to let their employees telework even after the pandemic, meaning the scale up will continue to grow and be present in normal times (Belzunegui-Eraso & Erro-Garcés, 2020). The forced teleworking situation that has occured due to Covid-19 is a rare situation that does not happen often. However, it does affect the ways of working due to regulations and recommendations and the ways of handling cyber security due to the changes in how to work (Evangelakos, 2020). Teleworking will continue to be present even after the pandemic, meaning the forced situation affects the future (Gartner, 2020).

2.2 Cyber Security

In this paper we will be focusing on the effect that cyber security threats and risks have on organizations. Cyber security within organizations attempts to ensure security and protect the cyber environment within an organization (von Solms & van Niekerk, 2013; Craigen, Diakun-Thibault & Purse, 2014). The cyber environment consists of connected computing- and mobile devices, electronic systems, services, networks, applications and infrastructure (von Solms & van Niekerk, 2013; Craigen, Diakun-Thibault & Purse, 2014). With cyber security you are striving to protect the cyber environment from malicious attacks that can harm the company or its ICS and these attacks are therefore seen as threats for organizations (von Solms & van Niekerk, 2013). One of the characteristics of the definition for cyber security is, what needs to be protected is due to the fact that usage of ICT, as a foundation of the cyberspace, creates vulnerabilities related to it (von Solms & van Niekerk, 2013).

Some studies are connecting cyber security with information security and although both phenomenons are dealing with security and have similarities, von Solmos and van Niekerk (2013) are claiming that the phenomenons are different (see Figure 2.2). Information security are mainly focusing on protection of the actual information, which can be information stored or communicated outside the cyberspace, while cyber security are focusing on protection of the cyberspace and on protection of those that are functioning in it (von Solms & van Niekerk, 2013, von Solms & von Solms, 2018).

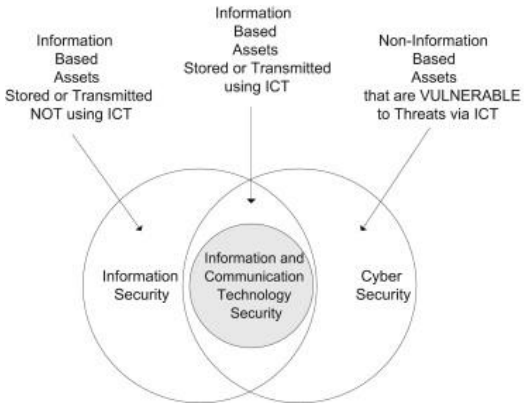


Figure 2.2: The relationship between information and communication security, information security, and cyber security. Adopted from von Solms & van Niekerk (2013).

2.2.1 Social Engineering

Social engineering is malware attacks that focus on the weakest security link in organizations - the employees (Abraham & Chengalur-Smith, 2010). Social engineering is the easiest method for hackers to reach organizational data as there are multiple ways of affecting, reaching and manipulating humans to do as they want (Breda, Barbosa & Morais, 2017). As organizations are increasingly focusing on IT-security to protect their data, devices and networks, the easiest way in is through humans with access to this (Abraham & Chengalur-Smith, 2010). Social engineers perform actions and develop malware that manipulate humans, making them perform actions that breaches the organization's security protocols without the humans knowing about it (Breda, Barbosa & Morais, 2017). In this point of view, social

engineers exploit innocent instincts from humans, not being criminal through threats or such, which makes it difficult to catch social engineers (Breda, Barbosa & Morais, 2017).

Phishing
Phishing attacks are fraudulent communications that are sent to users from what is believed to be a reputable source (Cisco, n.d-2). The fraud is often sent through email with a goal of stealing sensitive data or information (Cisco, n.d-2). The emails are often sent to lure the receiver and fool him or her into pressing a link or answering the email with the asked information (Cisco, n.d-2).

2.2.2 Malicious Attacks

Malware is a term combinated between the words, *"malicious"* and *"software"* to describe a software or code that criminals, often called hackers, use to infect and infiltrate computers, networks and data (Cisco, n.d-1). Malware attacks are used by hackers to steal data, trick a victim into giving away data, infect computers or taking control over computers and networks (McAfee, n.d). Malware attacks are delivered and spread through various internet channels (Abraham & Chengalur-Smith, 2010). There are multiple types of Malware used by hackers; viruses, ransomware, scareware, worms, spyware, trojans, adware and fileless malware (Cisco, n.d-1; McAfee, n.d).

Viruses
Viruses are malicious software that are attached to files or documents, often attached in emails, supported by macros that spread the malware from host to host once the virus is opened (Cisco, n.d-1; McAfee, n.d). Viruses disrupt a system and affect its operations (McAfee, n.d).

Ransomware
Ransomware is one of the most used malware, it installs itself on a machine and encrypts the files on the machine until the owner pays to get the data back (McAfee, n.d). Attackers can with ransomware get access to sensitive data and control when the owner gets it back, the payment is often done through Bitcoin and when the requested payment is received, the data is unlocked from its encryption (Cisco, n.d-1).

Scareware
Scareware are message alerts that hackers use to threaten and scare users with warnings like: *"Your computer is infected with a virus, follow this link to fix the problem!"* to advertise and psychologically get the user to purchase applications (McAfee, n.d; Cisco, n.d-1).

Worms
A worm is a malicious software that rapidly spreads and replicates to multiple devices within a network when it is downloaded (Cisco, n.d-1). The worm copies itself to have the ability to spread the malware to multiple devices within the network (McAfee, n.d), the effect is similar to viruses, it affects systems and disrupts its operations (Cisco, n.d-1).

Spyware
Spyware is a program that runs on a device without the user knowing it (Cisco, n.d-1; McAfee, n.d). This malware runs discreetly on a computer to report data to a remote user that

can steal the data and information, often being financial or personal information (Cisco, n.d-1).

Trojans
Trojans are applications that are advertised as harmless, helpful software programs, but whilst downloaded, trojans can steal information and data, delete it, crash devices or view activities within the device (Cisco, n.d-1; McAfee, n.d).

Adware
Adware collects data from a device and then uses the data to provide advertisements and pop-up windows on your screen when doing an action, these types of malware are most of the time not dangerous for the computer but annoying for the user (Cisco, n.d-1; McAfee, n.d).

Fileless malware
Fileless malware is a memory-resident malware that does not leave any tracks or evidence from its activity within a device, instead it uses programs to infect a device through a computer's memory (McAfee, n.d; Cisco, n.d-1).

Malware attacks are crimes being done through computers to harm individuals and organizations (Abukari & Bankas, 2020). According to a report from McAfee in 2014, malware attacks annually cost 445 billion dollars in damages for organizations and individuals globally (Abukari & Bankas, 2020). Steve Morgan (2020) on the other hand argues that cyber crimes cost 3 trillion US dollars in damages for organizations and individuals world-wide in 2015. The same author says that cyber crimes will cost 6 trillion US dollars in damages in 2021 and reach 10 trillion US dollars in 2025 (Morgan, 2020). These numbers differ much but all declare the huge negative impacts cyber crimes have on both individuals and organizations world-wide when it comes to economical effects. Moreover, according to Abraham and Chengalur-Smith (2010) malware attacks continue to grow with time, with an increased number of attacks and an increase in damage costs. With a growing number of teleworkers, the number of malware attacks have grown as well (Evangelakos, 2020), according to Firch (2021) cyber attacks have grown 600 percent since the start of the Covid-19 pandemic. According to Abukari and Bankas (2020) telework technologies need better protection than on premise infrastructure as there are a higher number of external threats for teleworking. Most malware attacks are based on social engineering, which is an increasing attack vector for malware attacks (Abraham & Chengalur-Smith, 2010).

2.3 Cyber Security Practices in Organizations

2.3.1 Security Standards and Frameworks

ISO27001
When investigating different security standards for information security, it can be stated that the big five are the most common practices, which are ISO27001, ITIL, COBIT, BS799 and PCIDSS (Susanto, Alumnawar & Tuan, 2011). ISO27001 is an international information security for management standard that provides guidance and risk management approaches, and the certification of this standard has high recognition around the world (Brenner, 2007). This standard specifies requirements for establishing, implementing, operating, reviewing,

monitoring and improving a documented information security management system for organizations (Susanto et al., 2011). The standard is said to be applicable for all organizations, private and public, and it follows an iterative process of plan-do-check-act (see Figure 2.3) (Susanto et al., 2011). The scope and coverage of an information security management system should be defined for planning and implementation, but also risks should be identified and assessed and control objectives should be defined for information security (Disterer, 2013).

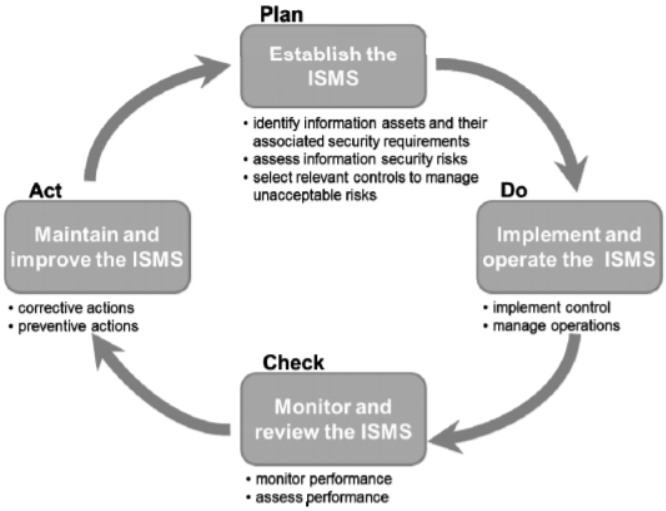


Figure 2.3: PDCA cycle. Adopted from Disterer (2013, p.95).

ITIL

ITIL (Information Technology Infrastructure Library) is one of the most accepted approaches to IT service management in the world, with an iterative multidimensional lifecycle structure (Sahibudin, Sharifi & Ayat, 2008). ITIL is a framework of best practices that encourages quality of computer services, and which was founded by the british government (Sheikhpour & Modiri, 2012). The security management of ITIL helps organizations to assess their risks and put procedures in place to log and respond to incidents (Sheikhpour & Modiri, 2012). The version 3 of ITIL has put information security management under Service Design in the ITIL framework, and the aim of that process is to align IT security with business security while ensuring that the information security is effectively managed in service management activities and all other services (Sheikhpour & Modiri, 2012). The security procedures of a company constantly change and need to stay up to date, and to ensure the quality of information security, the ITIL framework for information security management consists of five elements; control, plan, implement, evaluate and maintain (Sheikhpour & Modiri, 2012). It has been argued that the ITIL version 3 framework and ISO 27001 are very complementary to each other (Sheikhpour & Modiri, 2012).

BS 7799

BS 7799 was originally published by the British Standards Institution Group, and has evolved over the years (Susanto et al., 2011). It was originally designed to assure confidentiality, integrity and availability of data, which is achieved through security controls; this standard is however dependent on continuous monitoring and improvement (Kenning, 2001). Some key areas mentioned from this standard for implementation of information security management systems (ISMS) are information security policies, allocation of information security responsibilities and communication and operational systems security (Kenning, 2001). The first

version contained best practices for ISMS, and the later part focused more on how to implement ISMS, which later became ISO27001 (Susanto et al., 2011).

PCIDSS

The PCIDSS stands for Payment Card Industry Data Security Standard and was created in order to help industry organizations to process card payment and prevent fraud by increasing controls around data and its exposure to compromise (Susanto et al., 2011). PCIDSS provides a general set of requirements, in order for organizations to have the flexibility of implementing and customizing industry specific security measures to improve payment account data security (Gikas, 2010). The practical implementation approach of PCIDSS allows for clear guidelines and questionnaires, and the requirements that are included are for security management, policies, procedures, network architecture, software design and other protective actions (Gikas, 2010). This standard mainly applies to organizations that process or handle cardholder information and compliance is suggested to be assessed annually (Susanto et al., 2011).

COBIT

The last standard is COBIT, abbreviated for Control Objectives for Information and related Technology, which is a certification created by ISACA and the IT Governance Institute (Susanto et al., 2011). This IT governance framework and toolset allows managers to assess the gap between control requirements, technical issues, business - and security risks (Susanto et al., 2011). The five areas that COBIT concentrates on are strategic alignment, value delivery, resource management, risk management and performance measurement (Susanto et al., 2011). Eleven essential areas of control, called the 11EC, have been identified which are requirements and compliance of information security criteria for ISMS that should be implemented (Susanto et al., 2011). These standards and frameworks overlap in some areas of control from the 11EC (see Figure 2.4). The boxes that are dotted represent the standards and frameworks that do not use the areas of control, whereas the boxes that are checked use the presented areas of control.

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	*Information Security Policy*	√	√	√	√	√
2.	*Communications and Operations Management*	√	√	√	●	√
3.	*Access Control*	√	√	√	√	√
4.	*Information Systems Acquisition, Development and Maintenance*	√	√	√	●	√
5.	*Organization of Information Security*	√	√	√	√	√
6.	*Asset Management*	√	√	√	√	√
7.	*Information Security Incident Management*	√	●	√	√	√
8.	*Business Continuity Management*	√	√	√	√	√
9.	*Human Resources Security*	√	√	√	●	√
10.	*Physical and Environmental Security*	√	√	√	●	√
11.	*Compliance*	√	√	√	√	√

Figure 2.4: Features of the Big Five of ISMS standards. Adopted from Susanto et al. (2011, p.26).

2.3.2 Cyber Security Practices

Firewall

One of the oldest security practices for organizations that are connected to the internet are the use of some sort of firewall (Ingham & Forrest, 2002). This means that organizations have some level of protection from the outside (Ingham & Forrest, 2002). Even though properly managed and implemented firewalls ensure proper protection, it is not always enough (Broderick, 2005). Firewalls can be seen as the first level of defence, to prevent intrusions in organizations systems, but sophisticated attacks from hackers makes it difficult for firewalls to ensure full protection (Broderick, 2005). Firewalls work as a safetynet when data arrives from insecure communication channels, which however is used or generated by applications that lay out little effort on validating if the information being sent or received is valid (Broderick, 2005).

Document Cyber Security Policies
Even though the development of cyber security protocols seems vital in order to protect information within a company, it has been said that for some companies this prioritises last (McIntyre, 2018). This can be due to the fact that new evolving technologies come along and busy daily work (McIntyre, 2018). Fundamentally can cyber security policies and protocols be defined as the approach that achieves preparedness, protection, resilience and stability (McIntyre, 2018). They also include processes for critical assets, including how humans interact with systems (McIntyre, 2018).

Plan for Mobile Device
Mobile devices are becoming more and more popular within organizations, since it is believed it can create business value, efficiency for the employees and improve communication channels (Kearns, 2016). Some of the threats of using mobile devices include theft, infection and inattentive use of the devices, which can lead to data breaches that can be expensive for the organization in question (Kearns, 2016). Therefore, specific policies and controls of mobile devices are paramount, in order for organizations to stay safe (Kearns, 2016). When bringing your own device (BYOD), a number of security measures are recommended such as the use of Virtual Private Network (VPN), firewalls, email filtering, Network Access Control (NAC), Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Information Management (MIM) and desktop virtualization models (Downer & Bhattacharya, 2015).

Educate all Employees
Educating employees in best practices of cyber security is seen as the single most important security measure by many Chief Information Security Officers (CISO) (Reeves, Delfabro & Calic, 2021). However, too much training and education can damage the view on how important adequate security knowledge is needed within organizations (Reeves et al., 2021). In cases where employees are disengaged in cyber security, it is stated that one should determine whether it is the advice or the action that has made employees tired, and later determine if the disengagement is attitudinal, cognitive or both (Reeves et al., 2021). Moreover, to reduce information security incidents, it is advised to provide cyber security awareness training (He, Ash, Anwar, Li, Yuan, Xu & Tian, 2019). Furthermore it is stated that while a lot of employees might follow policies and guidelines correctly, they are seen as more general knowledge, which makes it important that employees build experience and learn how to act with various malware attacks through training and education (He et al., 2019).

Enforce safe password practice
There are a lot of benefits with strong password protocols, for instance, users never send their plaintext passwords to a website, but present a password verifier which is stronger than a hashed or salted password (Ruoti, Andersen & Seamons, 2016). Moreover, these protocols not only allow the user to authenticate to the website but also authenticate the website to the user (Ruoti et al., 2016). Finally, phisers learn nothing about the user password, do not require safe connection and are safe from force attacks by network hackers (Ruoti et al., 2016). However, safe password practice alone does not guarantee safety from sophisticated attacks (Ruoti et al., 2016).

Regularly back up data
Sensitive data on laptops or other devices run the risk of getting lost, stolen or corrupted and backing up the data are used to address these kinds of problems (Liu, Zhong, Chang, Xia, He

& Cheng, 2016). However, sometimes the backup servers cannot always be trusted, which can lead to solutions such as symmetric encryption or public key cryptography (Liu et al., 2016).

Install anti-malware software
Having anti-malware software is also vital in order to protect organizations intellectual property or safeguard them from financial losses (Rathore, Agarwal, Sahay & Sewak, 2018). Research shows that malware has been growing at an exponential rate over the past decade, which has led some organizations to use machine learning and deep learning methods to detect and analyze this malicious software (Rathore et al., 2018).

Use multi-factor authentication
With increased risks of different online environments, multi-factor authentication for identification has increased in popularity, since this method is based on two or more factors to identify a user (Kim & Hong, 2011).

Cyber security practices summary
To summarise, there are many different security practices for organizations, in order to protect critical assets and data. As firstly shown, firewalls are one of the oldest security measures, as well as a first line of defense to make sure data is protected (Ingham & Forrest, 2002; Broderick, 2005). Documentation of cyber security policies has a low priority according to McIntyre (2018), yet a crucial practice to achieve preparedness for organizations. Since BYOD is more common among organizations today, planning for the use of mobile devices through adequate security software and BYOD policies is of highest importance to make sure organizations' data are safe (Kearn, 2016; Downer & Bhattacharya, 2015). To educate employees to become more aware of security and threats can be seen as one of the most important security measures for organizations, it is however crucial to make the training engaging (Reeves et al., 2021; He et al., 2019). Even though safe passwords are highly important, it cannot be a guarantee alone of safety for organizations (Ruoti et al., 2016). Furthermore, backing up data is practice to solve problems if data gets corrupted (Liu et al., 2016), anti-malware software protects vital information and is paramount due to the growth of malware (Rathore et al., 2018), and lastly, the use of multi-factor identification decreases the risk when facing different online environments (Kim & Hong, 2018).

2.4 Security Practices Embedded in Teleworking

Evangelakos (2020) mentions six critical security considerations for organizations when teleworking. One challenge is having work laptops at home as they are less secure without DNS filters and good anti-virus systems, if the laptop is used for other things than only work, games for instance, the risk factor is increased (Evangelakos, 2020). Evangelakos (2020) describes the importance of changing VPN and firewall rules for having smooth communication between teleworking staff and office, this does however lead to more opportunities for hackers. These opportunities involve social engineering from employees' home wi-fi that allow hackers to bypass organizations security measures, which eventually can lead hackers to access corporate networks through the back door (Evangelakos, 2020). According to Abukari and Bankas (2020) teleworking organizations commonly use VPNs to remotely access organizational files and servers. VPNs are tunnels that are built for teleworkers, turning public internets into private networks, with encrypted data that protect the connection (Abukari &

Bankas, 2020). Rikitake et al. (2001) argues that VPNs work very well to protect the links between teleworkers and organizational systems. Moreover, other protective measures mentioned are firewalls and BNS filtering for organizations to protect against risks as it secures the internal data while teleworking (Evangelakos, 2020; Yang et al., 2013). Organizational data stored on the cloud must also be handled carefully, it is important to trust the cloud provider and identify misconfigurations that can have the chance to open the data for unintended people (Evangelakos, 2020). Abukari and Bankas (2020) mention desktop sharing as a remote access method when teleworking. Organizations can through desktop sharing give remote access to users to share files and presentations which results in security- and authentication risks if one employee's authentication credentials are hacked (Abukari & Bankas, 2020). The unauthorized user can in this case get access and attend digital meetings, seminars and webinars without anyone knowing it is not the mentioned credential (Abukari & Bankas, 2020).

Some companies have used on-line auditors to conduct work through teleworking (Natase & Ionescu, 2011). A main challenge has been to create a framework of accessing audited entity’s data under maximum security protection conditions of information security and integrity (Nastase & Ionescu, 2011). Audit managers that telework need to set procedures for technical support that meet team members' needs in case of network downtime, software malfunction and incorrect configurations (Nastase & Ionescu, 2011). Research has found that additional security measures needed to be taken to ensure vital information security attributes, such as confidentiality, integrity and availability (Nastase & Ionescu, 2011). Some security measures mentioned were the use of firewalls, anti-virus software, encryption software, one time password etcetera. (Nastase & Ionescu, 2011). However, it was identified that a computer security incident response team should be established in order to respond quickly to security matters (Nastase & Ionescu, 2011). However, Evangelakos (2020) argues that having a security team that follows and tracks every moment and change in a company’s data and network is expensive. Security risks for disclosure, destruction and modification of data can be assessed and solved by practices found in research, such as establishing formal policies of how to telework, develop training for employees and making sure that networks and devices can be secured and information is encrypted (Yang et al., 2013).

There are multiple possible solutions for the mentioned risks and vulnerabilities resulted by teleworking. Research suggests BAS (Breach and Attack Simulation) platforms that can help eliminate and reduce vulnerabilities through simulations and automations, by testing continuously every hour of the day (Evangelakos, 2020). Even though BAS platforms can help reduce the size, spread and time of malware attacks, other actions and services are required for an organization (Evangelakos, 2020). For safe email communication between different servers and end-to-end users, a method called PGP (Pretty Good Privacy) is suitable (Rikitake et al., 2001). PGPs are effective as it only requires end-to-end users to exchange public keys (Rikitake et al., 2001). Furthermore, research mentions SSL, Security Sockets Layer and SSH, Secure Shell, as secure communication tools for teleworking as they crypt and secure communications between devices (Rikitake et al., 2001).

Abukari and Bankas (2020) propose the use of different protocols for handling the security risks associated with forced teleworking. On an organizational level, a training protocol is proposed to spread the awareness of malware attacks throughout the organization as well as define a common way of how to telework in a safe manner (Abukari & Bankas, 2020). This is necessary as teleworkers are being more of a target for malware attacks than before and hackers know about the organizational weaknesses (Evangelakos, 2020). On an individual level,

Abukari and Bankas (2020) suggest an education protocol for individuals to get training in the use of internet and internet ethicals. This training will ensure less threats from employees pressing fake links, fake emails and overall phishing attacks from hackers (Abukar & Bankas, 2020). Lastly, Abukar and Bankas (2020) suggest a policy protocol for organizations working with teleworking as this policy can streamline the handling of organizational data, as well as internet behaviour.

2.5 Research Models

2.5.1 Main Aspects

In this section we present the aspects that build the research model. Since this study aims to investigate what security risks and threats related to forced teleworking bring to organizations, the literature review led us to identify aspects that can support the aim of the study. By looking closer on- and studying theoretical-driven aspects to better understand what makes teleworking possible but also vulnerable to security, the literature led to discover three main aspects, namely: the Social aspect (Bostrom and Heinen, 1977; Griffith and Dougherty, 2002); the Technical aspect (Gupta & Sharman, 2009; Griffith & Dougherty, 2002); and, the Risk Tolerance aspect (Liang & Xue, 2009; Carpenter, Young, Barrett & McLeod, 2019). The literature led to the reason that teleworking is affected primarily by the technical means offered at the workplace to the employees who are part of the society that in return affects the Social aspects of an organization. While the Technical and the Social aspects present complex organizational processes that affect security, it was recognized that the Risk Tolerance aspect is key to understanding how teleworking is made possible despite security issues. These three aspects were therefore of high importance and interest for this thesis. Following is an overview of each aspect to give further insight for the motivation.

The Social aspect
The Social aspect is described in various literature with different meanings. Bostrom and Heinen (1977) describes the aspect as social and psychological needs and capacities that the individuals within an organization hold. Moreover, individuals hold attitudes, skills and values that all affect an organization's outcome as individuals and their actions can result in both positive and negative effects (Griffith & Dougherty, 2002; Bostrom & Heinen, 1977). Griffith and Dougherty (2002) highlights that organizations are built around people and that people are the Social aspect. The Social aspect does also include how individuals work in groups and what psychological aspects that come as a result of the individuals and the group (Bostrom & Heinen, 1977). The relationships built between the individuals build a system that is affected by each individual (Griffith & Dougherty, 2002). According to Bostrom and Heinen (1977) the Social aspect investigates four areas: first, individual characteristics, needs and how they work in groups. Second, how organizational group work is characterized (Bostrom & Heinen, 1977). Third, how the external environment is for the group; and, lastly what support systems there are for the group (Bostrom & Heinen, 1977). This aspect is important to include in the research model in order to understand how individuals can influence and constitute security risks for an organization (Griffith & Dougherty, 2002). Changes due to forced teleworking can affect groups, organizational results as well as the security risks for an organization. The Social aspect for organizations, which involves individuals' well-being and stress (Bostrom &

Heinen, 1977), can be affected by changes where employees need to telework instead of work from a physical office. Of great importance to mention is that the definition of the Social aspect is used as an aspect in the Socio-technical Systems Theory (STS) where they combine the Social aspect with a technical aspect in order to achieve a better understanding of how technology affects an organization.

The Technical aspect

The Technical aspect is described by Gupta and Sharman (2009) as the technical conditions within an organization. Griffith and Dougherty (2002) argue that the Technical aspect centers around tools, techniques and knowledge to produce goods or services together with the Social aspect earlier mentioned. Technical mechanisms can be a new software program or new technical device for example (Bostrom & Heinen, 1977). As organizations use many technical tools, programs and services to enable teleworking, this aspect is of big importance for the research. This is important as this thesis believes a clear understanding of the teleworking tools is needed, in order to analyse the security risks related to them. The view of the Technical aspect is shared with the Socio-technical Systems Theory (STS) view of the aspect (Griffith & Dougherty, 2002). The aim of combining these two aspects is to understand and achieve a sustainable collaboration between the human systems and the technological systems in an organization (Griffith & Dougherty, 2002). The Social aspect is designed in relation to the Technical aspect and together they define how well an organization performs (Griffith & Dougherty, 2002). Moreover, these two aspects are the main areas for making teleworking possible as people, being the Social aspect, are using the technical tools, being the technical aspect, to work. This is found to be a great reason to include these aspects in the framework in order to see the connection between the teleworking tools and the organization itself. With this view one can analyze and understand the relation in between as well as understand where the cyber security threat comes from, if it is the Technical aspect or the Social aspect, or both.

The Risk Tolerance aspect

The last aspect, Risk Tolerance is particularly important in teleworking and is defined by Liang and Xue (2009) as the maximum level of uncertainty an user is willing to take, meaning a more risk tolerant user would be able to endure more IT threats than a less risk tolerant user. This can affect the perception of threat negatively, since a more risk tolerant user perceives a lower degree of threat (Liang & Xue, 2009). Risk Tolerance is a part of the Technology Threat Avoidance Theory (Liang & Xue, 2009), but the theory itself has been criticized by Carpenter et al. (2019) for not accounting for individual differences that can affect cyber security behaviour. These individual differences include risk propensity, distrust propensity and impulsivity (Carpenter et al., 2019). Nevertheless, while such differences are hard to recognize on a personal level, Risk Tolerance as an aspect is of value, since it gives a better understanding how the Social and the Technical aspects interaction is made possible in teleworking where Risk Tolerance is recognized. Moreover, the understanding of the sub-aspects of Risk Tolerance can show a richer picture of how Risk Tolerant a user is. An IT-user with a greater understanding of cyber security standards, frameworks, practices associated with an organization's security and in regards to forced teleworking might have a higher tolerance than those who do not. Furthermore, this aspect can also shed light on whether a high Risk Tolerance negatively influences IT-threats (Liang & Xue, 2009). Including this aspect in the research model can help to identify and determine risk from individuals that are a part of an organization or in charge of the security in an organization. The definition of the Risk Tolerance aspect is in line with Liang and Xue's (2009), but has the individual differences by Carpenter et al. (2019) in mind when investigating risk from the Technology Threat Avoidance Theory.

From combining these three aspects it is believed that a connection can be found between the teleworking tools and the organization itself, involving individuals, at the same time as security risks can be identified this collaboration constitutes.

2.5.2 Sub-aspects

The three identified aspects for the model consist of; a Social aspect, a Technical aspect and a Risk Tolerance aspect. Moreover, every main aspect contains sub-aspects that assume the literature from 2.1, 2.2, 2.3 and 2.4. Some sub-aspects pertain to more than one main aspect but with different perspectives. Each sub-aspect has relevance for its main aspect and gives depths to the analysis. Below is a description of how each sub-aspect has connection to the main aspects.

The Social aspect consists of these sub-aspects:

Cyber security involves *Social Engineering* which is explained in 2.2. Social Engineering. Social engineering is malware attacks that focus on the weakest security link in organizations - the employees. The employees are individuals that are part of the Social aspect. Moreover, the Social aspect consists of Social Influence and Personal Factors which are the reason behind successful Social Engineering attacks. Therefore, the relation between cyber security threats and the Social aspect is identified.

Security practices in organizations involve *Cyber security practices* which is explained in 2.3. Cyber security practices include education of all employees, meaning the individuals of an organization. Moreover, the cyber security practices also affect employees and the social parts of an organization and therefore the correlation between the Social aspect and security practices in organizations feel natural.

Teleworking involves *Timeline of teleworking* and *Effects of teleworking* which is explained in 2.1. Throughout the history of teleworking, described in the timeline, an increased number of individuals have started to telework. Nowadays, teleworking affects almost every person within an organization. The effects of teleworking on employees and Social aspects of organizations are many, both regarding individuals' physical work status and individuals psychological status. These effects are further explained in 2.1 as mentioned but do all have clear connections to the individuals within organizations. The Social aspect centers around individuals and as teleworking has effects on individuals, the connection between them is identified.

The Technical aspect consists of these sub-aspects:

Cyber security involves *Malware attacks* which is explained in 2.2 and have a clear relation to the Technical aspect as hackers use the technical conditions and tools that are used within an organization, especially as employees telework, to commit malware attacks. Without technology there would not be any malware attacks and therefore we identify the connection between the Technical aspect and cyber security threats.

Security practices in organizations involve *Security standards and frameworks* and *Cyber security practices* which is explained in 2.3. These are all based on the Technical conditions that an organization has to handle, as all security- practices and frameworks used by organizations

are developed for computers and other technical devices. Therefore the relation between the Technical aspect and security practices in organizations is identified.

Security practices embedded in teleworking which is explained in 2.4 is a sub-aspect of the Technical aspect as these security practices describe how organizations work with technological tools and software to handle its teleworking challenges. As the main focus for the security practices circles around technology, the relation to the Technical aspect is identified.

The Risk Tolerance aspect consists of these sub-aspects:

Teleworking involves *Effects of teleworking* which is explained in 2.1. With teleworking, an increased security risk arises for organizations as their network- and device security is emasculated when employees work away from the offices. Organizations do therefore have to consider Risk Tolerance and risk readiness for the organization and its employees, which describes the relation between the Risk Tolerance aspect and teleworking.

Security practices in organizations involve *Standards and frameworks* and *Cyber security practices* which is explained in 2.3. These security practices are considered and involved in organizations as an answer to the risks associated with cyber security threats. That is why there is an obvious connection between the Risk Tolerance aspect and security practices in organizations, since depending on knowledge about these practices and frameworks one might perceive IT-threats differently.

Security practices embedded in teleworking which is explained in 2.4 are effects and actions made by organizations as answers to risks associated with teleworking and cyber security threats. Risks that occur due to teleworking are handled by organizations with the help of these practices which can explain the relation between the Risk Tolerance aspect and security practices embedded in teleworking.

2.5.3 Organizing the Aspects and the Sub-aspects into a Thematic View

The thematic overview demonstrated in Table 2.1 below displays the main aspects in relation to its sub-aspects from the *Theoretical Background*. Table 2.1 includes three columns, the first one with three main aspects; Technical, Social and Risk Tolerance. The second column includes the sub-aspects for each main aspect followed by the last column with references for each main aspect area. Table 2.1 is intended to work as a guide for the reader to understand the process throughout the research. Moreover, the structure from the *Thematic Overview* will guide and structure the authors when building the interview guide.

Table 2.1: Research Model

Main Aspect	Sub-aspects	References
Social Bostrom and Heinen, 1977;	**Cyber security** • **Social Engineering**	Abraham & Chengalur-Smith, 2010; Breda, Barbosa & Morais, 2017; von Solms & van Niekerk, 2013; von Solms & von Solms, 2018; Craigen, Diakun-Thibault & Purse, 2014.

Griffith and Dougherty, 2002.	**Security Practices in Organizations** • **Cyber security practices**	Ingham & Forrest, 2002; Broderick, 2005; McIntyre, 2018; Kearns, 2016; Downer & Bhattacharya, 2015; Reeves et al., 2021; He et al., 2019; Ruoti et al., 2016; Liu et al., 2016; Rathore et al, 2018; Kim & Hong, 2011.
	Teleworking • **Timeline of Teleworking** • **Effects of Teleworking** • **Forced Teleworking**	Qvortrup, 1998; Babulak, 2009; Belzunegui-Eraso & Erro-Garcés, 2020; Harris, 2003; Kowalski & Swanson, 2005; Evangelakos, 2020; Gartner, 2020; Binchus, 2021; Skype, 2012; Protalinski, 2018; Johnston, 2017; Herhold, 2020; Mann & Holdsworth, 2003; Golden, 2007; Baruch, 2002; Yang et al., 2013; Bélanger & Allport, 2008; Greenhill & Wilson, 2006. Cambridge Dictionary, n.d, Krisinformation, 2021.
Technical Gupta & Sharman, 2009; Griffith & Dougherty, 2002.	**Cyber security** • **Malware Attacks**	Cisco, n.d; McAfee, n.d; Abraham & Chengalur-Smith, 2010; Abukari & Bankas, 2020; Morgan, 2020; Evangelakos, 2020; Firch, 2021; von Solms & van Niekerk, 2013; von Solms & von Solms, 2018; Craigen, Diakun-Thibault & Purse, 2014.
	Security practices in organizations • **Standards and frameworks** • **Cyber security practices**	Ingham & Forrest, 2002; Broderick, 2005; McIntyre, 2018; Kearns, 2016; Downer & Bhattacharya, 2015; Reeves et al., 2021; He et al., 2019; Ruoti et al., 2016; Liu et al., 2016; Rathore et al., 2018; Kim & Hong, 201;.Susanto et al., 2011; Brenner, 2007; Disterer, 2013; Sahibudin et al., 2008; Sheikhpour & Modiri, 2012; Kenning, 2001; Gikas, 2010.
	Security Practices Embedded in Teleworking	Yang et al., 2013; Nastase & Ionescu, 2011; Rikitake et al., 2001; Evangelakos, 2020; Abukari & Bankas, 2020.
Risk Tolerance Carpenter et al., 2019; Liang and Xue, 2009.	**Teleworking** • **Effects of teleworking**	Qvortrup, 1998; Babulak, 2009; Belzunegui-Eraso & Erro-Garcés, 2020; Harris, 2003; Kowalski & Swanson, 2005; Evangelakos, 2020; Gartner, 2020; Binchus, 2021; Skype, 2012; Protalinski, 2018; Johnston, 2017; Herhold, 2020; Mann & Holdsworth, 2003; Golden, 2007; Baruch, 2002; Yang et al., 2013; Bélanger & Allport, 2008; Greenhill & Wilson, 2006.
	Security Practices in Organizations • **Standards and frameworks** • **Cyber security practices**	Ingham & Forrest, 2002; Broderick, 2005; McIntyre, 2018; Kearns, 2016; Downer & Bhattacharya, 2015; Reeves et al., 2021; He et al., 2019; Ruoti et al., 2016; Liu et al., 2016; Rathore et al., 2018; Kim & Hong, 201;.Susanto et al., 2011; Brenner, 2007; Disterer, 2013; Sahibudin et al., 2008; Sheikhpour & Modiri, 2012; Kenning, 2001; Gikas, 2010.

	Security Practices Embedded in Tele-working	Yang et al., 2013; Nastase & Ionescu, 2011; Rikitake et al., 2001; Evangelakos, 2020; Abukari & Bankas, 2020.

3 Research Methodology

This chapter presents the methodology that was used in the research. It gives the reader an insight in how the research was designed and creates understanding for the thoughts and made choices. It presents the research philosophy for the study and the approach that will be used. The chosen data collection methods and analysis method are brought forward and the chapter ends with presenting the ethical considerations and scientific quality used in the research.

3.1 Research Philosophy

In order to answer the research question it was important to understand the subjective meanings of the answers, which is seen as essential in the interpretive paradigm (Goldkuhl, 2012). The use of a qualitative research method with a naturalistic approach enables the researcher to understand human experiences in a holistic and inductive way (Patton, 2015). For the researchers of this thesis, the importance of understanding the respondents' perspectives and experiences are of priority when investigating cyber security risks and threats for organizations. However Patton (2015) argues that qualitative inquiry is also highly personal to the researcher and that the researcher can be seen as the main instrument of this. The background, experience, interest and everything one has encountered in life can be seen as the building blocks for the credibility of this study (Patton, 2015). Furthermore, the core idea of using interpretivism as the research philosophy for this thesis can be explained by the definition of Goldkuhl (2012), where the emphasis lies on the already known subjective meaning in the social world. To acknowledge their existence, reconstruct them, understand them and avoid distorting them will be the pillars for theorizing (Goldkuhl, 2012). It is believed that all individuals have their own perception of the phenomena that were investigated, which is why the everyday experience is crucial for the research, and it would also provide useful insights and knowledge.

The methods of natural science can be seen as inadequate to the study of social reality by researchers that are advocates of an interpretive approach (Lee, 1991). The social and physical objects that interpretive researchers use are seen as different from how researchers of natural science view reality (Lee, 1991). Natural science follows a more positivist approach, which can be seen as the opposite school of thought from interpretivism, where the thought is that knowledge is created from experience of natural phenomena (Lee, 1991). Nevertheless, it is clear that interpretivism fits this thesis, since the social - and physical objects of an interpretive approach provides a clearer understanding of the social phenomena. There are two research paradigms in qualitative research in the Information System field, which are interpretivism and pragmatism (Goldkuhl, 2012). Paradigms explain an individual's point of view of the world through their own perception of what they think is important, reasonable and legitimate (Patton, 2015). It is found that stating which paradigm a study chooses and not chooses increases the trustworthiness and importance of the research (Patton, 2015). While the pragmatism paradigm has an emphasis on constructive knowledge which is suitable for action, the interpretivist approach aims to understand data from qualitative research that is interesting to investigate (Goldkuhl, 2012).

Furthermore, research suggests that qualitative research is many times closely related to interpretivism (Goldkuhl, 2012). Patton (2015) describes the process of working with an interpretive approach as moving from collecting the data, to later presenting it, analyzing it and finally comparing it with the rest of the acquired data. For this thesis, it was considered that this process fitted well, since the goal was to compare the perceptions from the interviews regarding what cyber security threats and risks that were associated with forced teleworking. The social world of people is constructed of subjective understanding, shared meanings and knowledge (Goldkuhl, 2012), which the research was based on. It is therefore paramount that the analysis and the information gathered from the interviews provide meaning and relevance to this thesis. An interpretive approach is also recommended when the research subject is specific to a context (Bhattacherjee, 2012).

3.2 Research Approach

In order to answer the research question, a qualitative research method was chosen as the research approach. For this thesis, a qualitative research method fits well as the research question is dynamic, complex, and interdependent (Patton, 2015). By connecting and contrasting the collected information, an answer can be given to the research question (Patton, 2015). The qualitative research method enables us to collect detailed information and data from specific interviews with specific persons from specific organizations (Recker, 2013). Through a qualitative research method, we have the opportunity to investigate how organizations face and handle cyber security threats and risks connected to forced teleworking (Schulte & Avital, 2011). According to Schulte and Avital (2011) the importance of presenting rich details and descriptions from the data collection is of high importance. This is to ensure the credibility of the collected data (Schulte & Avital, 2011). Thick descriptions and an overall high quality of the research can defend the arguments presented and ensure that the data is understood in the right way (Schulte & Avital, 2011). However, there is a risk when doing qualitative research that the answers from the respondents are interpreted incorrectly, often affected by the researchers own values and beliefs (Burke Johnson & Onwuegbuzie, 2004; Recker, 2013). Yet, the ethics are of high priority for the researchers to ensure the reader that the data collection and the data analysis have developed in a proper manner (Burke Johnson & Onwuegbuzie, 2004; Recker, 2013).

Nonetheless, Schulte and Avital (2011) argue that researchers within the field of Information Systems that use a qualitative research method, as a data collection method, provide deficient information regarding how the interviews were done. Therefore, our interviews were based on a carefully chosen interview guide that presented detailed information about the interview. A qualitative research method requires time and resources as the interviews must be prepared, realized, processed and finally analyzed (Burke Johnson & Onwuegbuzie, 2004). Nonetheless, by having a clear structure, a reasonable number of interviews and a distinct method, the required time will not be a problem for this research.

3.3 Data Collections Methods

3.3.1 Literature Review

The theoretical background in chapter 2 necessitates to review various literature that will be used in this thesis. When conducting a literature review there are certain components one has to think of and involve, these are firstly grounds of conducting a literature review, then a research question that guides the research, a plan for data collection, and lastly a plan for analyzing and presenting the data (Randolph, 2009). Prior to compiling the theoretical background, the introduction section clearly outlined the background, research problem, research question and purpose of the research. In order to make sure that the quality of the theoretical background was well thought through, certain keywords were used. Furthermore, Randolph (2009) suggests documenting the keywords that were used in the research. Keywords are crucial for effective research, as it sets the base of the research (Timmins & McCabe, 2005). It is important to consider all the synonyms and similar words to the keywords as well (Timmins & McCabe, 2005). To make the search broader we used the terms AND and OR when using the keywords, in order to capture all relevant information. When looking for words that had similar, or the same meaning, the term OR was used. When trying to identify terms and concepts that are different from each other the term AND was used. According to Timmins & McCabe (2005) is the word AND used to make the search more specific and the word OR is used to broaden the search. This led to the following keywords:

- *"Evolution of Teleworking"* OR *"Timeline of Teleworking"* OR *"History of Teleworking"* AND *"Effects of Teleworking"* AND *"Teleworking Effects"*.
- *"Cyber Security"* AND *"Cyber Security and Information Security"* OR *"Differences between Cyber Security and Information Security".*
- *"Cyber Security Threats"* OR *"Malware Attacks"* OR *"Social Engineering".*
- *"Cyber Security Practices in Organizations"* OR *"Security Practices in Organizations"* AND *"Cyber Security Standards"* AND *"Cyber Security Frameworks"* OR *"Cyber Security Standards and Frameworks"* AND *"Security Standards and Frameworks" "Cyber Security Practices".*
- *"Security Practices Embedded in Teleworking"* OR *"Cyber Security practices Embedded in Teleworking"* AND *"Teleworking Security Practices".*
- *"Technology Threat Avoidance Theory"* OR *"Risk Tolerance"* OR *"TTAT".*
- *"Socio-Technical Systems Theory"* OR *"Social Aspect (STS)"* OR *"Technical Aspect (STS)".*

The search engines that were used for this theoretical background were mainly Google Scholar and LUBsearch. The information found in the theoretical background was gathered from academic journals, books, e-books, academic articles and conference papers. In order to clarify some terminology or phenomena, information that is not peer-reviewed has been used in some cases. It is stated in research that non-peer reviewed information shall not be overlooked, since they can provide informative and valuable information (Timmins & McCabe, 2005).

3.3.2 Qualitative Research Model

The method for data collection that was chosen for this master thesis was in the form of interviews. A research interview is a process of exchanging views on specific areas and topics, which are discussed between the interviewer and the respondent (Schulte & Avital, 2011). By conducting and analyzing interviews, documents, and observations, patterns and themes could be found from the data which could result in an interpretation on the research area- and question (Patton, 2015). After having collected data from well-chosen respondents with unique knowledge we had the potential to analyze the answers as the qualitative research method studies how people and groups build meaning (Recker, 2013; Patton, 2015).

In order to collect valuable data, the belief is to gather the subjective understanding of the respondents, since we will be able to better understand how organizations work with teleworking. By collecting data through a descriptive interview this can be achieved, since this kind of method can provide interviewers with rich descriptions of a phenomena, as well as how the respondents perceive this phenomenon (Recker, 2013). Due to the circumstances of a pandemic time the interviews were for this thesis conducted virtually, instead of face-to-face. While face-to-face interviews are believed to be superior, interviews over the phone can act as a stand-in alternative, since the information provided has been found to be more or less the same when doing interviews over the phone (Sturges & Hanrahan, 2004). With this in mind every digital interview was held with a video camera turned on to ensure some form of face-to-face interaction. Moreover, a PowerPoint presentation was shared and used during all interviews to support the respondent and ensure that there were no misunderstandings regarding definitions nor questions. The PowerPoint presentation supported the interview conversations as the questions and definitions were written in text to support the mutual question. The PowerPoint presentation was built based on the interview guide and can be seen in Appendix 7.

Even though interviews have some clear advantages, it is stated that some disadvantages to this method exist (Recker, 2013). Some of the disadvantages presented by Recker (2013) involve that the respondent could respond with what the interviewer would like to hear, or that the respondent gives poor recall to answers. Even with this in mind, the belief is that a qualitative study through interviews is the most appropriate way for this thesis, since the advantages outweigh the disadvantages. The main advantages of an interview are that it focuses directly on a selected topic and that interviews are seen as highly insightful (Recker, 2013). The structure that was chosen for the data collection was in the form of semi-structured interviews. Semi-structured interviews are one of the most common approaches when doing interviews (Recker, 2013). This allows authors to formulate questions in advance, both open and structured questions, as well as being able to ask follow-up questions during the interview (Recker, 2013). For every interview there was a clear structure within the thesis group to ensure efficiency and clarity for the respondent. One person within the group was responsible for the conversation, asking the questions and leading the conversation forward. Another person was responsible for taking notes and lastly the third person asked follow-up questions and supported the leader when needed. The benefits of a semi-structured interview approach is that they are less intrusive and nurtures a two-way communication (Recker, 2013). It also allows the interviewer to confirm what is already known and at the same time the semi-structured interview format provides the opportunity to learn something, since the respondent can give reasons behind the answer (Recker, 2013). It is believed that the PowerPoint presentation that was used also supported and confirmed the respondent so that they knew they answered the right question with the same definitions as the authors had. Lastly, semi-structured interviews

are beneficial since it is easier to discuss sensitive topics, because it is seen as more personal and conversational than structured interviews (Recker, 2013).

In order to use interviews as a successful tool, it is highly rewarding if the one conducting the interviews possesses great social skills (Walsham, 2006). This is something that the members of this thesis group feel like they do, which enabled them to provide rich answers from the interviews. It was decided to conduct the interviews in English, since the Masters thesis is written in English and the language for cyber security circles around the English language. However, for every interview, before starting the recording, the respondents were asked if they were as comfortable with English as Swedish to ensure the quality of the interview stayed at its full potential. If the respondent would have been more comfortable with speaking Swedish, we would have decided to do the interview in Swedish and afterwards translate the findings into English. This was decided since the quality of the collected data might have decreased if the interview would have been in a language that the respondent was not comfortable speaking in. This was however not the case, all the respondents felt as comfortable in English as in Swedish. Finally, all interviews were recorded with the consent of the respondent and transcribed afterwards.

3.3.3 Selection of Respondents

In Table 3.1 below details about the respondents can be found. In Table 3.2 below details about the interviews can be found. The process of choosing the right respondents started off early. The goal was to find a mix of organizations within different industries. Regarding the respondents within each organization it was of big importance that the person had knowledge about the chosen organization's cyber security, either if it was the cyber security officer, information security officer or in a smaller organization, the CEO. Moreover, as mentioned in the delimitations, the chosen organization has to have an active operation in Sweden, which all of the interviewed companies are. It was decided to complete five interviews with persons from different organizations. When having a good number of identified organizations that matched the requirements, two templates were written for the email invitations, one in Swedish and one in English. Later the invitations were sent to the respondents with suggestions on dates and a short description of the thesis and the interview itself. When an interview was booked the interview guide was sent together with an accurate description of the thesis to the respondent. When conducting the interview, the respondents were carefully asked if they were okay with having their names, roles and organization names written in this thesis. Moreover, they were asked if the interview could be recorded for being able to transcribe it and later on use it in the text. As all of the respondents approved this, it was chosen that names, roles and organizational names were involved in the text as it gives extra credibility to this Masters thesis. As all five interviews were extensive regarding lengths and information, it is argued that five interviews are enough for the data collection.

Waboba, Swedish Television, Scania, Stora Enso and Klarna are the respondent organizations. All five are active in more countries than only Sweden. However, they are all having their headquarters in Sweden after being founded in Sweden, which allows the data collection to get an international perspective with a Swedish focus as the regulations are similar for all five organizations. Similarly for all the organizations are that they were all teleworking to some extent whilst the interviews were conducted. Moreover, they all work with cyber security in one way or another. Waboba is a company with offices in Sweden, China and the

United States of America (Waboba, n.d). They are selling products to consumers with a goal of keeping life fun (Waboba, n.d). Axel von Heland is the CEO and responsible for the cyber security within the company, he is the respondent for this thesis from Waboba. SVT is the Swedish public service television company that has four TV channels as well as digital services available in Sweden (SVT, n.d). Daniel Ekelöf is the head of Distribution and Cyber security and the respondent for this thesis from SVT. Scania is a global company active in more than a hundred countries, selling trucks, busses and services through business to business (B2B) (Scania, n.d). Fredrik Tomasson is the Chief Information Security Officer and the respondent for this thesis from Scania. Stora Enso is a global company that produces products based on wood and biomass and they work Business to Business (B2B) (Stora Enso, n.d). Patrick Andersson is the Chief Information Security Officer and the respondent for this thesis from Stora Enso. Klarna is a global payment supplier that offers flexible solutions to both businesses (B2B) and consumers (B2C) (Klarna, n.d). Mark Strande is the Chief Security Officer and the respondent for this thesis from Klarna.

Table 3.1: Summary of Respondent details

Respondent	Company	Country	Position	Appendix
Axel von Heland	Waboba AB	Sweden	CEO	Appendix 1
Daniel Ekelöf	Sveriges Television AB	Sweden	Head of Distribution and Cyber security	Appendix 2
Fredrik Tomasson	Scania AB	Sweden	CISO	Appendix 3
Patrick Andersson	Stora Enso AB	Sweden	CISO	Appendix 4
Mark Strande	Klarna AB	Sweden	CSO	Appendix 5

Table 3.2: Summary of Interview details

Respondent	Interview date	Communication Channel	Duration (record)	Appendix
Axel von Heland	22/04-21	Google Meet	35 mins	Appendix 1
Daniel Ekelöf	19/04-21	Microsoft Teams	47 mins	Appendix 2
Fredrik Tomasson	22/04-21	Google Meet	60 mins	Appendix 3

Patrick Anders-son	12/04-21	Microsoft Teams	57 mins	Appendix 4
Mark Strande	22/04-21	Google Meet	48 mins	Appendix 5

3.3.4 Design of Interview Guide

Before performing the interviews for the research an interview guide was built as the foundation for the semi-structured interviews. The interview guide was divided into four categories; Intro questions, questions related to the Technical aspect and its sub-aspects, questions related to the Social aspect and its sub-aspects and lastly questions related to the Risk Tolerance aspect and its sub-aspects. The sub-aspects are underlined and marked as bold while the different areas, in the sub-aspects, are marked as bold. The intro questions had the purpose of getting the respondents approval and to create understanding for the interview itself. The questions in the following three categories were related to the research model and had the purpose of collecting relevant data for the research. Following is Table 3.3 which is the interview guide:

Table 3.3: Interview Guide

Interview Guide
Intro Questions
-Is it okay that we record this interview? And is it okay that we use your name, role and organization in our transcription? - The thesis will later on be published by Lund University. -Is it okay that we use your name and organization in our Masters thesis? (Describe our thesis and purpose of the interview.) -All questions are focusing on the effects of forced teleworking, so try to focus your answers on a time frame from March 2020 to today. We will show a PowerPoint to make our questions easier and clearer for you to understand. -What is your name and role at organization X? -Are your organization teleworking? When did it start? Is it forced? And how many percent of the employees are teleworking?
Questions Related to the Technical Aspect and its Sub-aspects

Cyber Security

-What challenges and threats do you see with forced teleworking in an IT-security perspective for your organization?

Malicious Attacks

-Have you had any problems with some kind of malware attack towards your organization since March 2020?
-What happened? How was it handled? What did it cost?
-What kind of attack?

-Have you seen an increase in the number of malware attacks?

-Can you rank these types (from the most common to the least common) of malware attacks regarding threats for your organization when teleworking? (Describe them if needed)

Viruses, Ransomware, Scareware, Phishing, Worms, Spyware, Trojans, Adware, Fileless malware

Security Practices in Organizations

-Are you using any cyber security standards and frameworks to handle the threats from teleworking?

Security Standards and Frameworks

-Are you using any of these cyber security standards and frameworks to handle the threats from teleworking (Show picture of all the named ones below)?

- ISO27001, BS 7799, PCIDSS, ITIL, COBIT
-Anyone you see as extra important?

-Any other cyber security standards or frameworks you use?

Cyber Security Practices

-What security practices do you use to ensure safe teleworking for your employees?

-Do you use any of these cyber security practices to handle the threats from teleworking (Show picture of all the named ones below)? Firewalls, document cyber security policies, education of employees, plan for mobile devices, enforce safe password practice, regularly back up data, installation of anti-malware software or multi-factor identification.

-Anyone you see as extra important?

-Any other cyber security practices you use?

Security Practices Embedded in Teleworking

-Have you used any specific cyber security practices to handle the forced teleworking? For example DNS filters, VPNs, BAS, protocols or such.
-Do you see an increase in the use of these practices due to a growing number of teleworkers?

Questions Related to the Social Aspect and its Sub-aspects

Cyber Security

Social Engineering

-What is your organizational take on Social Engineering? Is it a big problem for your organization? Are hackers trying to use your employees to reach internal data and systems etcetera.?

Security Practices in Organizations

What security practises do your organization have in co-relations to cyber security when teleworking?

Cyber Security Practices

-Do you give training and education to your employees to minimize the threat from social engineering?
-How often? Have you added extra training due to forced teleworking?

-Do you have policies for your employees on how to telework to minimize the threat from hackers?

Teleworking

Timeline of Teleworking

-How has the evolution of teleworking been in the context of your organization? Is it many more employees teleworking now? Effects of this?

Effects of Teleworking
-How has forced teleworking affected the employees of your organization?
-Do they have to work in a different way then before to keep devices and networks etcetera secure?

Questions Related to the Risk Tolerance Aspect and its Sub-aspects

Teleworking

Effects of Teleworking

-Was your organization prepared for letting the employees telework when Covid-19 came?
-Did you see an increased security risk when an increased number of employees telework?
- What level of understanding does the employees of your organization have of the threats that might occur when teleworking?Do you consider they were/are prepared from an organizational point of view?

Security Practices in Organizations
- How well do the employees of your organization know the security practices of your organization?

Standards and Frameworks

- Do the employees have an idea of what framework/standard your organization follows?
- How important do you think it is for employees to know about the standard that your organization follows?

Cyber Security Practices

- Do you see a difference between departments of your organization about the knowledge of security practices? What departments seem to be more likely to get attacked, and which departments suffer from more attacks?

Security Practices Embedded in Teleworking

- Do you see that employees with more knowledge about security practices in teleworking are more risk taking?

3.4 Data Analysis Method

When the interviews had been conducted, the data was gathered by transcribing the interviews (see Appendix 1-5). Transcribing an interview can be explained as a transformation from oral form, for example, recorded interviews, to written form, to later support the analysis of the data (Kvale, 2008). An advantage of using a qualitative approach is the great volume of data that is generated, which is needed for analysis (Recker, 2013). Research says that the data that is gathered and transcribed from interviews do not have to be understood fully, for example, which parts are relevant for the final outcome and why (Recker, 2013). The importance when analysing the data is to make sense of the data and understand it, rather than explaining it (Bhattacherjee, 2012). To achieve a nuanced understanding of the phenomena an analysis gathered from the interviews and the literature is needed and recommended (Recker, 2013). Furthermore, when transcribing the interviews, different recording devices were used to allow functions as pause and fast forward, in order to not miss out on any information. The tools that were used for recording were Microsoft Teams own recording software, the thesis groups phones and Google Meets recording software.

To analyse the data for further use, this study used the concept of coding, which is a common and useful technique, since it is argued that it reduces a great volume of data to meaningful and sensefull information (Recker, 2013). Moreover, coding techniques organize and categorize data, which is useful when researchers need to grasp concepts, key ideas or themes that can unfold during the analysis (Recker, 2013; Bhattacherjee, 2012). The most common coding concepts are open, axial and selective coding (Recker, 2013; Bhattacherjee, 2012). This thesis used these concepts of coding, due to its ability to uncover and name concepts within gathered data (Recker, 2013). Other benefits of these coding techniques involve couple central categories, or organizing concepts into relationships (Recker, 2013). We do believe that coding is the best suited analysis technique for this thesis. Furthermore, it is important to understand that the analysis is built upon previously discovered aspects found in Table 2.1, which is how we grouped the insights found when coding the gathered data.

Furthermore, the belief is that it is important to remember feelings of the interviews when they need to be analyzed, which led us to write down impressions and personal thoughts from when they were conducted. This method is called memoing, which is a technique that enables the researcher to subjectively comment and reflect upon what was happening during the interview (Recker, 2013). Moreover, this technique can be used to describe *"hunches"* from the interview, as well as keeping track and refine ideas when analyzing the data (Recker, 2013). The coding in this thesis is mainly based on the previously discovered aspects in Table 2.1 and the interview guide was created as a product of this. In order to efficiently code the transcribed interviews, a coding scheme based on the aspects and sub-aspect from the research model was made, where Technical, Social and Risk Tolerance represent the codes, and the sub-codes are in line with the sub-aspects, which is presented in Table 3.4.

Table 3.4: Coding Scheme

Code	Code Description	Sub-Code	Sub-Code Description
S	Social	CS-SE SPO-CP T-TT T-ET T-FT	Cyber security - Social Engineering Security Practices in Organizations - Cyber security Practices Teleworking -Timeline of Teleworking Teleworking - Effects of Teleworking Teleworking - Forced Teleworking
T	Technical	CS-MA SPO-SF SPO-CP SPET	Cyber security - Malware Attacks Security Practices in Organizations - Standards and Frameworks Security Practices in Organizations - Cyber security Practices Security Practices Embedded in Teleworking
RT	Risk Tolerance	T-ET	Teleworking - Effects of Teleworking

		SPO-SF SPO-CP SPET	Security Practices in Organizations - Standards and Frameworks Security Practices in Organizations - Cyber security Practices Security Practices Embedded in Teleworking

3.5 Ethical Considerations

In the development of the study it was important to take ethical aspects into consideration throughout the entire process (Patton, 2015). These aspects are processing questions regarding morality that help to point out what is right and wrong in different contexts (Recker, 2013). The motivation for taking ethical aspects into account is that it can ensure for the research that the research is developed in a proper manner (Patton, 2015; Recker, 2013).

Interview processes can affect respondents in different ways, it can make emotions and memories come to the surface (Patton, 2015). For us as interviewers it is important to stick to the plan to collect relevant data in the interview and not dissociate from it (Patton, 2015). In the interview process it was crucial for us as interviewers to be prepared and aware of issues related to ethics when leading the interviews. We needed to ensure that the respondents rights were being protected and that we prioritised confidentiality and kept the respondents consent throughout the entire process (Recker, 2013; Ryan, Coughlan & Cronin, 2009; Patton, 2015). If the respondents wished to be anonymous we needed to make sure to preserve it and ensure that it cannot be revealed and that the research data was stored in a secure way (Recker, 2013; Ryan, Coughlan & Cronin, 2009; Patton, 2015).

It is of high importance for the interviewers to achieve full consent among the respondents that are taking part in the research (Ryan, Coughlan & Cronin, 2009). In order to get this, information about the study and the entire interview guide was shared with the respondents before the actual interview took place (Recker, 2013). During and after the interviews the respondents were asked for their consent again to make sure that they were certain in partaking in the research (Ryan, Coughlan & Cronin, 2009). The interviewers of this thesis were aware of the fact that respondents could change their mind during the entire process which strengthens the motivation to constantly check for consent to be prepared for changes (Recker, 2013). Since the research can touch upon sensitive company security information it was decided to let each respondent check their own interview transcription before it was used further on in the thesis and later on all the respondents got a copy of the thesis before it was published (Ryan, Coughlan & Cronin, 2009; Patton, 2015). During the entire research process, ethical aspects were always considered in order to be prepared for issues related to it (Recker, 2013; Roig, 2006). It was also of high importance for the authors to maintain a high standard and relevance through the entire text to achieve an unique text that could contribute to the field (Recker, 2013; Roig, 2006).

3.6 Scientific Quality

While developing and performing the study it was important for the authors to keep a high quality through the entire process. From the text below you as a reader will be able to get an insight into what actions were made to achieve research with a high scientific quality. When selecting a research area, it was important to select a topic that could contribute to the research field (Buchholz, 1995). When developing the research question it was essential to find a question that would be achievable at the same time as it would be stimulating to research about (Recker, 2013). To achieve a research question with a high quality it has to follow the ethical principles and be relevant at the same time as it is innovative to research about (Recker, 2013).

Besides the research area it is also important to make sure that the content of the whole research stays unique and non-redundant in order to achieve a high quality of the study (Buchholz, 1995). When developing the literature review it was important to only develop it through varied trustworthy high qualitative literature in order to get a reliable foundation for the research (Efron & Ravid, 2019). In the paper, transparency was of priority in order to allow the readers to get a full understanding of the whole research process which makes it possible for them to further develop the study or repeat it (Bhattacherjee, 2012). After performing the interviews the collected data was analysed in order to ensure that it kept a high quality, was accurate as well as useful for the research purpose and aim (Patton, 2015). When analysing, discussing and making conclusions from the collected data it is important that the authors are striving to be objective (Buchholz, 1995). Authors need to be aware of the fact that bias is hard to eliminate which makes it crucial to keep this in mind when developing the research (Sica, 2006). It is strived for developing the research in a non-bias way but it is crucial for the reader to understand and have this in mind when reading the research (Sica, 2006).

4 Findings

This chapter will involve findings from the interviews. The findings are divided into the thesis' three different aspects, where 4.1 handles the Social aspect, 4.2 the Technical aspect and then 4.3 the Risk Tolerance aspect.

4.1 The Social Aspect

When asking the respondents on the amount of teleworkers within their organization, it was clear that it differed. It had however gone up drastically since March 2020. Table 4.1 presents the number of teleworkers from the companies, gathered from the respondents' answers.

Table 4.1: Number of Teleworkers at the Organizations

Company	Number of teleworkers	Appendix
Waboba	70 percent of the organization in Sweden	I1, R10
SVT	Above 50 percent	I2, R6
Stora Enso	10 000 of 26 000	I4, R4
Klarna	100 percent	I5, R4
Scania	Everyone that can, except for factories, workshops etcetera	I3, R4

With the forced situation, due to Covid-19, all of the interviewed respondents were claiming that teleworking within their organization has increased (I1, R6; I2, R6; I3, R4; I4, R4; I5, R4). Some of the respondents were claiming that their organization was prepared and ready to telework while others were not. According to Patrick Andersson from Stora Enso, they were prepared and did already hold the needed capacity *"... remote working was a capability that was deployed to all our work stations already and the capacity was there already for all to be able to remotely connect"* (I4, R6). Employee stress has however increased, since more scheduled and unscheduled meetings have appeared due to the lack of physical meetings, according to Stora Enso (see Appendix 6). Mark Strande from Klarna claims that Klarna also had the capability to telework in place before March 2020 as they had remote capabilities to connect (I5, R4). Klarna also highlighted that with them growing into a more global company, their use of teleworking has increased (I4, R48). Axel von Heland from Waboba believed that Waboba workwise were prepared for letting their employees telework when they were forced to (I1, R68). Daniel Ekelöf from SVT believed that SVT was not prepared but at the same time he believed that the transformation went relatively smooth for them (I2, R44). According to Fredrik Tomasson from Scania the employees have been able to telework for many years and even if the amount of teleworkers increased from March 2020, it did not become a technical problem for them, but Scania claims that teleworking definitely has its effects (I3, R40). Stora Enso had everything in place for teleworking, it was more of an upscaling of their existing systems that had to be done (I4, R28). Teleworking was mainly not forced for the Swedish

part of Waboba and when asking if it was more of a recommendation he replied that Waboba followed the swedish recommendation model (I1, R8). It was more of a recommendation than forcing for Scania in similarity with Waboba (I3, R6). Also Stora Enso stated that it was not mandatory for their organization, but that some restrictions for the offices have been made (I4, R4). SVT and Klarna claimed that their employees were forced into the teleworking:

"[...] we did actually force a lot of people to not come into the office, saying we don´t want you here[…]" (I2, R6).*"[...]we naturally came to a point where we needed to evacuate and move out from our offices all together[…]"* (I5, R4).

SVT highlighted that some employees need to be located at their office in order to do their work and that teleworking was not applicable for that working group (I2, R6). Scania also pointed out that some of their employees could not telework as they needed to physically be on site (I3, R4). Also Stora Enso claimed that some employees, the factory workers, needed to be on site (I4, R4). Klarna mentioned that a few exceptions were made for some employees that had to work at the office (I4, R5). Many of the respondents presented issues that are factors of forced telework. Before the forced teleworking situation it was mostly the same employees at SVT, that were quite tech savvy, that were working from home (I2, R8). SVT also brings up that teleworking has led to employees being less focused while working (I2, R12). Scania claimed that while teleworking, hackers are more likely to trick the employees into doing things on their computer (I3, R8). Due to the forced teleworking, Waboba believed that the motivation of the employees at Waboba were affected in a negative way (I1, R64). On the other hand, Waboba thinks they have handled the forced teleworking from a business perspective quite well (I1, R64). At the same time Waboba highlighted that the forced teleworking affected them in some ways:

"[...] when everyone worked from home we had significant changes, everything takes more time and also decisions that should happen, don't happen and that could be security risks in itself and then all the phishing attempts that I mentioned before that you cannot check them with the person next to you, it is easier to fall for some" (I1, R72).

SVT also points out that due to the forced teleworking the amount of users on the VPN increased leading to it being a lot of traffic there at the same time (I2, R32). Because of the forced teleworking situation, SVT introduced some new security policies that were related to their employees, for example that they had to use longer pin codes and they had to be better at separating private email, phone and other devices from the company ones (I2, R42). SVT also claimed that the teleworking situation, with employees doing uncommon tasks remotely has led to a higher risk (I2, R46). Stora Enso believed that due to the forced teleworking, more offices, after the pandemic, will be more accepting of teleworking than they were before (I4, R36).

Issues that are related to cyber security are occurring in all of the interviewed respondents organizations. But some of the issues are not as easy for the respondents to determine whether they are effects of the teleworking or if they have increased due to something else. Waboba pointed out that hackers are using social engineering and have become more and more efficient in finding the right roles in an organization that they should reach out to (I1, R14). As previously stated, Waboba was not aware if it is connected to the forced teleworking or not (I1, R14). Waboba also mentioned that the existing phishing attacks are not much of a threat

because he believed that his employees were aware of the issue and knew how to handle it "*...someone sees something that is suspicious we reach out*…" (I1, R18). At Waboba they have seen an increase in social engineering as hackers are trying to reach out to them over LinkedIn in order to get a clear vision of their organizational chart that later can be used for phishing attacks (I1, R56). Waboba answered no on the question regarding if any hackers are trying to use their employees to reach internal data and systems (I1, R58). SVT claimed that they also have a lot of issues with social engineering and that for them as a media company it is quite hard to find a good workaround related to it:

"[...]the concept of not clicking on the link is completely useless since our whole job is to click on links, that's what we do. So for you as an IT department to say don't click on the links is like saying don't do your job." (I2, R34).

Scania claimed that risks related to social engineering have increased but he does not think that it is related to people working from home (I3, R34). Scania also believed that it is important that the employees are aware of this ongoing issue and that Scania as an organization is trying to stop hackers from reaching the employees before they accidentally click on the infected linkes (I3, R34). Stora Enso had some issues of social engineering in hackers trying to reach out to their employees, but at the same time they claim that this issue is something that is a part of their awareness program (I4, R30). Stora Enso believed that there is financial motivation behind the hacking attempts (I4, R30).

All of the respondents that were interviewed were claiming that they are providing training related to security issues for their employees (I1, R36; I2, R36; I3, R36; I4, R18; I5, R44). SVT provided training for their employees related to social engineering, but believes that it could be valuable to do it more often (I2, R36). For Stora Enso, training of the employees was very important for creating awareness of the dangers and threats of internet usage and IT (I4, R18). But on the other hand Waboba stated that they aren't providing any training related to social engineering for their employees, but that it is something that they probably should be doing (I1, R60).

During the forced teleworking phase, some of the investigated companies increased their training related to teleworking. Stora Enso added some extra training, education and provided extra material towards their customer services, since they were not teleworking to the same extent prior to the forced teleworking period (I4, R46). SVT also stated that they added training for their employees as a result of the forced teleworking *"In the beginning there was a lot of education both around the standards but also on which solutions that we should use"* (I2, R30). Scania said that they have added some training related to forced teleworking but also say that you can always do more (I3, R36). At the same time Waboba did not add any extra training due to the forced teleworking (I1, R62). Like Waboba, Stora Enso did not add any extra training due to the forced teleworking, but the reason for this is that they already were prepared for it:

"But we didn't add any extra training. The reason might actually be just the timing, we had just prepared, by coincidence a major awareness program as Corona struck, so we had already the material, the animations, the electronic documents already" (I4, R32).

To ensure safe teleworking, Klarna described that it is highly important with training of the employees, for instance their awareness training that is mandatory, which also has to be renewed annually (I5, R24). The main motivation for having this type of training is because of the fact Klarna believes that the most important factor that influences security, especially when teleworking, are the employees at the organization and their behavior (I5, R26). To ensure that Scania's employees are teleworking in a safe way they are using a phishing platform where the employees are exposed for fake phishing attempts, if an employee fails during these attempts they automatically end up in training (I3, R36). The training for the employees related to cyber security when teleworking should be focusing on various things according to the respondents. Klarna claimed that it should prepare them for certain circumstances (I5, R58). Klarna also mentioned the importance of educating the employees by stating that:

"[...]It also all starts and ends with employees. It's like technology is built by people, so unless you educate the people that build the technology or educate the people that use the technology, it's kind of useless to put a very complex and very advanced tool in the hands of someone who doesn't understand why they should be using it" (I5, R34).

A significant indicator of Klarna's methodology in how they handle the cyber security related to their employees is in the way that they do not allow BYOD and in the way that they are moving towards a Zero-trust infrastructure principle (I5, R32). SVT also stated they are using a Zero-trust principal within their organization (I2, R64). To avoid breaches they also have a playbook as guidelines (I5, R40). Waboba mentioned that their employees mainly used common sense when they were dealing with security (I1, R24). Due to the forced teleworking, Stora Enso had to make the employees more aware of how they use their equipment when working in a home office to avoid security risks (I4, R8).

4.2 The Technical Aspect

When asking the respondents about IT security threats for their organizations, all of them had a lot of precautions to handle these kinds of threats. In terms of malware, Daniel Ekelöf from SVT mentioned it is an ongoing threat landscape all the time and that they can see an increase in phishing attempts and spam, which eventually could lead to malicious attacks, such as trojans (I2, R10). SVT also said they evaluated almost every single video telecommunication tool during March and April last year before ending up with Microsoft Teams (I2, R30). Moreover, Axel von Helan from Waboba also mentioned phishing as a common problem for their organization, since a phishing attempt could lead to someone sending a fake invoice (I1, R12; I1, R90). Neither Fredrik Tomasson from Scania or Patrick Andersson from Stora Enso see telworking as a big change in threats compared to the time before upscaled teleworking (I3, R8; I4, R6). What Scania mentioned is that when hackers are trying to send emails or links to malware, they are focusing on the ongoing phenomena, which is covid, in order to trick the users (I3, R8). Scania also mentioned that the number of individuals that are able to affect the internal network is less now compared to before (I3, R8). Mark Strande from Klarna has made some slight changes in their client platform during the period of forced teleworking, it was however a natural evolution that was already planned (I5, R6). Stora Enso mentioned they do not have any significant problems with new challenges connected to forced teleworking (I4, R6). They did however mention that when people are sitting outside the office locations, a problem could be that their internet access is not filtered, nor scanned for threats on

the internet activities (I4, R6). The threats coming out of this are however manageable for Stora Enso (I4, R6).

"[...]a difference when people are sitting from home environments rather than in our office locations, and that is that their internet access is not filtered, it is not scanned for threats on the internet activities that they perform if they for example start up a browser and type in an address, there is no active threat scanning on that webpage." (I4, R6).

Furthermore, Klarna mentioned that they do not have any particular problem with malware attacks as of today, but they do have seen an increase in attempts (I5, R10). The rest of the respondents seem to have the same experience as well (I4, R8; I2, R12; I3, R8). A reason why security incidents might have gone up, according to Stora Enso, could be that people change work behaviour and try to execute new types of software in their home environment (I4, R8). They have however not had the time to digest or review the cause of it, as they can only see blocked software installation attempts, which ended with the short answer that there is an increase in security incidents, but the consequences were nothing they could not handle (I4, R8). SVT did not see a shift in attacks, just an increase, where the suspiciousness lies that hackers know that a vast majority of employees work from remote locations (I2, R12). Waboba responded that they did not know if there had been an increase, since it is something they have not thought about (I1, R18). Moreover, Scania did not want to call it an increase in attacks, but they mentioned that the workload is higher since they had to investigate more incidents (I3, R10). Furthermore, Scania mentioned that hackers are more concentrated on companies using Office365, since a lot of companies are using this solution which means that phishing attacks that get credential have also increased towards Office365 (I3, R14; I3, R34). In terms of hackers, Waboba said that hackers are not trying to use their employees in order to access internal data and systems (I1, R58). Both Scania and Stora Enso mentioned different types of hackers, which could be called hacktivists, state sponsored among other names, and it all depends on their focus and target, since different types of hackers will target different kinds of persons (I3, R50; I4, R30).

"[...]I mean it depends completely on what kinds of problem we are looking at, if we are taking a look at hacker groups or individual hackers or state sponsored hacking they all have different focus and they will of course target different types of persons[...]" (I3, R50).

When ranking the types of malware attacks presented during the interview, Waboba ranked phishing and business email compromise in the top, which they saw as the same type of attack (I1, R20). They did also mention that they have a lot of other malware, such as viruses, trojans and worms, but they did not really know the frequency and could not categorize them as easily (I1, R20). SVT, Scania, Stora Enso and Klarna all ranked credential phishing/ credential harvesting as the top threat for their organizations, but SVT mentioned that when phishing becomes advanced enough it is more classified as social engineering than spam (I5, R16; I2, R34; I2, R16; I3, R14; I4, R10). Furthermore, SVT mentioned that a lot of the phishing links come through your cellphone today as an sms, which people are not as used to (I2, R34). Scania also stated that the younger workforce work more through their phones than the older, and that they consume IT differently, however this is something that they take into account when they are developing new services, but also when they are recruiting (I3, R54). Stora Enso however separated credential harvesting/phishing from business email compromise (BEC), and saw that as their second biggest threat for their organization, while the third was ransomware, since the rest of the threats were detected fast (I4, R10). SVT saw a lot of the threats

shown as combined, since you get ransomware or spyware through phishing, but had a focus on the delivery of the threats, meaning the method of getting in, which is how SVT wanted to separate the threats (I2, R16). At Scania, the physical coding threats, such as viruses and ransomware were not seen as common ones (I3, R14). Klarna found it hard to categorize the threats, since they thought it was difficult to differentiate threats such as trojans, spyware and others, but the biggest volume come from email, but they did not carry statistics of all the attempts, since it was handled well (I5, R14; I5, R16). In Table 4.2 you will find a summary of the top three threats, in terms of malware, found during the interviews.

Table 4.2: Ranking of top Three Malware Threats

Malware	**Rank**
Credential phishing/harvesting	1
Business Email Compromise (BEC)	2
Ransomware	3

When asking the respondents about security standards and frameworks, Klarna mentioned that they naturally have a foot inside ISO27001, and since they also use cards they need to adhere to PCIDSS (I5, R18). They did not however use them to handle threats, since they use a risk based approach, but they do use a lot of different frameworks for compliance reasons, and also independently audited (I5, R18). Moreover, Klarna mentioned that they also apply their own framework, but their auditors sometimes use COBIT (I5, R20). Finally, Klarna said that they are looking more and more into NIST, since it is becoming more important for their business, but they saw challenges with using NIST, since it is extensive and wide as a framework (I5, R22). Stora Enso did not use anything that is related to teleworking, but they did try to follow best practices in terms of cyber security and information security (I4, R12). What they did use is the national institute of standards of technology cyber security framework (NIST CSF), in order to capture their maturity and do gap analysis of capabilities (I4, R12). They also use the NIST CSF to do top management reporting, and they also use it to map decisions, priorities and resources of activities to further improve their maturity (I4, R12). Furthermore, Stora Enso mentioned the CIS framework and also recommended the information security forum where Stora Enso had been a member since year 2000 and have published an information security management framework that they call the "*Standard only*" (I4, R12). This will eventually map the user to any of the security standards and frameworks mentioned earlier in this thesis (I4, R12).

When asking SVT about the standards and frameworks they use, they said that they are using some parts of ISO27001, but also NIST, which they saw as quite similar to ISO27001, but simpler (I2, R18). Moreover SVT said that they are trying to use a combination of the two, since they differentiate how information security works and cyber security works, but the importance lies in having a methodological way of working together (I2, R20). The view on the differences between cyber security and information security is something that Scania also mentioned, where cyber security exists only in the digital world and information security are all carriers of information, for instance paper (I3, R20). As for standards and frameworks, Scania said that their information and IT security department is in the process of becoming ISO27001 certified, but not all of Scania (I3, R16). Furthermore, Scania mentioned that the

standards shown during the interview is more for strategic security work and does not increase the protection, or take care of, threats (I3, R16). NIST is also mentioned by Scania, they are not however using it directly, it more influences their work, since a lot of the other industry specific standards are built from NIST (I3, R18). Waboba said that they did not really know what standards that existed, and added:

"[...]That is a very difficult question for me to answer as I don't really know what standards there are but I think in general the main thing that we are using is just common sense and just check[...]" (I1, R24).

Two of the respondents, Scania and Klarna pointed out a factor that plays a big role when handling their cyber security and choosing security standards and frameworks, this factor was regulations (I3, R16; I3, R18; I5, R18). Since Scania is a part of the automotive industry, they have to look at new legislations and regulations for the safety of their IT, both outside and inside their product, which means that the regulations that are for making the digital world around the vehicle more sage (I3, R16). When Scania says they are influenced by NIST and use it indirectly, they claim that they are focusing more on industry standards and regulations that in turn are based on, for example, NIST (I3, R18). Furthermore, they state that they are not only looking at international standards, frameworks and regulations, but also country specific regulations, since they are active in many different countries (I3, R22). This means that different countries have different views on how to handle, for instance, cross border traffic of information, where information needs to be stored, which affects design and how data should be treated and stored (I3, R22). Klarna on the other hand are a regulated financial institution, which means that they have to abide by frameworks and regulations specific to their industry when analyzing risks, building up controls and risk structure in accordance to both regulations and threats that are applicable to their organization (I5, R18).

The cyber security practice that Waboba used were mainly multi factor authentication (MFA), as well as built in firewalls into different services like the gateways, routers and computers, but they do however rely a lot on the security from using Office365 (I1, R24; I1, R30; I1, R32; I1, R16). Their internal system started to use MFA this year, but through their Office365 they have implemented it in a couple of steps going back three years (I1, R82). SVT said that they work with all the security practices mentioned in this thesis, but they have ramped up the use of MFA over the past year (I2, R24). SVT mentions however that it is sometimes hard with anti-malware software, since they have quite specific industrial systems that do not run the software the same way, as well as it depends on the type of computer a user is using, for instance Mac, Linux or Windows (I2, R24). One thing that SVT believed was missing for them was that if one has a big network, it could be beneficial to have some kind of network segmentation, so not all networks are connected to each other and the whole network is not connected to the internet (I2, R24). Furthermore, planning for mobile devices has become more important for SVT because before the forced teleworking their internal network was pretty open to use, so it created a safe perimeter, but when everyone is teleworking, the risk is that those clear perimeters from before are not as clear anymore (I2, R24). Since SVT has put more emphasis on mobile devices, they have implemented a concept called Zero-trust and explains it like:

[...]and also, as I said, we re-focus a little bit on protecting the device. It's a concept that is a bit popular that is called Zero-trust. So basically when you don't have a clear perimeter of

your network, because of the fact that people are home or wherever, you have to protect and authenticate the devices more clearly than if they only are on the network." (I2, R26)

Scania also mentions that they use all of the security practices mentioned earlier in this thesis, with an emphasis on MFA, an EDR tool and a HX tool which has a high protection function, but can be used for extraction of data (I3, R24). Moreover they use jump servers internally for doing administrational servers and infrastructure (I3, R24). One technical tool that Scania uses in order to measure how the employees click on links is through a phishing platform (I3, R36).

Stora Enso mentioned that first and foremost they use encryption, both in transit, which refers to the transmission of information and then encryption of the rest, which means if someone lost a Stora Enso computer in public, it does not count as a security issue (I4, R18). Moreover, Stora Enso mentions technical solutions for communications such as chatting, video calls and more, when using encryption (I4, R18). Traditional anti-malware software was seen as useless by Stora Enso, instead it was recommended to use endpoint threat detection and response (ETDR), but MFA was seen as a cornerstone in the security work (I4, R18). Filtering capabilities on the network and network threat detection and response, are two additional practices that are mentioned (I4, R22). The biggest practice that Klarna employs is MFA, as well as full disk encryption in order to protect if one multi factor token would be stolen, but they also possess remote wipe capabilities, meaning they can wipe a stolen device from remote (I5, R8). The rest of the practices mentioned earlier are also used by Klarna, they do not however allow for BYOD and since they are a 100 percent cloud based company, they do not have any data laying around (I5, R32). Moreover, they do have anti malware threat hunting and a lot of endpoint protection built in and their security operations center work explicitly with threat hunting, threat protection and threat intelligence (I5, R32; I5, R36).

When asking the respondents on cyber security practices that are more specific towards teleworking, Klarna mentioned that they have something called a red team, that works with offensive security that is populated by penetration testers, that do attacks against their own environment and processes (I5, R40). For their teleworking they multiplied their VPN tenfold and increased their capacity to handle all their users when Covid-19 came and teleworking became forced (I5, R42). Scania mentions that they use VPN as well, and the practices mentioned from this thesis also play a big role when employees are teleworking (I3, R24). One practice that only Scania mentioned was the use of VTS, which is a kind of remote desktop, or virtual machine, which will not allow hackers or viruses to jump over to the physical environment at the office (I3, R26; I3, R28). They do however try to become more cloud based, and web based, but since they still have certain applications on-premise they have to access those through either VPN or VTS (I3, R30). Furthermore they mention that monitoring the traffic is more important now than before, so they have a security operations center for people to look at logs and patterns to see if something strange is happening (I3, R30). Scania has not introduced a lot of new technologies during their forced teleworking period, but some technologies have become more important and how the company looks at things have changed slightly (I3, R30). Stora Enso mentioned that they were adding more licenses and more bandwidth, in order to make sure the transition to teleworking would go smoothly (I4, R28). But they have not made any addition in certain practices towards teleworking, since they were already prepared for it (I4, R28). SVT also mentions that the use of VPNs and Office365 has helped them handle the teleworking quite well, since the capabilities were there, but they had to upgrade them slightly (I2, R28). Another practice that SVT mentioned is the use of DNS filters (I2, R32).

Lastly, Waboba mentioned that they do not have any of the cyber security practices, specifically for teleworking, since they were not seen as relevant for their organization, they do however state that they have all their services on the cloud, which means they can handle teleworking (I1, R50; I1, R66).

4.3 The Risk Tolerance Aspect

Axel von Heland from Waboba mentioned the current hacking attempts being easy to see through and catch since they are quite obvious (I1, R12). Moreover, Waboba did not see themselves as a big target yet for some types of attacks since the hackers think they are not big enough of a company and therefore have not enough value for being attacked (I1, R22; I1, R54; I1, R52). Mark Strande from Klarna argued for the same thing when he says *"So it is something that is in the price of doing business as a global company, the more famous and more known you become, the more attacks you have"* (I5, R44). Waboba also said that hackers are looking for less and less value for every year that goes by (I1, R54). Waboba did however see a risk with the hackers being more and more advanced (I1, R12). Moreover, Waboba mentioned a problem and increased risk when teleworking, with not having the chance to ask a colleague if a specific email or invoice request was sent from that person or if it was sent from a hacker when they are not in the same office (I1, R12). Similarly, Patrick Andersson from Stora Enso said that they had to give their employees guidelines on how to write emails and how to communicate internally to give trust indicators as some employees could think internal communications were phishing attempts (I4, R38). Stora Enso said that this was a consequence of the high awareness regarding cyber security among the employees (I4, R38). The guidelines involved for example language instructions, trust indicators that could be used instead of only writing *"best regards HR*" and other instructions on how to telework and communicate (I4, R38). These guidelines were designed to instill confidence in the internal communication without having to worry about it being phishing (I4, R38). Klarna said that they have no set language that they use when teleworking, he means that their email infrastructure is difficult to hack and therefore it is not easy to send an email as an internal sender and in this way they can ensure control (I5, R30). However, multiple respondents mentioned that, if internal communication with suspicious, urgent requests appear, employees should look for additional indicators (I4, R32; I5, R30; I1, R18). Within Klarna, they have internal controls in place to make sure no one falls for a fake invoice request that is said to be from a colleague (I5, R30). The risk was avoided through needed authorization from both the sender and the receiver and two factor authentication (I5, R30).

Daniel Ekelöf from SVT believed there is a big risk and challenge with teleworking being scaled up, and an increase in the number of teleworkers internally (I2, R8; I2, R46). With more people working from home, than only the IT savvy employees, the risk increases as more threats come along together with new tasks being done remotely which requires more access to their own services and working environments (I2, R8). Fredrik Tomasson from Scania also mentioned some risks with increased numbers of teleworkers but he also says that other risks have become lower at the same time (I3, R42). *"Before, if the two factor authentications would not work properly, it wasn't so bad. It was down for one hour, not so many people were affected, now everyone is affected"* (I3, R42). Moreover, Scania mentioned that there are security risks associated with teleworking that they did not have before, for example all the printers that are used from home as they cannot control them in the same way as the few

printers that are being used at office (I3, R42). If papers are printed at home there is a risk that papers are laying around or that certain information happens to be cashed in the printer (I3, R42).

Klarna on the other hand mentioned people's behaviour as the most important factor for security, especially while teleworking (I5, R26). When moving from a well controlled, well defined physical space to teleworking at different places, there is a marginal increase in security risks according to Klarna (I5, R52). Klarna mentioned customer service agents as a potential risk as they talk with customers about sensitive information and need to have control so that nobody overhears or sees their screen at home, this is naturally a different risk according to Klarna (I5, R52). Scania believed the new risks that come with teleworking are roughly on the same risk level as before even though they are new and less comfortable with them (I3, R42). Waboba saw an increased security risk when teleworking regards to the phishing aspect mainly as they cannot directly check with a colleague if it was a phishing attempt or an actual internal request (I1, R70). SVT mentioned that with the upscaling of an increased number of teleworkers you have more employees sitting in cafes and at home with their own wifis and these things are considered as higher security risks (I2, R46). Stora Enso said that they are aware of the risks that come when the employees telework from home, for example the uncontrolled internet access and the unfiltered internet access but they also mention that these risks are under control (I4, R34). The respondent did however mention that Stora Enso's CEO has communicated multiple times to all the employees reminding them that the work equipment is not for other usage than work use (I4, R34).

Klarna was fairly prepared for letting the employees telework when Covid-19 came and today the organization is 100 percent teleworking (I5, R50; I5, R40). Klarna had the basic aspects prepared but had to refresh a little bit and improvise some of it to adapt to the situation, moreover, they had to apply their principles towards their service providers (I5, R50). Stora Enso was prepared for the forced teleworking situation (I4, R32). Scania was also prepared for the forced teleworking situation, although it was a new situation to handle (I4, R42). SVT said that they do not think anyone was actually prepared for Covid-19 and the effects of the pandemic such as forced teleworking, he says although that the transformation was surprisingly smooth (I2, R44). *"We have VPNs, we have ways of doing remote editing, we already moved to Office365 so we had a lot of cloud enabled services so all in all it worked surprisingly well"* (I2, R44). Waboba mentioned that they were from an organizational, work perspective ready for letting their employees telework when Covid-19 came as they are spread out in a lot of different offices so their daily work is on a digital basis anyways (I1, R68; I1, R12).

When it comes to employee understanding of security threats that are associated with teleworking all respondents thought the employees of their organizations have either okay or good understanding of the threats. Waboba said that they mostly employ young people that are used to these sorts of threats, it is something that they have been subjected to for a long time, all their lives (I1, R74). According to Waboba there is a risk difference between employees depending on their age, meaning the respondent has to talk more about the security threats with the employees in the USA than in Sweden and China as they are older and therefore more of a security threat than the younger staff (I1, R76). Most of the employees of Klarna have a good understanding about the risks and threats associated with teleworking (I5, R53). Klarna also said that the risks differ depending on what ages the employees are in and as Klarna has a young generation with tech savvy employees the risks are smaller than at organizations where there is a bigger generational knowledge gap (I5, R56). Scania said that the

employees in general have a pretty okay understanding of the threats that might occur when teleworking (I3, R44). Scania thought that normal users have an okay understanding of things like phishing whilst the difficult stuff that could happen outside of the office is nothing normal users know about (I3, R44).

"*For example, if you are sitting at home you are not running VPN to the company, but you are running communication another way, what happens if I hijack your home router and then play around how it does DNS stuff. I can do petty fancy stuff. For example, if you are doing banking, I could actually imitate a bank page and fool you of the bank id and steal money from your account"* (I3, R44).

These types of security risks are more likely to happen when teleworking than office working, but there is still a very little chance that it happens according to Scania (I4, R44). Stora Enso employees had a very high awareness of the risks and threats associated with teleworking even before Covid-19 and the forced teleworking (I4, R38). SVT employees are according to the respondent getting better and better regarding the security understanding, he says that the understanding is not super high but the interest is growing and that employees ask more and more questions regarding cyber security (I2, R48). SVT has a different angle when it comes to clicking links in comparison to many other companies as many employees within SVT are journalists that seek for new information and this is a security risk that they need to be aware of (I2, R34).

When it comes to employee understanding of frameworks and standards, SVT said that the employees do not know what standard or framework the organization follows (I2, R50). However, SVT also mentioned that it is not important that they know about it as long as they are not part of the security department, instead the respondent thinks it is only important that they know that SVT has a structured way of working with cyber security with long term risk management (I2, R50). Scania had the same argument, saying that it is not important for a normal office worker to know if the organization uses standard a or b, they think that would probably be more confusing for the employees, instead, they should know that they follow a standard which makes the work structured (I3, R46). Waboba said that their employees know how they handle their cyber security as he usually posts news and threat alarms from Office365 to the employees (I1, R80). Moreover, they had to go through how to work with the multi factor authentications with especially the US employees as they thought it was a big pain to use (I1, R80). Stora Enso thinks that the employees of Stora Enso do not know about the security practices that they use and the respondent does not think it is fully necessary that they do either (I4, R40). Klarna thinks it is a fool's errand to get all employees within an organization to understand and follow a framework or standard (I5, R58). Instead, Klarna thought it is very important for the employees to understand the routines and the structure that they have in place (I5, R58). The respondent said again that the user training material is very important for this, for example, educating the employees of Klarna on how to handle phishing emails rather than governance structures (I5, R58).

Within the Waboba organization, the respondent said that the knowledge about cyber security between different departments of the organization does not differ so much, neither between different countries, instead Waboba thought it is more of a generational gap where the age is the difference (I1, R86; I1, R84). Waboba did however say that the finance department suffers from more attacks than the rest of the organization (I1, R88). Waboba did not think employees with more knowledge about cyber security are more risk taking than the ones with less

knowledge, instead they think they handle systems and threats more carefully than the ones with less knowledge and therefore the answer to the question is the opposite (I1, R92). SVT saw a difference between the departments but also within the departments and it is mostly connected to interests and what people work with (I2, R56). The IT staff know more about it, especially the support or development team, but the respondent also mentions that some journalists of SVT know a lot, whilst others very little (I2, R56). Moreover employees within drama and entertainment do not worry at all about these questions and in those departments there is a big lack of knowledge as they never had to use it (I2, R56). The IT-departments suffer from some attacks within SVT, the news organization does it too, especially because they have valuable information in house and also because some of them work with clicking links (I2, R58).

SVT thought employees with more knowledge about cyber security in some parts are more risk taking and break some policies that SVT has, meaning some people that know more take more risks (I2, R62). The respondent from Scania saw some areas of the organization being more security aware than others and the respondent thinks people that generally work with regulated things have a higher interest in security (I3, R48). For example, finance, credit and certain development teams are more security aware than other parts of Scania (I3, R48). Regarding what departments that suffer from more attacks, Scania mentioned that it depends on which kind of attack and which kind of hacker it is, they have different targets and therefore different goals with the attacks (I3, R50). Scania also saw that employees with more cyber security knowledge could be more confident in their actions and therefore be more of a risk than other employees, but the respondent is not really sure (I3, R52).

"I can't really say but one would hope people with more security knowledge on them would not fall for phishing attempts etcetera. But they could of course be confident in that, I know how this works so I could just be along a little bit and I know when to stop, and then it can be too late. Or it could be that they are being curious about what is actually happening so that they press the link. Or, I know that this is very bad but I know that I don't have viruses on my computer and I have protection in my computer which should protect me, lets see if it triggers an alarm" (I3, R52).

At Stora Enso there is no general knowledge gap between the different departments, the respondent said it is a general awareness (I4, R42). It was however easy for Stora Enso to answer what part of the organization that suffers from most attacks, it is the customer facing, meaning sales and support organizations together with top management and seniors (I4, R42). Stora Enso said that employees with more knowledge about cyber security do not act more risk taking, instead he said that they are more suspicious and ask him for example if a request is real (I4, R46). Klarna said that there is no big difference between the organizational departments when it comes to cyber security knowledge, it is only a difference between security professionals and engineers versus non-professionals (I5, R60). Klarna tracks their awareness training to ensure that there are no knowledge gaps within the organization as that could result in risks and threats, the respondent adds that there are no differences in the results but that professionals have a greater ability to understand the threats (I5, R60). The financial departments and the executives run a bigger risk of being attacked within Klarna according to the respondent, Klarna said that threat actors have become more and more professional in directing their attacks towards the right individual targets (I5, R62). Klarna said that many direct attacks that are sent to individuals within the organization are more relevant than before, based on relevant content and relevant narrative that hackers can have found on social media

etcetera. (I5, R62). This could be due to teleworking and Covid-19 according to the respondent, but it is difficult to say (I5, R62). Regarding whether employees with more cyber security knowledge are more risk taking than the other employees is very marginal according to Klarna, it could be that they are overconfident and therefore more risk taking, but the difference is marginal (I5, R64).

5 Discussion

Conceptualizing on the basis of the Social, Technical and the Risk Tolerance aspect has shown that the empirical setting has potential to contribute to both the literature and to practice. The discussion is divided into the three mentioned aspects taking the approach of identifying implications to both research and practice. Therefore, this chapter ends with highlighting the key implications identified to research and practice and how these three perspectives can broaden the understanding of what security risks and threats exist when teleworking.

5.1 The Social Aspect

According to Evangelakos (2020) the teleworking trend has increased significantly during the Covid-19 pandemic which is something that all the interviewed respondents can agree on. Gartner (2020) claims that a high number of employees will continue to telework after the pandemic as well, which is something that some respondents are agreeing with. It might be because of the fact that forced teleworking has been an eye opener for many employers, which might have helped them understand that teleworking can work for their organization. Evangelakos (2020), Belzunegui-Eraso and Erro-Garcés (2020) claim that the upscaled teleworking due to Covid-19 is a forced action. All the respondents in the study have varying opinions regarding if their teleworking was forced or not. It could be assumed that the reason for some respondents not wanting to use the word forced might be because of the fact that it has a negative tone that they do not want to be connected to. It could also be assumed that each organization has their own definition of the word forced, which will make their view on the connection with it different from each other.

Abraham and Chengalur-Smith (2010) claims that social engineering focuses on the weakest links of the organization, being the employees. The respondents agree with Abraham and Chengalur-Smith (2010) regarding the target of social engineering. Some believe that the hackers within social engineering have become much more efficient in their findings of what parts of the organization that they should reach out to. Moreover, they have seen that the hackers have started to reach out to their organization via LinkedIn in order to map their organization. This action of social engineering is something that the presented literature has not brought up. One might assume that the reason for this is because of the fact that these actions are relatively new trends that the literature has not had time to process yet. It could also be due to the fact that Abraham and Chengalur-Smith (2010) are disagreeing with the findings and are not seeing it as threats.

He et al. (2019) claims that it should be advised to provide awareness training regarding cyber security for their employees. This is something that all the respondents agree with and some of them are highlighting the importance and many benefits of their training programs. The reason for this similarity between the literature and the practice might be because organizations have understood the importance of cyber security and the effects that it can have on them. However, Reeves et al. (2021) are stating that too much training can be damaging for the view on how important adequate security knowledge is. This is not something that the respondents claim, some of them believe that it is always good to provide the employees with more training instead of putting limitations on it. One might assume that the reason for this

difference is because of the fact that Reeves et al. (2021) are more focused on how it works in theory instead of the actual needs that employees in organizations have for security training. One could argue that the respondents of this thesis always will want more cyber security training for their employees as the respondents are the responsible ones for the whole organization's cyber security and if they see a benefit with more training to minimize the risks for the organization, they will probably ask for this. This is however not entirely in line with the fact that Liang and Xue (2009) argues that more cyber security knowledge within the employee group can result in higher tolerance and more arrogance in the use of IT and ICT which can result in threats for the organization. Moreover, the attitudes, skills and values of an individual will also affect the organization's outcome and risk, both positively and negatively according to the Social aspect presented by Griffith and Dougherty (2002). In the case of employee training, these two aspects might be more intertwined than first anticipated. The characteristics of the Social aspect might affect the attitude towards employee training of cyber security, which in return can affect their Risk Tolerance, depending on the attitudes an individual might hold in the organization. In other words it can be argued that when creating employee training, an organization needs to monitor the attitudes of the employees towards the training, otherwise it can be argued that it affects their Risk Tolerance negatively. He et al. (2019) and Reeves et al. (2021) raise the importance of letting the employees build experience in dealing with malware attacks. Some of the respondents are claiming that they are building these experiences for their employees with physical platformes and guidelines. From the findings one might assume that it is more reasonable for larger companies to spend more resources on security training, both because they have resources for it but also since they are a bigger target.

Some of the other organizations are smaller, making it reasonable for them not to have the same possibility to put those kinds of resources on security training for their employees. One of the responding organizations can be seen as a big target for hackers since they are a financial institution. Due to this risk they might have identified security training as something that is worth putting resources on, which is a statement that goes in line with what Pyöriä is claiming (2011). Abukar and Bankas (2020) and Evangelakos (2020) suggest that organizations have policy protocols in place concerning behaviors and handling of data while teleworking. Some respondents claim that forced teleworking has led them to introducing new security policies in their organization related to employee behaviour and data protection. One might assume that it is reasonable for organizations to update policies during changing circumstances, like the findings show. Although Reeves et al. (2021) are strong believers of security training for their employees, they do not present how it should change during forced teleworking. The respondents highlight that due to the forced situation, security training was added for their employees. One might assume that it is rather odd that Reeves et al. (2021) ignore this subject even if it is written one year into the pandemic, on the other hand their study might have started before the pandemic even took place.

Abukari and Bankas (2020) and Evangelakos (2020) suggest that there are many security practises related to teleworking, such as practices related to planning for mobile devices (Kearns, 2016). In the findings the respondents describe some security practise initiatives related to the social aspect. Some of the respondents express that they are moving towards a Zero-trust principle. Respondents express that they do not allow employees to BYOD and that they have restrictions for use of equipment outside the office. Only one respondent answers that they do not use any specific cyber security practice except from common sense, meaning employees should act with practical judgements in their daily work. One might say that the difference between the respondents' responses regarding their security practises differs

because of various reasons. One reason could be the differences regarding company size as well as what industry they are active within. Another reason might be that some companies are seen a lot in the media, which might increase the threat on them. That is probably one of the reasons for them moving towards a Zero-trust principle. One might say that you can see correlations between the Zero-trust principle and BYOD, which is related to the concept of planning for mobile devices.

Babulak (2009) and Evangelakos believe that teleworking can have various effects on an organization, both challenges that an home environment can entail, but also opportunities such as the saving of resources and increased productivity among the users. When having digital meetings, employees can have back to back meetings without breaks in between in contrast to physical meetings where employees take coffee and talk to colleagues. Some of the respondents are however presenting issues related to teleworking and are claiming that it has led to their employees being less focused, less effective and that teleworking has increased employee stress. It could be assumed that the literature has a bigger focus on organizations' non-physical resources while the respondents focus more on the actual employees, meaning that teleworking works better on paper than in reality. The Social aspect does claim that individuals' well-being and stress can be affected by changes such as going from office working to teleworking (Bostrom & Heinen, 1977). Mann and Holdsworth (2003) claim that teleworking is related to mental health issues. In this study none of the respondents bring forward mental health issues, other than stress, related to teleworking. One might assume that the mental health issues might not be as serious as the literature suggests. But on the other hand one could argue that mental health issues are a sensitive area that people might feel is too taboo to bring forward and discuss in interviews. One can argue that the size of organizations can affect how teleworking is affecting mental health with the argument that the smaller organizations have a better cohesion and open communication between all employees.

The Social aspect says that forced teleworking can affect groups and their results (Bostrom & Heinen, 1977). The respondents argue that forced teleworking has not affected too much of their daily work but more the social part of work. One could argue there is a difference here between the mentioned working results but a similarity regarding the social group effect in organizations (Bostrom & Heinen, 1977). Communication tools have in this view changed the way of working, enabling efficient work structures digitally, it has however not had the same positive effect on groups and individuals. Even though literature says modern communication tools, that offer face to face contact, have changed the understanding whilst communicating digitally (Babulak, 2009), the technology has not revolutionized the social interaction which can compete with physical meetings. The mentioned coffee breaks and small chats are for instance not possible to satisfy in the same way online as in the office. When the social group effect is affected negatively, cyber security risks occur as employees can start acting less focused and thoroughly while working digitally.

5.2 The Technical Aspect

The empirical results partly disagree with the information found in the literature stating that when a majority of an organization is forced to telework, more problems might occur (Vrchota et al., 2020). Almost all the respondents somewhat agree that there has been an increase in cyber threat attempts when teleworking, but that attempt is not synonymous with

greater risk, threats or problems. Moreover, some of the respondents said that while incidents increased due to the forced teleworking, the consequence of the incidents is nothing that the organizations could not handle. One could assume that more teleworkers equals greater exposure to threats, which could partly be seen as true, especially for those with less resources. The technologies that exist today seem to work as a first line of defence to decrease the threat level that the literature seems to disagree with in regards to teleworking (Abukari & Bankas, 2020), meaning that the technologies that organizations use is more than adequate to handle the threats and risks related to teleworking. Various literature mention the huge costs that malware attacks have on organizations, where some researchers mention the costs of malware attacks in trillions of dollars globally (Abukari & Bankas, 2020; Morgan, 2020). However, very few respondents mentioned that cost was an issue for their organization in terms of malware attacks. One could perhaps consider these organizations lucky, or prepared, since no major incident has happened. Even though no attacks have made any significant costs on these organizations, the proactive work of preventing threats must cost more than one could think. The empirical findings show not only that almost all of the respondents have chief information security roles, but also many technological capabilities, such as MFA, jump server, ETDR and much more, as well as threat hunting teams. Furthermore, since some of the respondents have departments dedicated towards security, all the measures put in place must be a big cost for organizations. These thoughts are however more applicable towards the bigger organizations, considering that small organizations do not have the same proactive measures as the rest of the respondents, but still there were no threats recognized as the literature suggests (Pyöriä, 2011).

The literature mentions five common security standards and frameworks that are extensively used among organizations, which have given them the nickname *"the big five"* (Susanto et al., 2011). In the empirical result many of these standards and frameworks were recognized, but not as used as one would assume. Most respondents recognized, partly used or tried to get certified with the ISO27001 standard. Although NIST was not mentioned in the literature as one of the big five (Susanto et al., 2011), the empirical findings mentioned it more than first anticipated. Furthermore, a majority of the respondents ranked NIST higher than all the other standards that were mentioned. Some frameworks were also used depending on industry which walks in line with how Susanto et al. (2011) describes them. Empirical findings also showed that NIST could be seen as too extensive, which could be a challenge. Even though the literature mentioned ITIL's security management framework and COBIT as common practices for security (Susanto et al., 2011; Sheikhpour & Modiri, 2012), none of the respondents thought they were of value for their security work. It could be argued that this is because both ITIL and COBIT handle much more than just security, which means that they could be overwhelming to use for cyber and information security work when others are more specific to only cyber security work. Even though a lot of standards and frameworks exist, the empirical findings show that many respondents work with their own frameworks that sometimes are influenced by those mentioned in the literature, and others. What also could be assumed is that if an inflation of standards exist, confusion might eventually occur on how to work with security both in the cyber world, but also for physical assets. With teleworking becoming more of a new norm for organizations (Evangelakos, 2020; Babulak, 2009), one could also think that an emphasis could be placed on developing a cyber security standard for how to telework.

The empirical findings furthermore shows that the standards and frameworks shown were more used for strategic work, and not for handling threats directly. One interesting insight in

the empirical findings also shows the big role of regulations and legislations when handling cyber security, which the literature does not mention (Susanto et al., 2011). Not only does the empirical findings show that one has to account for international regulations, but also country specific in how to handle, for instance, cross border traffic of data. One would perhaps assume that when looking from a technical perspective that the literature would mention industry specific regulations for standards and frameworks. However, the standards and frameworks in the findings were seen as wider, which is why one could assume that some of the respondents only used them partly.

One assumption prior to the empirical research was to find some correlation between the type of framework and standard that were used and the kind of malware attacks that the respondents organizations suffered from. This was however difficult to see, since all respondents agreed that credential harvesting/phishing was the top threat and most of the threats mentioned in this thesis were not seen as a problem, even for organizations that did not follow any framework or standard. Almost all respondents used Office365 and relied on their solutions for security to some extent. Scepticism of the safety of the service existed among some respondents, but they still used it.

The empirical findings show that the cyber security practices that the literature review mentions were used to some extent by all respondents. The most mentioned practice was MFA, which corresponds to Kim and Hong's (2011) claim that it has increased in popularity. This is something that is understandable, since more risks exist today in different online environments, and to make sure that one's device, or a user's credentials, stay safe is imperative. One can understand that MFA is crucial when teleworking is scaled up, since more devices are connected, more services are in use and employees need to connect to cloud services or internal applications from different locations. Empirical findings mention that traditional anti-malware software was more or less useless, which is a different view from Rathore et al. (2018) that claims that anti-malware software is more important than ever due to the growth of malware attacks. Perhaps Rathore et al. (2018) count all kinds of anti-malware software, however, some respondents clearly argued against traditional practices.

What is commonly mentioned in the literature is the importance of VPN to ensure safe teleworking (Abukari & Bankas, 2020; Rikitake et al., 2001; Evangelakos, 2020). The empirical findings show that all the respondents use VPN, which could be argued as a natural response to ensure safe teleworking, since it has historically worked well for organizations of all sizes. Evangelakos (2020) describes, however, the risks that can occur when using VPN, which makes it interesting to see what practices the respondents use that are not mentioned in the literature. The empirical findings mentioned the use of VTS, which seems like one of the better practices to ensure safe teleworking, which is similar to what Downer & Bhattacharya (2015) mentioned as desktop virtualization models. Since it was rarely mentioned in the findings it could be seen as unknown for the rest of the respondents, cost too much or are inefficient to their organizations, but of all the practices it seemed arguably like the best one. This practice seemed to work best when an organization had applications on-premise, which could also be a factor to why the rest of the respondents did not use it, because they are more cloud based. This means that their security work is becoming more and more reliant on their cloud providers, which in the future might become a problem of trust, since more conservative organizations might not accept cloud providers to store data on their servers.

Nastase and Ionescu (2011) argued for establishing a computer security incident response team which Evangelakos (2020) said to be too expensive for organizations. There does not seem to be a consensus in the literature, but the empirical findings show evidence that having teams dedicated to proactive cyber security work can be beneficial. One respondent mentioned a red team that tries to penetrate their own environment, and other respondents seem to have other teams in place to handle cyber security threats from all angles. Since this view differs in both literature and empirical research, a discussion might spark again about the cost savings that might occur. What can be stated from empirical findings is that the bigger an organization is, the more threats come their way. As stated earlier, attacks on organizations cost a lot, which makes these response teams worth the cost. Yet, Evangelakos (2020) argues that it can be too expensive, but the cost if one breaches an organization's home environment might be considerably more. This trade-off is worth thinking about, since smaller companies perhaps do not feel the need to invest in cyber security as much as bigger companies.

5.3 The Risk Tolerance Aspect

Yang et. al (2013) argue that organizations that have teleworking staff need to be sure they know about the risks associated with teleworking, but also that they have solutions to handle the cyber security risks. Evangelakos (2020) says that organizations that are not prepared for the mentioned risks, have a harder time handling situations like Covid-19 when teleworking becomes forced. All the respondents from the interviews say that their organizations were fairly prepared for letting the employees telework even though new risks came along. The most complicated consequence for the respondent organizations was the big scale up. It is interesting that all the mentioned respondents and their organizations were well prepared for a situation like Covid-19 when the literature mentioned it as a crisis for organizations (Belzunegui-Eraso & Erro-Garcés, 2020). Belzunegui-Eraso and Erro-Garcés (2020) say organizations had a lack of contingency plans and Evangelakos (2020) argues organizations were not prepared. One could argue that there also is a difference between how the literature mentions the transformation from office work to forced teleworking in comparison to the empirical findings. Belzunegui-Eraso and Erro-Garcés (2020) mention that the organizational movement towards teleworking takes longer than expected whilst all the respondents say that the movement was smooth and not too challenging. Moreover, the respondents could enforce the movement to being a teleworking organization from one day to another which cannot be explained as a long term transformation (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020).

Pyöriä (2011) argues that security issues exist for organizations when teleworking but it is also mentioned that it especially covers smaller companies as they have less expertise and resources. Out of the five interviewed companies, only one can be considered as a small organization, with less than 50 employees. In this case, where the five interviewed organizations believe the transformation from office working to forced teleworking was not too big of a challenge, the sizes of the interviewed companies could affect the situation. If it would have been other companies that were interviewed, one could guess that the result could have been different. Smaller organizations have less resources for handling cyber security risks and can therefore encounter more threats. Belzunegui-Eraso and Erro-Garcés (2020) describes the situation that occured for organizations when Covid-19 appeared as a crisis. The organizations of focus for Belzunegui-Eraso and Erro-Garcés (2020) were of similar character and size as the

respondent companies of this thesis. The respondents of this thesis did not see Covid-19 as a cyber security crisis, instead they saw risks and challenges that were possible to handle. This can also be a consequence of what industry each company is figuring within. Vrchota et. al (2020) describe that some industries were more open to telework before Covid-19 than others and that the prepared companies had already adapted to the style of teleworking. On the other hand, Vrchota et. al (2020) argues that teleworking and other effects of the pandemic resulted in great cyber security risks for organizations of all sizes, both small- and big. The five companies of interest for this study are active within different industries but have a similar view on the situation, which one could argue is different from what Vrchota et. al (2020) say.

The empirical findings show that organizations cannot use forced teleworking whenever they want, particularly because they often deal with production lines where employees must be physically present. Such cases are obvious and can be noticed in the empirical findings, yet again, the difference in how full teleworking organizations and partially teleworking organizations feel about forced teleworking does not change much. While it is made possible to force teleworking for any organization, new risks, however, became more visible for all of them. Vrchota et. al (2020) describes the situation not as a crisis situation as Belzunegui-Eraso and Erro-Garcés (2020) describe it. Risks with forced teleworking show that it becomes even more important to understand information classification. For example, those that work with sensitive information and are forced to telework compared to those that work with less sensitive information. While this has been visible in our findings, studies like Yang et. al (2013) confirm it. More importantly, risks based on the sensitivity of information found across the empirical findings show a clear difference that they are information-related security risks rather than cyber security-related risks. For example, sensitive information can be seen on physical papers and overheard from people listening to phone calls when forced teleworking changes their work setting that can be from places where the worker does not have time or the means to consider security. However, it has to be noticed that information security risks of this nature can lead to cyber security problems as a sequence of the leaked information.

This risk is being handled by most of the organizations with employee training as they believe user training is of highest importance for handling risks that are difficult to handle when employees are forced to telework. User behaviour is according to some respondents possible to affect and that is more important than the technology side. On the other hand, the literature says that this problem is difficult to handle when it comes to a larger scale (Yang et. al, 2013), All of the respondents have or had a majority of their employees teleworking which one could say is of large scale. Still, they see the threat as possible to handle, in this case with employee training. As Evangelakos (2020) mentions, it is difficult to change an organization's cyber security landscape over a night, it is something that takes time to do. This was not applicable for the mentioned organizations as they all were prepared for letting their employees telework. Most respondent organizations did however do some small changes in their setup to enable the big scale up when employees had to work remotely. These changes seem to not have affected the daily operations for neither mentioned company, meaning the cyber security changes might have been small enough in comparison to the changes Evangelakos (2020) describes. The reason for the difference between literature and the empirical findings can be explained with the fact that the interviewed organizations were well prepared for a situation like Covid-19. Another reason is that all the organizations already offered teleworking possibilities to their employees to different extents. The literature did not focus on this as a positive aspect for organizations, even if literature talked about the growth of teleworking for organizations worldwide. If the transformation towards being a fully teleworking organization

would have taken much time, it could have been considered as a crisis for the organizations, but with Covid-19 it was smooth for all five organizations (Evangelakos, 2020; Belzunegui-Eraso & Erro-Garcés, 2020).

Two of the respondent companies think employees with more knowledge about cyber security could be more risk taking when using ICT- and IT tools. This means employees that know more also take bigger risks. Liang and Xue (2009) argue that an IT-user with greater cyber security- and teleworking knowledge might have a higher tolerance than less knowledged employees. This tolerance can have a negative influence on IT-threats as employees can expose the organization to risks and threats even though they have knowledge about it as they are comfortable and tolerant (Liang & Xue, 2009). One could argue that there is a similarity in what Liang and Xue (2009) say and what some of the findings show. There could be a possibility here with extra education to knowledgeable employees on the additional threats that comes with knowing more about cyber security. These types of training are not offered by the interviewed organizations as of today. On the other hand, some respondents mean employees with more knowledge are more suspicious and ask questions to the cyber security department to ensure they are not being tricked by social engineers. Moreover, the same organizations argue that different parts of their organization have different knowledge about cyber security, meaning there is a knowledge gap within the organizations. One could argue that this is an interesting finding as it is the same companies that think knowledge workers are more risk taking and tolerant, in line with Liang and Xue (2009). This could mean organizations with knowledge gaps within cyber security also suffer from extra risks when knowledge workers are too risk taking.

It is difficult to find similarities between what departments that are being exposed to most cyber security attacks and what departments that the respondents think have most knowledge about cyber security. The empirical findings show that employees within customer facing teams as well as top management together with the finance departments are suffering from more attacks than the others. Findings also show that only the security employees and the engineers have more knowledge than other employees from the interviewed organizations. On the other hand, hackers might know that top management, finance and customer facing teams are not any specialists within cyber security, and therefore they are easier to target. One might argue that the cyber attackers are targeting differently depending on what goal the hackers have with the attack which is in line with some findings. Whilst the literature did not focus on any specific organizational group as easier to hack, some of the respondents target older employees as a bigger risk. Some respondents mention they employ younger people than most other organizations and that this younger generation has grown up with cyber security threats being present since young ages. Moreover, older employees have a harder time changing from one digital behaviour to another and might also be an easier target for phishing attacks. This is an interesting finding as multiple respondents believe they have to educate the older employees more than the young staff, seeing a bigger cyber security risk in the uneducated. This might lead to a younger employee group being employed to jobs that involve work with potential cyber security risks. In this case, less education is needed for young, newly employed staff which of course is a cost saving for the organizations.

5.4 Key Implications to Research and Practice

While the literature (Liang & Xue, 2009; Griffith & Dougherty, 2002; Gupta and Sharman, 2009) shows that the Technical, Social and the Risk Tolerance aspects are essential to understand how security practices, technological tools and an individual's characteristics plays a big role in order to understand threats and risks for cyber security, the regulations have not been highlighted to the same extent. Therefore it would strongly be suggested that the Technical aspect and the Social aspect particularly include regulations as an integrated part of the processes that happen in developing security practices, rather than something independent or detached from these processes. For practice, regulations matter more than one assumes. *Therefore, it is essential that guidelines for security practices in organizations show that regulations should be proactively envisioned, but especially depending on what industry an organization is active within.*

An implication to research is the new trends that the respondents have spotted within social engineering. If the literature discussed these topics as well it could lead to *organizations being more prepared for the new ways that social engineering acts and could help them to predict and prepare for future threats.* An implication to both practice and literature is the fact that modern communication tools that become more popular with time are efficient for productive teleworking but not for social interaction. *Literature needs to consider whether this negative social consequence can lead to cyber security threats and risks as a result of less focused and satisfied employees.*

Although the costs of cyber security threats and risks are extensively discussed in the literature (Evangelakos 2020, Abukari & Bankas, 2020; Morgan, 2020), it is important to highlight the costs of the proactive work to ensure that an organization stays safe. None of the respondents seem to have suffered from great costs of attacks, but many of the respondents spend a tremendous amount to ensure nothing happens, *therefore it is crucial for the literature to consider the tradeoff between costs of proactive measures for cyber security and costs if an actual attack happens.*

Moreover, it is also important to recognize the fact that literature, such as Belzunegui-Eraso and Erro-Garcés (2020) describes forced teleworking as an organizational crisis as a reason of Covid-19, none of the respondents considered their organizations to be in a crisis, but rather found themselves in dealing with risks. It is important to recognize the difference between risks and crisis because risks can be foreseen and overcome, however, being in a crisis can halt organizational operations. *It is therefore imperative for the literature to distinguish between risks and crisis situations and that they are not the same from a security perspective.*

Lastly, an implication to practice is the relation between knowledge workers and risk taking behaviour. If an employee knows more about cyber security, there might be an increase in risk taking behavior from that employee, which could damage the organizations in line with what the Risk Tolerance aspect says (Liang & Xue, 2009). Not all organizations in this study agree on this fact, but still, all interviewed organizations thought this question was very interesting as it is something of value and truth in it. Neither respondent had thought about this question or the mentioned correlation before which is interesting as literature mentions it and some respondents found it true. *Therefore, a possibility exists for literature to execute whether or not knowledgeable workers are bigger threats for organizations or not as different respondents argue for opposite meanings.*

6 Conclusion

In this thesis, the objective to address cyber security risks and threats associated with forced teleworking is answered on the basis of the following research question: what cyber security risks and threats are there for organizations associated with forced teleworking?

From a social point of view, social engineering is the biggest threat for organizations when teleworking is forced, since employees are seen as the weakest link, which organizations seem to solve through training and education of employees. The importance of training and education is paramount for an organization's awareness towards cyber security threats and risks. Moreover, the trends of social engineering seems to have changed and been more updated compared to before. The effects of forced teleworking seems to have an impact on employees health, which consequently could lead to cyber security risks and threats. They do however execute the practice plan for mobile devices, for instance Zero-trust, which works as a precaution to handle an organization's device being out of office when teleworking. All organizations also seem to have been prepared workwise for this forced teleworking period, but not socially, which means that technical tools cannot replace the social contact one achieves at the office.

This study shows that immediate threats in forms of malware attacks have increased during Covid-19, however the threat level has been, more or less, similar to times before forced teleworking. An increase in phishing attempts has not had any consequences towards any organization we have interviewed, regardless of standards and frameworks used. Even though prior information points towards risks and threats for organizations with forced teleworking, all findings show it was nothing more than a scaling problem, which was solved smoothly. The respondents do however see an increased risk when an increased number of employees are being forced to telework, these risks are however manageable. Moreover, the risk of high cost from malware attacks does not seem to be considered a threat, there are however a lot of resources invested in proactive measures to keep organizations safe, especially for the bigger organizations. Also, country specific regulations and legislations are important to consider when looking at risks and threats, since it can partly determine what practices, standards and frameworks that can be used to ensure safe teleworking.

From a Risk Tolerance perspective the forced teleworking period during Covid-19 cannot be seen as a cyber security crisis, but rather a risk, which needs to be clearly distinguished in both literature and practice. The more knowledge an employee has about cyber security threats, risks and practices, seem to have a correlation with a more risk taking behaviour, which in turn can be seen as a risk or threat for teleworking organizations. Furthermore, while there can be differences in risks and threats depending on industry, this study shows that there are no differences, whether it comes to size or type of organization. What can also be seen is that those departments that are exposed to most threats and risks are the top management and the finance departments. Moreover, the older employees in organizations are also a bigger threat in terms of social engineering than the younger and more tech-savvy employees. Lastly, the risks are more determined by employees' home environment, where information can be breached, or other people in one's home that can accidently put an organization at risk if someone that is not supposed to use their computer will use it.

Finally, the Social, Technical and the Risk Tolerance Aspects were all relevant to apply when answering the research question as they correlate and give the opportunity to involve important sub aspects that are relevant for all kinds of organizations that are teleworking.

6.1 Future Work

This thesis shows that research within the field of teleworking should increase. Due to the fact that forced teleworking, as a result of the Covid-19 pandemic, is rather new, lack of research in the field is natural. When investigating the research question, it is found that further research can be done regarding the difference between actual teleworking and forced teleworking. One could also say it would be interesting to investigate other aspects than the ones this thesis have looked into, as well as their relationship to forced teleworking. In this study, none of the respondents claimed that they have suffered from great costs or suffered from a crisis related to cyber security. In contrast, it would be interesting to further investigate organizations that have been victims to large cyber attacks and then compare them to the organizations of this thesis that have not suffered from problems with cyber attacks. Lastly, in years to follow after Covid-19 pandemic, it would be interesting to investigate how forced teleworking affected organizations' cyber security in the long run and whether new and dominant aspects would explain the causes better.

Appendix 1

Interview 1 (I1)
Company: Waboba AB
Interviewer: William von Heland - W.H
Respondent: Axel von Heland - A.H

Row	Person	Question & Answer	Code
1	W.H	To begin with, what is your name and role at Waboba?	
2	A.H	My name is Axel von Heland and I am the CEO of Waboba AB which is the group company, we have two subsidiaries.	
3	W.H	Okay, nice. Is Waboba teleworking as of today?	
4	A.H	Yes, in Stockholm we have around 30 percent attendance in the office, whilst in China everyone is in the office now back and in the US they are mainly in the office as they are based in Atlanta, in Georgia where there are not too much restrictions.	S-T-FT S-T-TT
5	W.H	Okay, and I know that you had the possibility to telework even before the pandemic as you are very spread out over the world but when did this start with the teleworking?	
6	A.H	So, in China they started by the Chinese new year which was in end of February, so they were home for all of March I believe and then they came back quite quickly and in Sweden it has been more, if you need to come in, come in, otherwise stay home, that started around April or May 2020.	S-T-FT S-T-TT
7	W.H	So, you would not say it is forced but it is a recommendation?	
8	A.H	Yes exactly, the Swedish model haha.	S-T-FT
9	W.H	How many percent of the employees are teleworking now on average?	
10	A.H	That is a good question. In China it was one, two months were all of them teleworked and then they were all back pretty much, in Stockholm 70 percent teleworking.	S-T-FT S-T-TT
11	W.H	Okay, let's move on. We have focused on three aspects for this thesis, it is the Technical aspect, the social aspect and the Risk Tolerance aspect. And we would like to start with the Technical aspect	

		and start with asking you what challenges and threats do you see with forced teleworking in an IT security perspective for your organization?	
12	A.H	Well so compared to the day to day office work, also before, we have a lot of phishing attempts constantly. It can be emails that look like they come from me and it is like, why is this amount to this account and even though we are catching this now, because it is still quite obvious, I mean when we are all in the same office it is much easier to just ask the question, is this something you sent or is it not. And if you are away from the office you can't really answer that question directly and since it is very urgent every time to transfer the money, maybe someone could do that. That has not happened but could be seen as a concern or threat, for us as we are quite spread out, these decisions have been made in a teleworking environment before too. We are spread out in a lot of different offices so our day to day work is on a digital basis anyways.	S-CS-SE T-CS-MA RT-T-ET RT-SPO-CP T-SPO-CP
13	W.H	Okay, have you had any problems with some kind of malware attack? You mentioned phishing?	
14	A.H	Yeah, so I think phishing is the most common one or at least the easiest one to detect and that is quite regular and I think that gets more and more sophisticated in that they (hackers) know the roles of the ones in the organization and they know how to send too. Usually they send emails from me to the CFOs and then we have had factories that have had email addresses stolen and then hackers have logged in there and they have sent invoices from those factories. So that has happened during this time, since March 2020 but I am not sure it is connected.	T-CS-MA S-CS-SE
15	W.H	Is it a problem handling those issues or do you have like systems that can detect if it is a phishing attack or such?	
16	A.H	I mean we are relying on external systems, we have office 365 from Microsoft that filters out most of it, but the things that get through I mean people are so used to it so it is not really a big problem, I mean people know that don't ask someone to send money, they know that you don't do this. With common sense you come a long way even with these phishing attacks, but we are talking about it as they are becoming better and better so sooner or later there is not gonna be too obvious, they might ask things that are a little bit less obvious and things that lead to something instead of asking directly.	T-SPO-CP S-SPO-CP RT-SPO-CP
17	W.H	Okay, and have you seen an increase in the number of attacks since March 2020?	

18	A.H	Honestly I don't really know, it is not something I have thought of. But it is one thing I wanna add on that we do and that is if someone sees something that is suspicious we reach out and then we reach out in a different channel, so we always have different channels to make sure if we get a suspicious email then reach out by phone or this to confirm. So we don't have sophisticated methods but I think right now it is enough for us.	T-SPET T-SPO-CP S-SPO-CP
19	W.H	Okay, let's move on. Our next question is, can you rank these types of malware attacks regarding threat for your organization when teleworking, please rank them from top to bottom. We have viruses, ransomware, phishing, spyware, trojans, adware and fileness malware.	
20	A.H	Okay yeah so I think phishing is the top one for us together with business email compromise. They are basically the same in my point of view and when we get phishing emails, at least the ones that tend to be successful, they always look like they come from us. But they are not compromised in the sense that no one has hacked my account, but it looks like it comes from my email address instead of somewhere else. So that is the main threat I would say. I mean we a lot of malware or viruses or trojans or worms, I have not really checked myself haha, but it is being sent to us in different forms but they are still not a big threat as I think most people are used with not clicking on attachments that are usually web links that you don't wanna go or we have a lot of these you know voice calls emails with what I suspect being some kind of malware. But still, I don't think they are too problematic and when I look at a compromised account in our organization we don't have any so it does not seem like, I mean it might be viruses on the computers, that is nothing I know but at least they are not getting in on our systems, that is something I know.	T-CS-MA T-SPO-CP RT-SPO-CP
21	W.H	Okay and I know that you handle a lot of personal information as you work with clients all over the world that buy Waboba products, is it any hackers trying to get that information, trying to get that personal information regarding your clients if you understand what I mean.	
22	A.H	I don’t think we are targets of that yet, I hope to become big enough where we get to that level but I think right now, no we don't see that sort of activity at least.	R-T-ET
23	W.H	Are you using any cyber security standards and frameworks to handle the cyber security threats from teleworking?	

24	A.H	That is a very difficult question for me to answer as I don't really know what standards there are but I think in general the main thing that we are using is just common sense and just check and then in terms of security when it comes to passwords we enforce multi factor authentications on all our services to make sure that even if passwords leak we are safe from attacks because that is the biggest problem that we have had before that people have passwords that are not too good into their accounts with us and then they use the same passwords for elsewhere and then that goes out in the open and then we have a problem.	S-SPO-CP R-SPO-SF T-SPO-CP
25	W.H	Have you heard of any of these cyber security standards? ISO20700, ITIL, COBIT.	
26	A.H	No	T-SPO-SF
27	W.H	So it is nothing you look into and actually follow to strengthen up your security?	
28	A.H	No	T-SPO-SF
29	W.H	Then we can move on. What security practices do you use to ensure secure teleworking for your employees? You mentioned multi-factor identification. Is it anything else you use to ensure safe teleworking?	
30	A.H	No I don't think so. It is pretty much it.	T-SPO-CP
31	W.H	Okay, I can go through eight practices that we have found in literature and see if you use any. Do you have firewalls?	
32	A.H	Yeah but built in to different services, like everywhere in the gateways, routers and computers.	T-SPO-CP
33	W.H	Okay and do you have documented cyber security policies for your organization	
34	A.H	No, or well that depends. Usually when people say policies and documents I see this long laritine but for us it is more like use common sense, do this if something happens then and yes, it is documented in one way, I mean we tell people specific things.	S-SPO-CP
35	W.H	Okay and that maybe leads up to the next question which is, do you have education for your employees?	

36	A.H	Yeah	S-SPO-CP
37	W.H	Do you have a plan for mobile devices or bring your own device?	
38	A.H	No	T-SPO-CP
39	W.H	Do you have regular backup of data?	
40	A.H	Yes	T-SPO-CP
41	W.H	Do you have installation of anti-malware software?	
42	A.H	Yes but actually now it is pretty much included in the systems. But we don't have any anti malware system for browsers and such, we don’t have that.	T-SPO-CP
43	W.H	It is already installed in Office365, is that what you mean with included?	
44	A.H	Yes, usually for these kinds of systems you know both the operating systems you will have some kind of a protection already pre-installed.	T-SPO-CP
45	W.H	Yes, and then you have multi factor identification as mentioned before	
46	A.H	Yes	T-SPO-CP
47	W.H	We can then move on to the next section. Have you used any specific cyber security practices to handle the forced teleworking? For example DNS filters, VPNs, BAS or such?	
48	A.H	No we have not	T-SPET
49	W.H	So no VPN tunnels to...	
50	A.H	Ah okay you mean VPN connections to our, well we don’t have those kinds of servers so that is not relevant for us.	T-SPET
51	W.H	Then we move on to the Social aspect which is more focussed on the people and employees. The first question is what is your	

		organizational take on social engineering? Is it a big problem for your organization?	
52	A.H	Not yet, I think it's going to be a bigger problem for our organization too in the future. But as I said I don't think right now that we are a target for these kinds of things but I think more and more people are doing these sorts of activities and they are targeting smaller and smaller companies.	RT-T-ET
53	W.H	So you think you are not a target right now because of the size of the company?	
54	A.H	Yeah, I don't think they see enough value yet but they look for less and less value.	RT-T-ET
55	W.H	Okay so you don't think it is like you will grow so much so that you become a target, it is more like they are going down in the target list, looking for smaller organizations.	
56	A.H	Yes and I mean it depends on how you see social engineering because one could say they have our organizational chart already because they know what emails to send now etcetera. So you could say they have some of it, it depends on where you draw the line. Some are reaching out through LinkedIn to do like maps but we don't see too much activities like this yet.	S-CS-SE
57	W.H	Okay, so hackers are not trying to use your employees to reach internal data and systems?	
58	A.H	No	T-CS-MA S-CS-SE
59	W.H	Do you give training and education to the employees to minimize the threats from social engineering and how often?	
60	A.H	No but we probably should	RT-SPO-CP S-SPO-CP
61	W.H	Okay so you have not added any extra training due to the forced teleworking since march 2020	
62	A.H	No	RT-SPO-CP

			S-SPO-CP
63	W.H	How has forced teleworking affected the employees of Waboba? Do they have to work in a different way now? Let's say for the swedish office.	
64	A.H	Well yes and no. It affected a lot in the social sense of course, I mean you have fun, from a workflow perspective it has not affected much as all of us here in Stockholm are working with people from other offices so the interactions within the office is generally more social than work related. So from a work perspective I believe we handle it quite well, but then I don't know the long time effects of a social perspective, I mean I am quite worried that people are getting less and less motivation, you don't really get the energy that you get from working together.	S-T-ET S-T-TT
65	W.H	I understand that. But do you have any different ways of working now or do the employees have to add an extra step to reach your internal data when they work from home for example?	
66	A.H	No, our services are online to begin with, they are on the cloud and not on site, so they are connecting as usual	T-SPO-CP
67	W.H	Alright, then we are going to the last aspect which is the Risk Tolerance. Was your organization prepared for letting the employees telework when covid-19 came?	
68	A.H	Yes, as an organization, work related yes.	RT-T-ET
69	W.H	Okay and do you see an increased security risk when an increased number of employees telework?	
70	A.H	Yes from the phishing aspect mainly	RT-T-ET
71	W.H	So the scale up when you go from only having like a couple of employees teleworking to having 50 percent or 70 percent, that scale up is actually a security risk?	
72	A.H	Yeah and I think it is easier for me to draw conclusions from what happened in China instead because in Stockholm we are not too many anyways and I mean it does not really affect us in any way but in China when everyone worked from home we had significant changes, everything takes more time and also decisions that should happen, don't happen and that could be security risks in itself and then all the phishing attempts that I mentioned before that you	S-T-ET S-T-TT S-T-FT

		cannot check them with the person next to you, it is easier to fall for some.	
73	W.H	Okay and what level of understanding would you say your employees have on the threats that might occur when teleworking?	
74	A.H	I think they have a good understanding, everyone, because it is something that they have been subjected to for a long time, all of their lives, I mean we employ people in generally in ages that are quite used to these sorts of threats so I think the things that we are seeing within our organization is a little bit specification but it is still very recognizable for most people as it's a good difference.	RT-T-ET RT-SPET S-T-ET
75	W.H	Also, I know as you mention that you have what we could say is young employees compared to many other organizations, do you think that is a difference to if you would have a totally different employee group?	
76	A.H	Yes, I mean we notice that we have a different group in our US office for instance and I am talking much more to them about this so yeah it would be a big difference.	RT-SPO-CP S-T-ET
77	W.H	So you could say that in this case, the American office, they are more of a security threat or risk than the Stockholm office	
78	A.H	They are yes but they have also not been teleworking really as it has not really been enforced in Atlanta	RT-T-ET
79	W.H	Interesting. Would you say your employees know about your concerns and how you work with security practices? How do you handle cyber security?	
80	A.H	Yes I would say. Usually 3-4 times a year something new comes to my inbox in terms of these threats and then I always post them to everyone so that everyone can see what threats there are and also when we get notifications about threats from our Office365 I tend to bring them up whenever there is something of interest and then with the multi factor authentication setup of our services we had to go through a lot, mainly with the US office because they thought it was big pain.	S-SPO-CP RT-SPO-CP T-SPO-CP
81	W.H	When did you implement the multi factor authentications?	
82	A.H	In a couple of steps so actually it was during this time coincidently we did it for our own systems, so we use internal systems which started to enforce multi factor authentication this year. In our	T-SPO-CP

		office365 systems we have implemented it in steps going back three years.	
83	W.H	Okay great. Last couple of questions. Do you see a difference between the departments of your organization about the knowledge about cyber security?	
84	A.H	Maybe not so much the departments. Well of course we have people that are employed like in IT and they are more familiar with all of these things and there I see a difference but on a department level not so much. It mainly comes down to age and that stands for all the departments.	RT-T-ET S-T-ET
85	W.H	Okay and we talked about this more before about the country difference but is there a big knowledge gap between countries like USA, China and Sweden for example?	
86	A.H	No I don't think so or to me people within the same age group have the same knowledge wherever they are in the world it seems so it is more of a generational gap for us.	S-T-ET RT-T-ET
87	W.H	And what departments seem to be more likely to get attacked?	
88	A.H	It seems like the finance department is something that they are more interested in for reasons haha.	RT-T-ET
89	W.H	Haha a lot of fake invoices	
90	A.H	Yeah, a lot of fake invoices and other things.	T-CS-MA
91	W.H	Okay and lastly, do you see that employees with more knowledge about cyber security in teleworking are more risk taking than the ones with less knowledge?	
92	A.H	No, I don't see them as more of a threat risk. I think they use more stuff and systems but I think they generally use them with care than required so I would say that people that are less informed about the risks are usually the ones that would do things that you should not do.	RT-SPET RT-SPO-CP S-SPO-CP
93	W.H	Okay thank you for today!	

Appendix 2

Interview 2 (I2)
Company: Sveriges Television AB (SVT)
Interviewer: F.S = Fredrik Sundström
Interviewer: W.H = William von Heland
Respondent: D.E = Daniel Ekelöf

Row	Person	Question & Answer	Code
1	W.H	What is your name and role within the Swedish Television?	
2	D.E	I am Daniel Ekelöf and I am the head of distribution and cyber security. Distribution is how we reach the audience, so the DTT, the cable network, it is our streaming services in SVT play, it is basically how all the programming reaches the audience. And then I also have a role in cyber security, part of that is because it is linked to distribution in a traditional way and that is what we need to protect as a whole and that we reach the audience in times of crises or other difficulties, so that goes quite well with that assignment but also cyber security is obviously bigger than just distribution. It is also supporting the rest of the organization on best practices and how we work generally.	
3	W.H	Okay, and what is the official title for your role?	
4	D.E	Head of distribution and cyber security.	
5	W.H	Is the Swedish Television teleworking as of today and if so, when did it start and is it forced and if you know, how many percent of the employees are teleworking approximately?	
6	D.E	Yes, we are teleworking. It has been ongoing for a while, for several years but that is why it is interesting when you say “is it forced”, because, yes, but there were a lot of people that did it before as a matter of flexibility and availability and also support people on call and things like that. That was voluntary and worked very good with the way we work. The forced part came as you say in March 2020 when we basically forced, we did actually force a lot of people to not come into the office, saying we don´t want you here, because of the pandemic and that became forced. And then of course there was a lot more than the people doing it on flexibility on a Thursday afternoon and the whole Friday and stuff like that. So that is the big shift. I would say before it was like 5-10 percent teleworking on a regular basis and now it is above 50 percent. So we are not a full remote, forced teleworking, basically because we cant as a lot of the things	S-T-TT S-T-FT

		we do are not really possible to do from distance, through teleworking yet. You can imagine things like recording a TV show, where people are in the studio, and things like that. And then we also have a lot of infrastructure that is not really IT based or connected to the internet so you need to be on the premises to manage that.	
7	W.H	Great. Let's move on to the next slide which is our first aspect of the three main aspects that we focus on in this thesis and that is the Technical aspect. Up in the right corner you can see a definition for Malware that we have used. Our first question is "What challenges and threats do you see for your organization when teleworking, in an IT security perspective"?	
8	D.E	So, I think the biggest issue with the forced setup is scaling and all of this is kind of linear in the threat landscape so basically if you have five to ten percent working from home, doing specific tasks, that is one challenge, if you need to have 50 percent plus working from home doing all other kinds of tasks, you get a new challenge, so basically it is a scaling problem and it is like statististics right, if you have two people working from home it is quite often the same people that worked from home before that were a little bit more IT savvy and used to working remotely and now we have everyone basically working from home, so that itself is a challenge and increases the risk on the organization I would say. And also a lot of new tasks that we did not do remotely before, we have to do now from home, so we need to have more access to our own environments than we had before.	S-T-FT S-T-ET RT-T-ET
9	W.H	Okay. Have you had any problems with some kind of malware attack against your organization since March 2020?	
10	D.E	I mean, it depends on how you calculate, so basically there is an ongoing threat landscape all the time, like boots trying to knock on the door and see what is happening. There is spam and phishing happening all the time so in that sense of course we have had. I would say it has increased, especially the phishing and spam part, so that is always happening. Some of it, most of it does not really mount to anything basically because we either block it in the firewalls or in the email program but some of it gets through and we did have some accounts affected and some of our accounts started sending out spam and things like that. We also had a lot more, a little bit more intelligent spam and it was handled through support through our IT-security help desk and you basically block the accounts, you do all types of remedies. Regarding cost, I don't really have a cost that I know, it is mostly time spent like if you have a little bit more complicated attacks, it does that a lot of man hours for a number of people to go through it so of course that is a cost. But I don't have a number. And regarding what type of attack, it is all kinds but the mostly ones are	T-CS-MA T-SPO-CP

		through phishing and that can be malware or trojans and that is hard and this has increased I would say.	
11	W.H	Do you think that this specific attack that you mentioned or it might have been several attacks but do you think they would have occurred if it was not for teleworking?	
12	D.E	We have not seen a big shift in the types of attacks, I think it is just an increase. It could have happened but also the malicious hackers know that people are teleworking and know that they are less focused and in that sense it is probably more happening right now than before but it is not really that new yet. We have not had any specific like video calling attacks on Zoom or stuff like that, we did not use Zoom, we used Teams, and we have been so far, knock on wood, blessed with not having any specific teleworking attacks.	T-CS-MA S-T-ET S-T-FT RT-T-ET
13	W.H	And I think you already answered the last question regarding the increase of the number of malware attacks?	
14	D.E	Yeah	T-CS-MA
15	W.H	Let's move on. Here you can see a number of malware attacks that we have seen from the literature as popular or normal. Our question to you is if you can rank these types regarding threats for your organization when teleworking. From the biggest threat to the smallest.	
16	D.E	Few of them are combined. I think phishing is the most common. Through phishing you get ransomware, you get spyware and you get trojans. It is basically depending on what is the delivery method, so phishing and credential harvesting is the most common and people are just looking for different you know Facebook logins and things like that. And through those you can have trojans and spyware. A few years ago we had some problems with ransomware, so far we have kind of not been too affected yet, which is good. And again, a lot of them go together, worms and viruses and trojans, they kind of interfine. It is a difference in delivery meaning what's the method for getting in, and what is the payload and that depends. You probably need to separate them in that sense.	T-CS-MA
17	W.H	Let's move on. Are you using any cyber security standards or frameworks to handle the threats from teleworking?	
18	D.E	Yeah so we are looking at and using some parts of the ISO2071 standard, ITIL is not really a security standard, it is more on how you work with support, and change management. And the other ones we don't use. The other standard, one that we have been using is	T-SPO-SF

		NIST, it is quite similar to ISO27 but I think it is a little bit simpler so that is something to look at.	
19	W.H	Okay, so you mentioned NIST as the one that you probably use the most is that right?	
20	D.E	Yeah, NIST and then also, the thing is that you have to work together with cyber security and information security as a whole and it depends on where you come from, the information security people they usually like ISO more and it depends on where you come from. The infosec people usually like ISO more and the people in the other room like NIST more. So we try to use a combination of them. The important thing is that you have some sort of framework and methodological way of working together.	T-SPO-SF
21	W.H	Okay, I think we can move on as you have answered the other once as well. So what security practices do you use to ensure safe teleworking for your employees? You can start by answering the question overall and then we can move on to the once that we have mentioned down there.	
22	D.E	So what security practises that we use to ensure and then answering the question below right?	
23	W.H	Yeah you can go directly to that one. These are some of the practices that we have found in the literature and maybe you can answer if you work with these once or if you have any else and which ones are the most important ones.	
24	D.E	I would say that we work with all. With firewalls, education. And when you have a plan for mobile devices BYOD, it's basically when you don't have an SVT owned device. We also need to handle the SVT owned devices. You have to have all mobile devices handled in some way. Both our own, the ones that we own and give to our employees and the ones that just connect to the network. We have password policies and we have multi-factor identification. I think we have been ramping up the multi-factor and putting that up the last one or two years. Much more focus on having multi-factor than just having a good password. And we have some anti-malware software. Sometimes that's hard because we use quite specific industrial systems that don't really run on malware-software in the same way. And also it depends on if you are using Windows, Mac or Linux. So we try to work that out. One thing that I think is missing is that if you have a big network you usually want to have network segmentation so not all of the network are connected to each other and more importantly the whole network is not connected to the internet. You want to segment your network and separate it in different ways. And there are a number of ways to do that, firewalls are one different part. One thing that I can say is the difference between this forced	T-SPO-CP T-SPET

		teleworking and before is that a lot of the security parts in organizations, such as us, have been protecting our network to make sure that nothing gets in and once you are in the network it's pretty open to use so it creates a safe perimeter. And when you move into this teleworking scenario that perimeter is not so clear anymore and that's one of the challenges. So you have to start looking more on the device and protecting the device. Because the device becomes a way into your safe network.	
25	W.H	Okay, would you say that you have started to involve these practises more since march 2020? Or is it anyone that has been added up? Or did you have all this since before?	
26	D.E	So most of these were in place already before. I think we have put more focus on how to handle mobile devices, being both personal devices and company devices. And also, as I said, we re-focus a little bit on protecting the device. It's a concept that is a bit popular that is called Zero-trust. So basically when you don't have a clear perimeter of your network, because of the fact that people are home or wherever, you have to protect and authenticate the devices more clearly than if they only are on the network.	T-SPO-CP T-SPET RT-SPET
27	W.H	You said that maybe 5 procent tele worked before the pandemic from home and now it's almost around 50 percent so you had the standards for reaching the network since before it's not any new technical setup?	
28	D.E	Basically in the use of VPNs and firewalls, which we use, we also use office 365, so that's a cloud service for teams and mail and everything. That helped us quite a lot, having that already in place or VPNs where actually working quite well, we had to upgrade them a little bit but the capability was there. Again it's about the scaling, just making it work for hundreds of people instead of tens of people. And also the fact that people are not used to working from home, they can also make more mistakes. Like I said we did a little more focus on clients. We also had to update our policies more on which wifi is that you should connect to and which shouldn't you connect to, those kinds of practices.	T-SPET T-SPO-CP S-T-ET S-T-FT RT-SPO-CP RT-T-ET RT-SPET
29	W.H	Was it a lot of education for the employees involved in those new standards?	

30	D.E	In the beginning there was a lot of education both around the standards but also on which solutions that we should use. Because what happened in March was that when everyone went home they still had to do their job everyone starting to find their own different solutions on how to telework, how to connect to the internet, to the office, to work together in teams, so there was a lot of creativity on new solutions. And I think that our organization pretty much evaluated every single video telecommunication tool that existed. Like this doesn't have multi-duplex, we don't like the way that this one has emojis and everything. So there was a lot of discussion of what tools that we were going to use and why. And that's ongoing but that was really big in March/April.	S-SPO-CP T-SPET S-T-ET
31	W.H	Okay, interesting. So let's move on to the next one, that is the last one on the Technical aspects. You have already mentioned some of it but have you used any specific cyber security practices to handle the forced teleworking? For example DNS filters, VPNs, BAS, protocols or such.	
32	D.E	Yes, the DNS filter and VPNs we already had in place, that was more of a scaling discussion. And some internal work. Because you need to connect the VPN to the internal solutions as well and enable them to work remote. There has been a big increase of the use, we went from hundred a month to five hundred a day that worked on the VPN. Sometimes we had up to thousands of people that worked at the same time on the VPN so there is quite a lot of traffic.	T-SPET S-T-ET
33	W.H	Yes I understand that it is a big challenge. So when we come over to the social aspect, regarding the individuals and the group, what is your organizational take on Social Engineering? Is it a big problem for your organization? Are hackers trying to use your employees to reach internal data and systems etcetera?	
34	D.E	Yes so this is quite closely related to phishing. When phishing becomes advanced enough it's more social engineering than spam, it's somewhere where that spectrum is. It goes from you knowing it's completely fake to something that you are interesting in that you want to work with. That would be the most common social engineering. And take over of social media accounts, that also happens and it's a problem. I think it's very specific for a media company, as SVT, is that the role of the journalists is to seek information and they also get contacted by a lot of people. A woman, that I had a conversation with, a famous author, she said that the concept of not clicking on the link is completely useless since our whole job is to click on links, that's what we do. So for you as an IT department to say don't click on the links is like saying don't do your job. We have to have a different angle on that. So that's an interesting thing that we are trying to work with. People should be able to click on links,	T-CS-MA S-CS-SE RT-T-ET RT-SPO-CP T-SPO-CP

		but they need to be aware of the risks with it. So there are some discussions around that. And also much more links now come through the mobile and the sms once are people still not used to, they can still be phishing when you click on a link in an sms. Thats a tough one. Usually they are quite harmless, they are more about trying to phish for that specific individual's credentials than getting into our network basically.	
35	W.H	And we talked about this a little bit before but do you give training and education to your employees to minimize the threat from social engineering?	
36	D.E	Yes so basically, we did a big push on what teleworking tools that we should use and which not to use. We also used a company that I think is called Nano learning, where you have these short sessions in a few minutes with some questions and answers on how to recognize these things. So we tried to push them up. We should probably do it more often, but we have done that.	S-SPO-CP S-T-ET
37	W.H	Ok, and you mentioned that you had policies for employees on how to telework, to minimize the threat from hackers. Do you think that your employees know about these policies and actually have read them through so to say.	
38	D.E	Of course not everyone but I can say that less people have done it before the pandemic, because they didn't think it affected them. I think the awareness of people now, compared to one or two years ago is much higher, so there are much more questions, there is much more interest in how to use it. I don't think everyone has read all the policies but I feel it is a big increase in how interested people are and that most people actually want to do the right thing and that they ask more questions about these things now, which is good.	RT-SPO-CP S-SPO-CF S-T-ET
39	W.H	Ok, and that is also kind of a question on, the question how has the forced teleworking affected the employees of your organization?	
40	D.E	Uh, that is a very broad question, so uh, I mean from a security point yes. I think people are more aware, working better generally, I mean it's a huge effect on an organization that everyone has to work from remote and that is hard in so many other ways.	RT-SPET RT-T-ET S-T-ET
41	W.H	yeah ok and in a security aspect, or like viewpoint, do they have to work in a different way to get access to the network, for example…	
42	D.E	Yeah so we have done a lot of work on securing up the mobile phones, securing up the PCs, because we don't, before if you got in to SVT and sat down at your desk with your computer we had	T-SPET

		control of that inside the network and now we basically, you know, shut down some access of unknown devices. So we have to make sure all devices that connect to our network from outside are known and that includes mobile cell phones, we have done quite a lot of work on, you know, getting certificates and validating that it is the right device for both phone and PC, or laptop. So yeah, we have done quite a lot of those policies, we introduced that you have to use longer pincodes, more often you have to log in to get access to email and you can't mix your company email with your private email on your phone and things like that. We have done a few things.	T-SPO-CP S-SPO-CP RT-SPO-CP
43	W.H	Ok, thank you, and if we move over to the last one, which is Risk Tolerance. Would you say your organization was prepared for letting your employees telework, when Covid-19 came?	
44	D.E	Uhm, I don't think anyone was prepared but it was surprisingly smooth. We have VPNs, we have ways of doing remote editing, we already moved to office 365 so we had a lot of cloud enabled services so all in all it worked surprisingly well.	RT-T-ET T-SPO-CP T-SPET S-T-ET
45	W.H	And you said earlier that you see an increased security risk when you see an increased number of employees telework.	
46	D.E	Yeah it is like a scaling thing, right, the more people you have that are doing things that are uncommon, the more risk you have. Then also, you have more people not sitting in cafes now but being home on their own wifi and things like that is a higher risk.	RT-T-ET S-T-ET S-T-FT
47	W.H	And what level of understanding does the employees have of the threats that might occur when teleworking?	
48	D.E	In general it is not super high understanding. But I would say it is much more interest in the security practices, and curiosity, and they ask much more questions so I think they getting there	S-SPO-CP RT-SPO-CP RT-T-ET
49	W.H	But do you think they, or the employees have an idea of what frameworks and standards your organization follows?	

50	D.E	No, but I'm not sure they need to know which framework. What do you mean? I mean no one actually needs to know that we are actually using NIST, unless you are in the security department.	RT-SPO-SF S-SPO-CP
51	W.H	Ok	
52	D.E	Does that answer your question or?	
53	W.H	Yeah, yeah, because that is also the last question if it is important that the employees know about it but I totally agree with you that it makes sense that everyone shouldn't know. Or that is no better result if they know what standard you are using.	
54	D.E	No but I think it could be important that we are using a standard and that we are using this in a structured way, or that we are using best practices, because it can increase confidence in our work. But the actual standard itself is not that important.	RT-SPO-SF RT-SPO-CP S-SPO-CP
55	W.H	And the last questions here, do you see a difference between the departments of your organization about the knowledge of security issues and practices? Now when teleworking?	
56	D.E	Yeah, of course there is a difference, I mean you have differences within the departments as well. It has a lot to do with interest, but generally of course people who work in IT know a little bit more. Especially if they work with support or development, I think some of the journalists know quite a lot, because they have to protect their sources and are quite savy in that way. Some of the journalists are, don't really know at all, because they don't work with that but we have those really investigative journalists, probably a lot of them know more than I do about, you know tips and tricks of how to get sources, I mean not revealing your sources. And then you have people who work with entertainment programs, or drama and they don't have to worry about these things at all usually so that, of course there is a big lack of knowledge. Because they never had to use it.	RT-SPO-CP RT-T-ET S-SPO-CP
57	W.H	What departments seem more likely to get attacked and which departments suffer from more attacks?	

58	D.E	So I think IT-departments suffer from some, but other than that it is the news organization. Because some of them have high value information of course, for people to use and also their, as I said before, their jobs is to click on links and follow leads and review information so mostly them I would say.	RT-SPO-CP RT-T-ET S-T-ET
59	W.H	And if they press the wrong link you can directly through your security that you have close them down, the links or is it a problem that they have to find new fun facts. And they got of course a lot of links sent to them..	
60	D.E	I mean, so far we have caught a lot of things and we have a lot of help from the software we have on our computers, that you can block and if it is not a normality you can block, I think we need to get much better at that. Then some of these systems are quite advanced now that you don't see them straight away. And also the credential phishing is not really something that we see, because then you go to another site and you put in your own information right, that is not always something we can block. But if there is like a trojan, that is known or a virus then the system quite often picks that up.	T-CS-MA T-SPO-CP
61	W.H	And the last question, do you see that employees with more knowledge about security in teleworking are more careless, so that they take bigger risks?	
62	D.E	That is an interesting one actually, how did you come up with that? Because it is interesting, because in some parts it is true actually, and I'm not sure if I would be careless, but I would say that it is quite common that people who know more about security practices take more risks in that sense, that we would think are risks. Or maybe even break the policies that we have, sometimes because they know. All policies are quite broad, so in those specific cases, those policies may not be really that applicable, so that you have to have quite a lot of confidence in yourself and in your knowledge, to break that policy in that specific case, so that one way of being careless. Or hopefully I would think, taking calculated risks, that's why I said it is quite an interesting question, because it is something about that, that you could see that sometimes that people who know more take more risks and that's. Yeah that could be perceived as careless, hopefully it is not.	RT-SPO-CP RT-SPET
63	W.H	Ok, Thank you for that, do you have anything extra that you would like to add? Or do you think that everything is covered?	
64	D.E	Uhm, I think one thing that is interesting that I mentioned is that, just to give you a tip is to look at this concept of Zero-trust. And the	S-T-ET

		whole idea that it is not one perimeter anymore, Like a fort. Mounts and firewalls and all that, and that is quite hard to do now. So you have to look at it in a different way, and also services going into the cloud. That is not on your premises anymore, so you have to trust your suppliers, there are a lot of interesting concepts of how you have to think about security. Compared to how you did it five years ago, or even two or three years ago. And I think the pandemic and forced teleworking has basically been a catalyzer or lubricant to this movement. You have to do it now.	S-SPO-CP T-SPET T-SPO-CP

Appendix 3

Interview 3 (I3)
Company: Scania AB
Interviewer: F.S = Fredrik Sundström
Respondent: F.T = Fredrik Tomasson

Row	Person	Question & Answer	Code
1	F.S	Ok, thank you Fredrik for this interview, and we would like you to focus on the timeframe from march 2020, and you can start by stating your name and your role at Scania.	
2	F.T	My name is Fredrik Tomasson, and I'm CISO at Scania. CISO, that is Chief Information Security Officer. So I'm responsible for IT and Information security for the company.	
3	F.S	And as of today, are your organization teleworking? And if so, when did it start? Is it forced? And, approximately how many percent of the employees are teleworking?	
4	F.T	My organization, which is the IT and information security department, is generally everyone teleworking. So to say or remote working, with the exception of me and one more person, because we would like to stay at the office. And we do also then handle some physical stuff, that sometimes need to be handled at the office. If we look at Scania in general, those who can work from home, they basically work from home. It is quite empty in the office spaces, I would say. But for the factory and workshops etcetera, there, of course everyone is working on site, because you need to do physical stuff on site. Yeah.	S-T-ET S-T-FT
5	F.S	And we also would like to. We wonder if this teleworking is forced. Like they are recommendations perhaps for Scania to, the best of your capacity to work from home right.	
6	F.T	It's highly recommended, I wouldn't call it enforced, in the way that you are not allowed to be at the office. If you have a need to be at the office, you can of course come in to the office. But most personal are commuting and want to have distancing etcetera, so this it is highly recommended, and actually works quite well. So it is very few persons that you see at the office, on a daily basis.	S-T-FT
7	F.S	Alright, then we would like to move on to the next slide. And as I sent to you In the email prior to this, we are investigating this from three different aspects. And the first one we will address is the Technical aspect. And in the upper right corner here, you have the	

		definition of Malware that we use, for our thesis. And for the first question then, what challenges and threats do you se with forced teleworking, in an IT security perspective, for your organization?	
8	F.T	When it comes to malware specifically, and remote working it is not a big change from what it was before. What has happened over time, especially over the last year, or maybe two years, is that the hackers, when they are sending for example emails with the links or malware etcetera, are focusing more on a phenomena which is ongoing which is Covid. So they use covid in various forms to trick users to do things on their computers. What has also happened over time, depending of course on what technology companies have, is that these people are not sitting at the office, they are sitting at home. They connect to the office remotely. When we went into Covid, we had quite a good set up at Scania, when it comes to the possibility to do remote working, because we have a combination of VPN, but also VTS. Which is remote desktop so to say, for the users. So when all this shift happened on the network side, so not a lot of traffic on the inside, it's more coming from the outside we did no have major problems, like many other big companies had, because they had limited functionality towards remote working. But our solutions here have more or less, we have had an approach to have this possibility for a quite long time. But it was only adding a little bit of capacity, while many other companies, industrial companies, had to increase capacity quite a lot. And since we have this possibility, some of the solutions, specifically VTS, is more protected towards malware, because when you do a connection to the company from the computer that you're sitting at is not a part of the internal network, like it is when you have a VPN. So, the number of individuals being able to affect the internal network is less now, compared to before. So from that point of view, it is better.	T-CS-MA S-CS-SE S-T-ET T-SPO-CP T-SPET
9	F.S	And in terms of malware, have you had any problems since march 2020, and if so have you seen an increase in the number of malware attacks?	
10	F.T	I wouldn't say it is an increase. But we have not had more incidents I would say, we have had more investigations and taking a look at things, but we have not had any more cases that are actual incidents. So there is a higher workload of course, but incidents as such where things actually have happened has not increased.	T-CS-MA
11	F.S	Alright, let's move on to the next slide. Here if you can see on the powerpoint, we have different types of malware attacks regarding threats. We wonder if you can rank these from the most common to the least common malware attacks regarding threats towards your organization when teleworking?	

12	F.T	You mean threats as what could happen or threats.. occurrences where we have to handle something?	
13	F.S	Yeah, occurrences, frequency we mean by that	
14	F.T	Ok, I would say viruses and ransomware, worms etcetera, I mean physical coding, it has not really increased. But what has increased quite a lot is of course phishing attacks to get credentials, to be able to log in or fool for example two-factor authentication, things. But viruses and malware as such, I wouldn't say it has increased a lot, maybe a little bit. But on the phising side, it is much much more. And that is of course phishing for credentials. And, like a lot of companies, also Scania has gone in the direction of Office 365. And Office 365 in general is more targeted towards this, because there is so many more companies using Office 365 so of course hackers and such would like to do bad stuff, concentrate on making fake office 365 log in pages etcetera.	T-CS-MA T-SPO-CP
15	F.S	Ok, and then for the next. We are wondering if you use any cyber security standards and frameworks. To handle threats from teleworking.	
16	F.T	Yes, I am familiar with all of these. The PCIDSS we are not affected by because we are not doing credit card transaction and stuff like that. Well, we don't have the solutions ourselves, if we need that in some kind of application it is a service, so we are not, have to follow the PCI. We are actually in the process of becoming ISO27001 certified. We are actually in the middle of it, and our aim is to have the certificate by summer time this year. But only for the information and IT security departments, not Scania as a whole. These standards here, I wouldn't say that they directly increase the protection of, or take care of the threats when it comes to remote working or teleworking. They are more focusing on making you as a function, working more strategic and structured and through that doing a better job. So, but they are other standards also coming that will affect the company so to say, because we are in the automotive industry and the auto motive industry is having new legislation and new regulations coming, not only for IT, but also for the IT, so to say, inside the product. So in the vehicles, as you know Scania is going in the direction of connected vehicles, autonomous vehicles etcetera etcetera. And there are regulations coming into that area also to make the digital world around the vehicle more safe. There is one UNESE that has released a regulation, and there is also ongoing I would say ongoing from the European Union the NIS 2 directive, so there are more regulations coming.	T-SPO-SF RT-SPO-SF
17	F.S	Are Scania using NIST as a standard or framework?	

18	F.T	I wouldn't say that we are using it directly. NIST, I would say it influences us. We are more focusing on other industry standards and industry regulations, and they are built from NIST. I don't know if it make sense. But for example, German automotive industry has a collaboration with a, doing an assessment methodology of partners. And pluses companies basically, it is called BDA, and one can have a result in BDA that you audit and can get certified and then it is called PSUCKS, this standard or German industry standard is growing in europe and we will start to use that one towards our suppliers. And when we, if I'm looking at the content of this, it is based on for example NIST. So we are not using NIST directly, more indirectly.	T-SPO-SF
19	F.S	Alright, and other question just out of curiosity for this thesis. How would you, or what differences would you say there are between cyber security and information security? Or do you use them interchangeably?	
20	F.T	I have a view on it. I don't know if everyone actually agrees with me, but my interpretation and when I explain things. Information security is all carriers of information, so it can be in the digital world, but it can also be in the physical world like paper. Or it could be a prototype. A prototype is also information in a sense. But paper security, things that are on paper, is not generally in scope when you talk about cyber security, because cyber security means more the digital world. So I would actually argue and say that information security is slightly bigger than cyber security.	
21	F.S	Alright, and I actually think you answered the rest of the questions here when you talked about the other standards, and frameworks. So I think we can move on to the next slide.	
22	F.T	I can just mention on that we are not only looking at international standards and frameworks and regulations, we are also have to look at the local country specific legislations and country specific regulations. Because we are active in so many countries around the world so we have Russia, we China and other countries that have slightly different view on how to do things, for example cross boarder traffic of information or where information needs to be stored, so all that affects design and how data should be treated and stored.	
23	F.S	Alright, and then in terms of security practices, we wonder what security practices do you use to ensure safe teleworking for your employees?	
24	F.T	You mean on the list here? We use all of them. If we start with something here, if we go to the bottom. If we have services that have information that is classified as confidential or higher, if you are accessing that from example the internet, multi factor authentication is needed. So MFA is needed, if you need access to remote working	T-SPO-CP T-SPET

		desktop or VPN services etcetera, MFA is always mandatory. So multi factor is always something that is more in use now compared to before. Because before not everyone was using the services so they didn't need the function, now they need it more. Installation of anti-malware software we have several products that we use, we have a antivirus, we also have an EDR tool, and EDR is a tool that is more for certain dedicated things for example, we use a tool called HX, which has a pretty high protection function, but it can also be used for extraction of data for example. And this I quite important, so we have it on all computers, and this is actually quite important now when people are working from home, because there is a differences if you are sitting on your intranet and something happens to your computer, if someone needs to go in to that computer and extract data, and analyze data to see what actually happened. Malware, or whatever, there are multiple ways of doing it, but when people are working from home many of these functions are limited. You don't have access from the company, so you can always remote a computer, at someone's home, but through the hx we can still extract necessary data to be able to analyze what has actually happened. So we have a combination of two software that we have installed on all clients that people have. So there is a slightly different way of working when people are at home, when you need to do an investigation on what happened on a computer. Yeah, regularly back up of data etcetera, I mean there is no difference there compared to before. I would say to enforce safe password practice, there is not really a big difference compared to before either there, we use jump servers internally for doing administrational servers and infrastructure. And that solution we already had in place before Covid. And it also can facilitate people that are working from remote, because we don't have people sitting at the office during night and if something happens, a person that works, what do you call it. An on duty person, they don't sit at the office at night time, there are at home, and if they need to do some administration or fix something they can log in and then go to our remote access solution so therefore password safe practice is more or less the same. Bring your own device, when it comes to mobile devices we have actually practiced for quite a long time but these are mostly devices used for, let say, mobile phone for example for connecting to office 365 to read emails and stuff like that. And when a user has a private device they have to give an approval that scania will have access to that computer, because we will of course need on board that device to office 365 through in tune. So that one is pretty important, And when it comes to remote working through VTS. Which is basically you have a desktop. That you can do from any type of device at Scania. Still two factor, but you get a desktop, so there is still no physical connection to the intranet. I have a question, do you understand all these terms that I talk about like VTS?	

25	F.S	I think we, the rest of them we pretty much understand, but VTS I don't think any of us has read about it earlier.	
26	F.T	Ok, do you know what RDP is? Remote desktop? It is basically.. From my computer I go to a home page. I log in with two factor, the browser becomes a desktop of a computer, a computer that is inside the data center so I actually then have a virtual desktop. So basically I can start software, I can start, I can do cud, I can look at email, I can do basically anything you can do on a normal computer, but it is a virtual computer somewhere else.	T-SPO-CP
27	F.S	Ah ok, like a virtual machine?	
28	F.T	Yes exactly. And since you are only getting a picture through the browser, a virus can not jump over to that environment since it is a picture. So from that point of view, that type of technology separates me sitting at home from the physical environment at the office. And a virus can not jump in between. And we've been running this for ten years, well more than ten years at quite a big scale. So a lot of users actually use this technology and it is pretty good, and pretty safe for the company.	T-SPO-CP T-SPET
29	F.S	Alright, I think you actually answered all the questions here on this slide. So we can jump on to the next one. So these questions are perhaps more specific to cyber security practice to handle forced teleworking. And we wonder if you have used any specific practices? I know you mentioned now the VTS and VPN, but are there any others that you use?	
30	F.T	I mean, how should I explain. Of course the company has gone in the direction of being more in the cloud, and being more in the cloud the more web based things are. That is good, we still have certain applications and systems on-prem that you need to reach and access either through VPN or through the VTS, what is important. Both before and extra important is that we the whole time look at how are the users using these services, and what is happening the traffic. So monitoring is very important now. So we have a SOC, security operation center, for people that look at logs, patterns to see if there are any strange things ongoing. So, I wouldn't say that we have introduced a lot of other technologies, it's just that certain technologies have become more important. I mean earlier, looking at logs in a CM system, Security logs, was very much focused on what happened on the premises and on the clients. Now, it is more what Is happening on the clients and how are these clients talking to the company, so it is kind of a, how you look at things have changed slightly.	T-SPO-CP T-SPET
31	F.S	And, you answered this question a little bit earlier. But do you see an increase in the use of these practices due to the growing numbers of teleworkers?	

32	F.T	You mean, yeah of course many more people are using VPNs, many more are using the VTS, many more people are outside the company so to say, and need to reach things that are on the inside. That one has of course grown, and through that the log in need has also grown.	T-SPO-CP T-SPET
33	F.S	Alright, then moving on to the next aspect. The Social aspect, we are wondering what is your organizational take on social engineering, and if it is a big problem for Scania?	
34	F.T	Certain things, if you think about phishing as a thing under social aspect, yes that has. The problem has increased and it has increased not only because we have covid and people are working from home, but also because we are utilizing services that are more in focus of the hackers, like office 365. So that has increased quite a lot how phishing attacks to get credentials and the possibility to break into office 365 things. Another thing that of course generally has happened is that all types of phishing attacks has increased, and it is quite important that people, staff and employees is understanding that this is ongoing. It is pretty hard to stop it. So what we are doing now, like what most other companies are, we are taking a look at are there technologies or ways of doing things that we haven't been doing before, but we need to put more emphasis on. So for example, SPF and DMARK, I don't know how much you know about how email works. But e-mail, if you have an email domain like scania.com, you will by default, because that is how email work, you will accept email coming from other places that say that they come from scania.com. So, that means that perpetrators can pretend to be sending in the name of Scania. You could stop this to a certain degree, that is the best way that phising, or a persons conducting phishing, can pretend be someone at Scania. The likelihood of you clicking on things is much higher. So what we need to do is get rid of those who pretend that they come from Scania, and for that there are a number of technologies that can be activated and put in place, SPF and DMARK are two technologies, and we are in process now of going live with these. And looking at the whole Volkswagen group, only a couple of brands are doing this. Some of the brands plan to do this next year, which I think, maybe they should put more focus on it.	S-CS-SE S-T-ET T-CS-MA T-SPET S-T-TF
35	F.S	And also, moving on this. For social engineering. Do you provide training and education for employees to minimize the threat from this? And have you added any extra training due to covid 19?	
36	F.T	I would say that we have done a little bit yes. Have we done enough? You can never get enough training, you can always train more. But we do have training and we also have introduced so called phishing platform, where we do phishing by ourselves. To see how users actually click on things that they shouldn't click on, so we can actually	S-T-ET S-SPO-CP

		measure how good the organizations is doing, are they becoming better. Do they avoid more clicking on unknown stuff compared to before, But we have had some quality problems with this platform so far. So, we are trying to improve the quality of this one, but the intention is to do much more testing of the users. And if they fail, then they automatically end up in education.	
37	F.S	And do you have policies as well to minimize the threats as well?	
38	F.T	The information security policies don't really take up this specific area as such. However, in the underlying management system, I mean our rules and standards and instruction within the company we have quite a lot regarding this area and we also publish information internally at Scania. For example, with examples on how this looks and why this is dangerous, and we actually published on Scania, the global Scania site which every employee all over the world can see. Last week, a specific article about phishing, and the dangerous etcetera, how to behave. And there are also examples on how phishing emails look like. So we do quite a lot, but it is hard to get it really good.	S-SPO-CP S-T-ET S-CS-SE
39	F.S	That is totally understandable, and how has the evolution of teleworking been in the context of Scania? Is it many more employees now? I know you answered this earlier in the beginning of the interview, but are there any effects of this?	
40	F.T	Scania has been doing remote working for quite some time. It has been possible for office users to do this for many many years. And of course the volume increased a lot even if it didn't become a technical problem, it increased a lot last year. And what happened then is that the traffic patterns around and in the company change so that certain areas need to be improved while others that were discussed for improvement don't anymore need improvement. If you had certain amount of volume over here, now that volume is over here so that then you have to add over here instead of over here. So it has had quite an effect on more people working from home compared to before yes. And also certain applications before were pretty tricky to use from home, so people more accepted being at the office. Now, it's more of a problem so that application has to be smoother when you are working from home. So specially applications with low number of users, for example. There is quite a lot of effect from people working from home, yes.	S-T-TT T-SPO-CP T-SPET S-T-ET
41	F.S	Ok, then we can move on to the next slide. Which is actually the last aspect that we use. It is called risk tolerance, I know you also touched upon this. It is similar but they have some differences between these questions. And the first one is, was your organization prepared for letting your employees telework when Covid-19 came?	

42	F.T	I would actually say that the organization as such was pretty mature for being able to work from home, or from remote. Of course there are certain risks that have increased while other risks have become lower, risks that have increased is if, what can we take. Depending on what type of risk one looks at, certain types of disturbances, not security risks, but disturbances which also are a risk have a higher impact now compared to before. Before if the two factor authentication would not work properly, it wasn't so bad. It was down for one hour, not so many people were affected, now everyone is affected. So certain components, certain areas are more important that they are up and running all the time compared to before. Not necessarily a security risk, but it is still a risk. If we take a look at security risks explicitly I would say sure, there are certain risks that we have now that we did not have before, in the same sense, for example when everyone is working at the office there are all using the printers at the office. Now if everyone is working from home, they are using the home printer, we don't control and we cannot control the home printers, so if there are doing printing at home, there we could have a risk that papers are laying around etcetera, or certain information is happened to be cashed in the printer and etcetera. But on the other hand, at the office there could be many more persons that could have access to that specific printer while at home not so many. So it is actually quite hard to see all the risk and measure all the risk but they have changed. Things that we were comfortable with before, we are less comfortable with them now, certain things that we knew, this is how it works. Now is a little bit more uncertain. So, there is a big change, but are the risks higher now compared to before? I'm not convinced, I think it is roughly the same risks, well the same risk level. It is just that some certain risks went away and other risks were added.	T-SPET RT-T-ET S-T-ET S-T-FT T-SPO-CP RT-SPO-CP
43	F.S	What level of understanding do the employees have of organization of the threats that might occur when teleworking?	
44	F.T	General things like phishing, I think it's pretty ok. But then there are, for a lot of areas where normal users can see and understand the phenomena, I think the level is not bad. I think it is ok. But there are some really advanced stuff that can still happen outside compared to on prem, there are highly technical stuff and the likelihood of that happening is not that high. For example, if you are sitting at home you are not running VPN to the company, but you are running communication another way, what happens if I hijack your home router and then play around how it does DNS stuff. I can do petty fancy stuff. For example, if you are doing banking, I could actually imitate a bank page and fool you of the bank id and steal money from your account. But at the office the risk is not so high, it is higher at home, but how many actually, how often does it happen, how high is the likelihood that someone will do it, how much money can they earn	S-CS-SE S-T-ET RT-T-ET T-SPET

		from it etcetera. So, risks calculation of that one is tricky, but to be able to explain that specific phenomena to normal users is kind of hard because it is very advanced stuff and also being able to protect yourself may be pretty hard, of course we have some general things that we advice users, like update your router, make sure it is patched etcetera. But it still their responsibility but we cannot describe that for the users that your home router, make sure it is patched and have all docing that is not needed etcetera. but that will be on a more general level, we cannot really start to explain to the users the really advanced stuff that can happen when you have a home network, that is pretty hard.	
45	F.S	And how important do you think it is for your employees to know about the standards and frameworks that you follow and the security practices that you follow?	
46	F.T	If we mean normal office workers, I am not really sure they need to care if it is standard a or b, I think it is more important for them to understand and expect that we are following a certain standard, not specifically which one. For the technical staff, like the IT staff, there is more important that they know what we are following, whether it would for example be NIST or BDA or whatever it can be, but for normal users, if I take a normal office user, I don't think they know what COBIT is and ISO20701 etcetera. I think that is more confusing, I think they more like that we follow a standard, not exactly which one.	RT-SPO-SF S-SPO-CP
47	F.S	Understandable. Do you see a difference between departments when it comes to knowledge of security practices?	
48	F.T	Yes certain areas are more security aware than others. For many different reasons, people that are working with more regulated stuff in general have a higher interest I would say in security so finance, credit areas, things like that, certain development teams seem also to be a little bit more security aware I would say, so yes of course there are differences inside the company.	S-SPO-CP RT-SPO-SF
49	F.S	What departments seem to be more likely to be attacked and which department might actually suffer from more attacks?	
50	F.T	That question is kind of difficult, I mean it depends completely on what kinds of problem we are looking at, if we are taking a look at hacker groups or individual hackers or state sponsored hacking they all have different focus and they will of course target different types of persons I would say, so it completely depends on who is on the other side. And there are hacker groups that focus on certain things I mean lets say a hacker group that wants to earn money by bribery towards the company by the use of ransomware, if I would be that hacker I would of course go for persons that have reasonably high	T-CS-MA RT-T-ET S-CS-T-ET

		credentials and privileges within that environment because that is the best way of spreading that ransomware, If I would be interested in secrets within the company, maybe you go for persons that are handling those types of secrets, so I mean hackers are like everyone else. They go for the easy target and they don't wanna overwork things. So I would say they go for what their goal is, is it money or secrets or just to make a mess you go for different targets.	
51	F.S	And then the last question, do you see that employees with more knowledge about security practices in teleworking are more risk taking?	
52	F.T	That is hard to say, it is an interesting question, maybe but I am not really sure, it is nothing I have thought about, very interesting question. I can't really say but one would hope people with more security knowledge on them would not fall for phishing attempts etcetera. But they could of course be confident in that "I know how this works so I could just be along a little bit and I know when to stop" and then it can be too late. Or it could be that they are being curious about what is actually happening so that they press the link. Or "I know that this is very bad but I know that I don't have viruses on my computer and I have protection in my computer which should protect me, lets see if it triggers an alarm, I cannot say if they think like that, I hope not.	RT-SPO-SF RT-T-ET
53	F.S	Now we are actually done with the interview, is it something you want to add?	
54	F.T	Well no, but we have not really touched upon the trends in the world, if we look back let's say 10 years, and what will happen for the next coming years further on. Now covid, at least for Scania and I guess for many other companies, at least companies that I know about, many companies have started with technologies that simplify working from home, before covid, they did not have it lets say five to ten years ago but a lot of companies have increased their possibilities for the last two or three years, which made the technical things and possibilities for people working from home, rather okay now with covid, it would not had been as easy if Covid would have happened like two or three years ago. And that is due to more people, especially young people, expecting when they take employment from companies today, that they will be able to work slightly differently compared to how their parents used to work, that is my feeling. So with this one (showing Iphone) I talk to people and I read emails, I don't do anything else, but most people 20-30 today, they use this device for ten times more stuff, I don't do that. So younger people are more, they consume IT in another way and this is of course something that big companies like Scania and many other companies have to take into account, not only when they are recruiting people but also when they are creating services, that we need to have services that are not only	S-T-ET S-T-FT S-T-TT

		good for those who really work at the company today but also to be able to attract new people that are younger because they expect a certain way of working that we don't have already in place. I think younger people today don't want to sit in an office everyday, they would like to have more flexibility. My generation accepts sitting at an office. So I think there is a change going on in the world and it has been ongoing for some time and it will grow more over time. I will guess that the years to come now, of course there will be, when covid ends a lot of people are really tired of it and will like to come back to office, but there will also be an expectation that the possibility to work from home will be greater in the future compared to the past. That is one thing and the other thing is the service, especially if you buy services, not creating them yourself, when you are buying services, new applications for example, they are more made for that type of work, especially things that are in the cloud. A lot of companies are going more and more into the cloud which simplifies working from home so these trends going on at the moment and what covid will do is make these trends go faster. So the transformation from onprem to the cloud will go faster, the companies adjusting to be able to work from home, to be more flexible, which already started before they could see that young people would expect this, it will go faster so that is just my reflection about what has happened in the past and what will happen maybe the next five years.	

Appendix 4

Interview 4 (I4)
Company: Stora Enso AB
Interviewer: F.S = Fredrik Sundström
Interviewer: W.H = William von Heland
Respondent: P.A = Patrick Andersson

Row	Person	Question & Answer	Code
1	F.S	First you can perhaps give us your name and role at Stora Enso?	
2	P.A	Yes of course, so my name is Patrick Andersson, I am the head of Information and Cyber security. It is a small unit within the larger IT and Digitization unit. We are right now seven people and we take care of the governance which is IT policies and IT guidelines, organizational capability developments such as new technologies and new services that we currently don't have in order to increase the information security within our organization, awareness, the awareness activities towards our employees and lastly but definitely not least, the privacy as the privacy program is owned by this unit. So the formal title is Chief Information Security Officer. But the role is leading this unit.	
3	F.S	Alright, thank you. For the next question, which is questions within questions. To start off, are your organization teleworking today? And when did it start? Is it forced? How many percent would you say approximately, of the employees of your organization are teleworking?	
4	P.A	So right, Yes we are definitely teleworking. And this started, I am trying to remember if it was already during February or if it was in the beginning of March. So let's say it was in the shift there between February and March 2020. Because there were already some individuals that wanted to work from home but then the general requirement or actually communication because it is not mandatory, so requirement is the wrong word but the request and the information about working from home was possible and communicated in March. So, it is not forced, we have factory workers managing the physical productions, they are of course required to be on site. We have the knowledge workers or the information workers where possible it is said to work from home. And then there are some restrictions on how many individuals that can be on each given office. If people would like to be or for some reason would want to be at the office, with small children at home or such, then there are these time sharing requests to be in the office depending on the quota on	S-T-TT S-T-ET S-T-FT

		how many that are going to be at the office. If it is below the limit, you would be given green light to go to the office. We have 26 000 employees and we generally consider a bit north of 12 000 being information workers and then it depends a little bit but I would say there are about 10 000 employees working from home right now.	
5	F.S	Alright, then if we move on to our first aspect, the Technical aspect. Up in the right corner of the PowerPoint you can see a definition for Malware that we have used in our thesis. The first question here is: what challenges and threats do you see with forced teleworking in an IT-security perspective for your organization?	
6	P.A	Yes, and here I would like to be clear that it is for our organization. I don't see any specific challenges and actually I do not see any particular threats for us. I am aware that there are slightly changed threats being present in these now teleworking situations. But the risk level for us are fully manageable. So, I don't consider any challenges for us, there are no issues with the technical issues in the tools we use, in the underlying support services, technical support services, the technical functionality of the tools, we don't have any challenges in accessing our systems, it actually doesn't matter where we are. We had already prepared and were actively using this for remote working. And then it was an agreement with the manager to what extent the remote work was done, if it was when people were sick or if it was something that was regularly occurring. But remote working was a capability that was deployed to all our work stations already and the capacity was there already for all to be able to remotely connect. So, no challenges, when it comes to the threats, there are as I mentioned, in the pre-information leading up to this interview, a slight difference, a difference when people are sitting from home environments rather than in our office locations, and that is that their internet access is not filtered, it is not scanned for threats on the internet activities that they perform if they for example start up a browser and type in an address, there is no active threat scanning on that webpage. Anything that would interface, that would try to connect with their computers, that would be scanned, but they are able to access anything on the internet which they are not if they are in their office environments. But the threats coming out from this are manageable.	T-CS-MA RT-T-ET S-T-TT S-T-ET
7	F.S	Alright, you perhaps already answered the question that comes next, but that is if you have had any problems with some kind of malware attack towards your organization since March 2020? And that is when the teleworking increased. And if, then what happened? How was it handled? What did it cost? What kind of attack was it?	
8	P.A	So, as you have already figured out, we have not had any incidents. Or let's say significant incidents, of course we have had security	T-CS-MA

		incidents. There has been an increase in the number of security incidents going up following home office working. Predominantly, the numbers went up from changing work behaviour so people tried to execute more types of software on their computers than if they were in the office environment. What was the cause of this is more difficult to answer as we have not had any time to digest or review the types of software yet, we can only see that there were more blocked software installation attempts. Archaeological malware, viruses popping up, I mean stuff from the 1990s and the 2000s were being detected and of course blocked. We made a decision that we needed to make people more aware than what they were already of the equipment that they had on home is work equipment, they are not to provide that work equipment to their children to install or try to install gaming applications, they are not to install or connect their home USB drives, penn drives, whatever they might have which is clearly what had happened as we saw in the security incidents these legacy archaeologically viruses from removable media that were connected. So, yes there were an increase in security incidents but the consequence of these security incidents were nothing.	T-SPO-CP S-T-ET S-SPO-CP
9	F.S	Yes, well handled. Here on the next slide you can see a couple of common malware attacks, then we ask you if you can rank these types from the most common to the least common attacks regarding threats for your organization when teleworking?	
10	P.A	Yes and when reviewing your questions that I received prior to this call I did notice that you are missing the threats and types of attacks that we have seen actually even before teleworking but picked up now with teleworking is credential phishing. So basically, phishing emails that are designed to lure people to fake logon screens, so not to install any viruses, no ransomware, no scareware. Nothing of what you have here but simply to steal their passwords and then through automatic means try to, because we know what happens to other organizations that are lacking multi-factor identification protection, or even the technical filtering mechanism to clean away those types of credential phishing or credential harvesting emails. The thing is that they steal the password, the credential, they try to log on, if they are successful they try to install logic or programming into the mailbox that redirects certain types of incoming emails or even deletes them, steal the address book and then immediately set forward to send new credential phishing emails out from those mailboxes. And this whole thing is designed to very quickly spread from organization through organization because people will recognize the sender, saying “yes I normally send emails to this address, what does she want now?”, they open up the email and see this attachment or web page or so you need to look at because whatever reason and then their credential will be stolen. The end game from credential harvesting to reaching the organization you want to hit and then	T-CS-MA

		there is ransomware if you sort of get the credentials to the target organization you want to get at. So that activity is our prime threat and the second one would be various types of frauds associated with breached organizations. So if a threat actor that is not interested or sort of has a secondary objective of launching ransomware later on but the primary objective is financial fraud, they will use these breached mailboxes and inject themselves into business conversations and change invoices and banking details in order to very quickly benefit from ordinary business transactions and payments of invoices. This is generally referred to as Business Email Compromiser (BEC). From your list then, what I would be worried about is ransomware. Worms, spyware, trojans not so much, the few cases they pop up every now and then are detected, either on the end points for those files gets deployed from the advanced endpoint threat detector that every organization actually needs to have that will tell you when the usual attack vectors and how you take control over a computer is active and will then signal your response teams to come to that work station and have a look on what is going on. So, yeah I would say: Top threat missing here is credential harvesting, second threat is BEC or attempted financial fraud from fake emails and then ransomware. That would be my one, two three.	
11	F.S	Okay, yeah. Let's see, for the next here, we are wondering if you are using any cyber security standards and frameworks to handle the threats from teleworking?	
12	P.A	Well, not specifically, sort of related to teleworking. But yes, managing threats and risks of cyber security or information security we are definitely trying to follow best practices and not trying to invent the wheel ourselves. Out of the standards you have listed here, the british standard is actually the precursive of the ISO27001 and the others, PCIDSS is more for financial card processing or businesses where you process credit cards. That would predominantly be in a business consumer environment and we are business to business. ITIL is a very general IT management framework and COBIT is effectively managing risk associated with IT processing. What we actually use is the national institute of standards of technology cyber security framework, this is what we used to capture our maturity, do gap analysis of capabilities that we would need to have in place. So this is extraordinary good to use the NIST CSF to do the top-management reporting because it consolidates a quite complicated area into five domains and you can read about them but to summarize your capabilities depending on these five domains and what these domains mean is something that you then are able to communicate to top management. So NIST CSF is what we are mapping our decisions and priorities and resources of activies to further improve our matority and then there are other frameworks like CIS framework, which I link here. Which gives you, depending on the criticality of	T-SPO-SF

		the information access that you are trying to defend gives you a prioritized controllist. Very very handy. You can actually download specific control lists for certain types of applications or use cases which is extraordinarily helpful. And lastly I would even request you to have a look at the information security forum which is a non-profit organization but it does require membership to join, and they have since well a think they are almost 30 years old now and Stora enso have been a member since 2000 published a best practices information security management framework that they now call the standard only, it used to be called the standard of good practise but it was to much of a mouth full. So now it's just the standard. And if you follow that it is extraordinarily extensive it is 3500 different controls but if you follow this you are able to map your information security to any of these standards that you have on screen as well as the once I just added. So it's like a meta or super framework this ISF standard. Yeah we don't use any particular framework to manage teleworking because it's just like an aspect of information security management. But yes we are using cyber security standards and frameworks to manage information security at large per dominantly NIST CSF.	
13	F.S	Alright, and I think that also answered the following question a little bit. Even though it wasn't one of the once that we had on the screen you? With 3 different standards that seemed a little bit extra important. But regarding the meta maps that you said, does that one guide you towards these standards and the ones that you said previously depending on how your organization is structured or how it works?	
14	P.A	This ISF standard, the benefits is that it is industry agnostic, it can be applied to any kind. It contains way more controls that you are ever going to need or use. Being built up from there they also provide very good threat event catalogues, so if you need to create some risk scenarios or specific risk treatments plans they have the threats that can kick start the risk scenarios to materialis. So the ISF is extremely valuable for understanding what information security is all about and what you would need to focus. Now I lost the original question. What was that?	T-SPO-SF
15	F.S	I just asked that the last one that you linked, that meta map, would that eventually lead to these standards on screen or the one that you are using?	
16	P.A	Right, yes, it includes them all. It's like the rings from the Tolkien lord, that wants to control them all, haha. Let's put it into context, when we did the first maturity assessment the idea and intent was to use the ISF standard because it also provides a benchmarking platform so you are able to compare yourself either in the same vertical	T-SPO-SF

		or globally across anything and then based on geography where you are located so you are relabled to match where you are. But then in the process of understanding how to execute the maturity assessment what are the good thing to do and what are the unnecessary that we should not be focusing on, we learned that other organizations where starting to use the NIST CSF and it is a sub-set of standard but it makes it easier because it's more focused on cyber security it makes it easier for identification of where your priorities should be in order to maintain good security and its able to condense and describe information and cyber security maturity in 5 visual simple ways. So it's very powerful to communicate to individuals that may not have a good understanding of information security and cyber security at all. So you could argue and say that we came from the ISF standard having used that and done self assessment there and are now using that for reference only and actually looking for activities from the NIST CSF controls from the NIST CSF instead.	
17	F.S	Okay, well thank you. I think you answered all the questions actually. Which is really good. So moving on to the next slide then. And this one is a little bit more focused on the practises. And the first one would be what security practices do you use to ensure safe teleworking for your employees? I think that you have been touching up on that but if you could go a little bit deeper on this, or as much as you are allowed to.	
18	P.A	So first and foremost encryption. And there are two key practises when it comes to encryption. That is intransit or addressed and intransit obviously refers to the transmission of information from where the individuals are working to where the information systems that they are currently working with or on are located. So in our case that means that we are recurring our services to follow best practises in encryption so no.. well without going into too much of technical details there are certain encryption standards that are sub-par. They were good in the 80s and 90s but they are not adequate today so our systems that we use have to support transmission encryption according to current requirements. And then encryption at rest means that the devices that our employees are using are all encrypted so if we lost a stora enso laptop in the public transport it’s not a security incident or issue that is waiting to happen. The device is completely useless for anyone who would pick it up or in worst case steal it. So encryption is the key. Then there are various technical measures that help sort of layer on layer that help to protect the human operating device. I think i briefly mentioned these.., the top threats being harvesting and the business email compromise. So that should give it a way that email or the unified communications tools of chatting for example, or teams, web conferencing. Those are extroderly important that you have technical measures in place to help to protect users of. Different technology providers or solution providers have	T-SPO-CP T-SPETS-SPO-CP

		different technical capabilities. The platform that we are using have certain of this technical capabilities that you for an extra fee can enable and one might have a sort of personal view that it should be illegal to sell IT services today without those type of advanced features being active but clearly it isn't so it's up to the providers to shart extra for those. But certain advanced technical features are trying the links before the user is receiving the emails or in the chatt windows before that chat message is arriving to the user the links have been pre validated to not go to anything dangerous with the attachments. And if I file transmitted over a system that we are currently in or through an ordinary email have already been in a way detonated in a safe environment and any potential dangers that might have been there have already been discovered before an attachment is handed over to the user. Downside of this is that you will see a slight delay during peak-hours and you are not able to get to the documents immediately. Because it's actually being processed in the background. Installation of anti-malware software I think that one as well as the last one (multi-factor identification) are the key Technical aspects that you have to have in place for teleworking to be safe. I might say enhanced endpoint threat detection and response (ETDR) is sort of more appt. Anti-malware could be a traditional anti-virus which is absolutely and utterly useless. You need to have ETDR or EPP if you sort of look up those solutions that you need to have in place. Multi-factor identification if you don't have that for all your users you will be a headline in the media. That's just the case. And your third choice would then be the non-technical but more of a protective preemptive measure - Awareness. Safe behaviours to the employees. It can not be overstated. It's insanely important- You have to give the employees a chance to do the right thing by telling them what is safe and what is unsafe. The others are not as important as the once we have talked about.	
19	F.S	All right, but then you would say that Education for all employees is a way to medal how important it is to actually act in a good behavior when teleworking.	
20	P.A	Well I would actually put it like this: That without good awareness our users/ the employees will based on lack of understanding realize the dangers of internet usage or IT. They will cause security incidents. So a well informed user is basically security incidents that didn't happen.	S-SPO-CP RT-SPO-CP
21	F.S	And I think you also mentioned other cyber security practises that you use...	
22	P.A	Yes, these filtering capabilities can also exist on the network. So when your users are connecting back into the company internal	T-SPET

		networks any traffic that might try to piggyback home would then be detected. Any sort of unusual nonomolys from the remote office work endpoints or station would then also be detected. So network threat detection and response would be an additional one. I wouldn't write it as a top one but it could be sort of other security practises. That may or may not be in use.	T-SPO-CP
23	F.S	Okay I think we can move on unless William or Agnes have anything to jump in on this?	
24	W.H	Just one question, you might have covered it already. But regarding firewalls. How important are firewalls for you?	
25	P.A	Yes, they are good. But what is a firewall, it is a piece of software that stops a communication attempt. If there isn't anything on the receiving end if the computer isn't instructed by the running piece of software to listen for those incoming. If you have a computer that is stripped down when it comes to functionality and it has a purpose, nothing else is running. Is not able to listen or understand anything else than its purpose then a firewall is not really adding any security. So to answer your question, firewalls are good, firewalls are a part of a portfolio of technical controls but there are other mitigation controls like hardening of your server platform or applications that would decrease the usability or benefits of firewalls. But I wouldn't take them away but they are not. Let me say it like this, if you are installing a firewall and believe you are going to be safe you will be a headline.	T-SPO-CP
26	W.H	Thank you! I think we need to move over.	
27	F.S	Yes, you touched upon this as well. And this is if you have any specific cyber security practices for the forced teleworking situation. But I think you also mentioned it a little bit.	
28	P.A	Yeah I think I actually did that. If you review my answers I think you will see that I'm answering these questions. Yes there are other specific practises that we have in place. Not because we started teleworking but because we already were prepared for remote working. So it wasn't anything that we purchased then added. We were just adding some more licenses. There were a few aspects of adding a bit more bandwidth, because obviously if you have, lets say, a thousand travelling sales people remote office working, then suddenly you have 12 000. Yes there is going to be a little bit of a wider internet connection, you need to accommodate that but we already had these practices. We didn’t add anything in order to switch. I know of organizations that had to build capabilities in order to support teleworking, so depending on who you are going to interview the message will be different. But in our case there wasn’t anything that we sort of added. An increase (in the use of teleworking practices), no,	T-SPET S-T-ET S-T-FT

		again based on the same underlying answer that you need these practices to be in place if you support remote working, like people being out traveling or popping up in guest offices and then be expected to work from those locations. But the importance of having that in place of course is growing if you have teleworkers, but I would argue that you need to have this anyway.	
29	F.S	Then also, I think in the email you sent prior to this interview you also mentioned a lot of these things as well. But moving on to the Social aspect. Then the first question here is: What is your organizational take on social engineering? Is it a big problem for your organization? And if hackers are trying to use your employees? And I think you mentioned a little bit, that, for instance when you mentioned that employees are not allowed to install gaming and such, but please elaborate a little.	
30	P.A	Social engineering is definitely a threat. There has been a little bit of those types of attacks. Predominantly, the attacks we have seen were as already mentioned, credential harvesting and business email compromise, or breach organizations. Or sending fake emails, and part of fake emails I certainly social engineering, trying to lure the recipient of the email, or even a phone call, to do something specific. I think you may have heard of the fake support scams, so people get call from Microsoft within quotation marks, they are then told that there is problem with your computer and we would like to help you with that, can you install this software and we can get rid of your problem. Then of course, the malware is actually installed. That is also a little bit of social engineering, trying to convince the employees to trust that this activity is legitimate. So social engineering is part of our awareness, that sort of warning signs these dangers exist, and the second question there. Yes, well maybe not hackers. That is the wrong term here i would say. There are basically three types of threats operators that target organizations. Hackvisist, not hackers, hacktivists, people with maybe a social agenda or any kind of other viewpoint that they would like, or they might disagree with an organization's view point. For us, those are not a threat. State sponsored, there you might say hackers, potentially, then you have very state or nation state to further their political agenda by disrupting certain businesses or reaching or getting hold of strategic business information by coming investments or investments decisions. Not a threat actor or threat operator that we are worried about, based on the type of business we do. Then lastly, the financially motivated, basically the criminals. They go after any employee, using any means, if you end up in their sights, to reach there endgame which is getting hold of your money. And then the business you are in, the vertical you are in, is completely irrelevant. Any successful enterprise that is making profit is by definition a target. So yes hackers, but I would the financially motivated threat actors are indeed trying	T-CS-MA S-CS-SE

		to use our employees trying to get a hold of maybe not our internal data or systems, to reach our business conversation or sort of divert monetary funds, that is sort of a threat.	
31	F.S	Ok, and leading on to the next question, I know you mentioned a little bit earlier about how important awareness is for all your employees. And if you provide any training or education to minimize the threat from just social engineering, and how often and if you have added any extra training since corona hit.	
32	P.A	So, yes it is definitely a part of our awareness. There is a chapter regarding social engineering and sort of giveaways, urgency, just to give you one example. If you get communication where there is an urgency, that should trigger a little bit of suspiciousness, why is this urgent. Then you should look for additional indicators. This is not maybe not entirely legitimate, asking your manager for device now. Or also, you have to run these, or you must use these documents and these guys may not recognize these documents, ask IT for support, is this legitimate, so these types of advice. But we didn't add any extra training. The reason might actually be just the timing, we had just prepared, by coincidence a major awareness program as Corona struck, so we had already the material, the animations, the electronic documents already that existed so it wasn't any need to do any specific for corona.	S-SPO-CP S-CS-SE RT-SPO-CP T-CS-MA
33	F.S	Alright, and I think also a little bit maybe, you answered the next question, if you had any policies for minimizing threat. For potential hackers, hacktivists or...	
34	P.A	No, I wouldn't say policies, the message we sort of communicate is work as you do in the office. That said then, we are aware we have these, a little bit, uncontrolled internet access, or unfiltered internet access in their home environments, but the mitigating controls, the additional control we have in place that eliminates the risk or making the risk neglectable. So no policies, but there has been a number of communications, three to four messages, even actually from the CEO during all employee calls to be very aware of that these equipment is work equipment and not for well other usages, can't remember now, we specifically said gaming but anyway not to let anyone else than yourself access to the work computer.	RT-SPO-CP RT-T-ET S-SPO-CP
35	F.S	Alright, and then I know you also said that your answer was you already had very good teleworking capabilities before Corona, but we still wonder how has the evolution of teleworking been in the context of your organization? And, yeah..	
36	P.A	Well there has certainly been a social realization that telecommunication or that teleworking is manageable is effective, is functional, so there has been some hesitation. Maybe partly cultural in some	S-T-TT

		countries, maybe partly historical expectations that you show up 9-5 at the office, that's work. But I'm seeing, sensing, hearing that there will be changes coming, there will be some offices where there might be less physical workplaces than before, there might be a higher willingness to accept that employees are working parts of the week, number of days per week from home than before. So, that will be the last thing, legacy, that home office working or teleworking is going to be considered a natural part of work. So 9-5 might not necessarily be in a physical location called an office.	S-T-ET S-T-FT
37	F.S	Perhaps we should move on, because the next question is already answered in the email prior to this. And, I think also this question if your organization was prepared, that one is also already answered. And did you see an increase in security risks, that also actually answered or actually security incidents. What level of understanding does your employees have of threats that might occur when teleworking?	
38	P.A	Very high, we had a high awareness already before Covid or this home office working became a thing. Threats from emails, threats from cyber fraud or financial fraud, we actually. The awareness was so high, just to give you some examples, there were some bases of internal communication written in such a way that it gave concerns of authenticity to the employees receiving those messages, and they were actually reported as attempted phishing. It is quite hilarious, we actually had seriously speaking. Don't quote me on that. Seriously speaking, we had to give guidelines of how to write internal communication. What is the type of language you use, what is the type of trust indicators that you need, that you, and some examples, you have to have a personal sender. You can't just sort of say best regards HR, just make proof in point. So those guidelines, so those guidelines were communicated way before covid and were designed to instill confidence to determine that this is internal communication and not phishing. So we were prepared.	S-SPO-CP RT-SPO-CP RT-T-ET RT-SPET
39	F.S	Ok, then you also spoke about the awareness program earlier. How well did the employees know of the security practices of your organization?	
40	P.A	This is an interesting question. And I honestly don't think that the employees are too aware of the security practices. Definitely not the ones they are not seeing, like filtering, the advanced scanning and threat detection they are not seeing. They are noticing the multi factor authentication or the request for additional measures to be taken when they try to access or authenticate towards our organization from home. So those practices they visually see, but generally speaking I wouldn't say that the employees are aware of technical or other security practices. And I don't necessarily need to be. And that	RT-SPO-CP S-SPO-CP RT-SPET

		actually answers your next question. There cannot be a need for employees to understand any type of security standard that we are following, the only practical examples might be that it is actually sales where you need to convince the customer that we have the house in order so to speak. When it comes to information security practices and when we talk about certifications, some kind of evidence, accreditation or something. But that is the only use case I can think when employees would need to know. So short answer no.	
41	F.S	Ok, then this is the last slide, so we are soon finished. That is if you see a difference between departments of your organization about the knowledge. And I think you just mentioned that the sales department might have a little bit more knowledge than the others. That also comes a little with the next question, like what departments are more likely to get attacked and which departments actually suffer from more attacks?	
42	P.A	So this one is really simple. Generally speaking there is no difference between departments, when it comes to knowledge. There is a general awareness. Definitely top management, they by definition get singled out and targeted. There are specific threat actors that are targeting seniors or top management and then the customer facing, so sales or support organizations they definitely see the business email compromise, they see those others organizations that have been breached and believe this is the customer that is now communicating requesting to change invoicing information. And it is not, it is the threat actors that is sort of abusing those organizations. So top management and sales.	RT-SPO-CP S-CS-SE T-CS-MA
43	F.S	Ok, and then for the final question. That is if you see employees with more knowledge about security practices in teleworking if they are more careless than the rest of them?	
44	P.A	Oh wow, that was an interesting question. Careless, uhh..	
45	F.S	Like if they are more risk taking..	
46	P.A	I actually don't see any carelessness, but what I would say and see, and notice is suspiciousness. So the more knowledge you have about security practices, or maybe sort safe behaviors or well general threat, the higher the suspiciousness is. So I can get contacted about certain practices from customers, or suppliers about what you think about this. Is this real? So, employees with more knowledge about security practices, I do not see any reason to see that they are not careless, I would actually turn it around and say that they are more suspicious.	RT-SPO-CP RT-SPET
47	F.S	And I think that actually wraps the entire questionnaire.	

48	P.A	Ok awesome, I will have to jump in to the next meeting.	

Appendix 5

Interview 5 (I5)
Company: Klarna AB
Interviewer: F.S = Fredrik Sundström
Interviewer: W.H = William von Heland
Respondent: M.S = Mark Strande

Row	Person	Question & Answer	Code
1	F.S	Okey welcome, what you can start by saying, What's your name and your role at klarna?	
2	M.S	So I am the CISO of Klarna and my name is Mark Strande. And I lead the domain engineering assurance. And in Klarna as we are a financially regulated institution, engineering assurance is a second line of defense function. The second line of defense means we are basically a control function for the area of ICT and security risk management, as well as for information security and for cyber security areas. So basically, we control what all the operational capabilities are doing, what they should be doing.	
3	F.S	Okay. And then for the next question, all your organization, teleworking? And if so, when did it start? And is it forced, if you approximately how many percent of the employees are teleworking as of today?	
4	M.S	So, Klarna has always had teleworking or always had remote capabilities to connect up. Klarna is located at multiple locations around Europe and US, as well as in many other continents and countries. But we've always had the capability of teleworking. As of forced teleworking, we naturally came to a point where we needed to evacuate and move out from our offices all together. So that means that previously non teleworking business units, or we call them domains, had to start teleworking and that could be for example, the customer service domain, and all our other domain that would normally come into the office also had to start teleworking. So as of today, Klarna is 100 percent teleworking. So all of our employees can work from home, except for very few exceptions, where, for example, they have work that relates to the office environment that can’t be done from anywhere else than in the physical office.	S-T-TT S-T-FT
5	F.S	All right. And then we can move on to our first aspects. As I sent in the email. Prior to this interview, we have three aspects from different theories that we're investigating from. And if you look in the top right corner, you see a definition of malware. And the first question	

		here is what challenges and threats, do you see with forced teleworking and an IT security perspective for your organization?	
6	M.S	So, with forced teleworking in comparison to prior there isn't really that much of a difference. Our managed client platforms are basically the same. It isn't that we haven't evolved them during Corona. That was a natural evolution that was already planned. So it wasn't something that we were forced into with teleworking. So basically, the capabilities that we use is that you have to have a managed device, and it has to fulfill some sort of special security requirements in order to access our infrastructure. And that gives us the ability to then monitor and manage those threats on those devices. Are you interested in the malware aspects or are you interested in the other aspects as well, regarding teleworking?	T-CS-MA T-SPET T-SPO-CP
7	F.S	I think we would say actually all aspects. We have some questions further down in the interview, that's more specific to some malware and cyber security practices. But if you can come up with anything right now on top of your head, so please share it.	
8	M.S	Yeah, so the biggest thing in our environment is that we employ two factor authentication. So two factor authentication is something that basically alleviates one of the bigger concerns that you have when it comes to teleworking. We utilize it across the board. So everything that we use, and do utilize this two factor authentication with a hardware token device. So that eliminates one security concern and one security flaw that you have with remote workers. Another one is basically your physical presence and how you can be overheard. Now, that is something that when you walk out from the office, that becomes more apparent, you are sitting inside of a home, there are other people who are not employed by the company. So for that area, we employed guidelines, as well as educational material and training for everyone to understand how to manage their work, working from the home environment. So that was also something that had to be addressed. Naturally, then the physical security confines of how you're working with your devices. For example, if someone steals one of your devices or steals one of your two factor authentication tokens, for example, that is also handled with the standardized platform that we already had. So that is also some nothing that really changed. Because we use full disk encryption. And we use those types of capabilities as well as have remote wipe capabilities. So in case of a device loss, that can be reported, and we can remote wipe them.	T-SPO-CP T-SPET T-SPO-SF
9	F.S	Okay. And then for the next question, we are wondering if you've had any problem with some kind of malware attacks towards your organization since March 2020?	

10	M.S	So we haven't had any problems with malware attacks, we have seen that the increase in malware type of attempts have naturally increased. But to be perfectly honest, it hasn't significantly influenced us. The attempts of different types of send outs and emails did increase so that you could relate it to Corona as well as towards people working from home. And also executive impersonation type of attempts, you saw a slight increase, but it wasn't substantial enough. We see increases in other threats. But we haven't yet been affected by them. So our threat intelligence capabilities are identified, for example, there being a much more organized malware around ransomware that we call big fish ransomware. We haven't seen any of that towards us. So those are the things that we have. That's how we see the landscape right now.	T-CS-MA
11	F.S	All right. I think you actually answered the last question here as well, where you said that you have seen an increase in the number of attacks. So I think we can move on to the next slide. If you look here at the screen, you have different types of malware attacks. And we would like you to rank these types of malware attacks regarding threats for your organization from the most common to the least common.	
12	M.S	Just give me a second, I'll just bring up my Q1 report so that I can have some reporting on this subject.	
13	F.S	Perfect. That's very cool.	
14	M.S	So I can work off the numbers instead. So if you look at in general, the biggest problem is, how do you know the difference between a ransomware, a Trojan or spyware, phishing worms. It is really, really difficult to actually categorize them differently. The biggest volume that we see is some type of malware that is coming in of course, usually emails, so that's the bigger bulk. And that could actually be most of those categories. I think less malware, I'm not sure what you mean with that. What do you mean with fileless malware? Are you meaning hacker attacks where exploitation ulnar abilities or?	T-CS-MA
15	F.S	Yeah, exactly.	
16	M.S	It would not be something that you won't be exposed to by emails or anything like that. That will be something that you would see in a general attack. I think that the majority of the bulk of what we've seen is malware being sent in phishing. To be perfectly honest, we don't even carry any statistics about the volume of all the phishing that comes in, because most of it is actually quite efficiently stopped. Though we have seen a couple of attempts on trying to do phishing against our employees, that has been good enough to be designed to get around the general phishing prevention's that we have in place.	T-CS-MA

17	F.S	All right. I think we can move on to the next. And for the next slide we're wondering more about the cyber security standards and frameworks and which one you're using to handle threats from teleworking?	
18	M.S	Well, it's either a philosophical question or it's a regulatory question. In our world, we are regulated financial institutions. So the big important frameworks or regulations that we have to abide by, is either the Swedish Financial Supervisory authorities, FFFs 2014, colon five, or its European banking authorities. Guidelines for that's called e by gl 2000 1904. So those are the biggest frameworks if you're looking at it from a regulatory standpoint. Just for those we naturally have a foot inside of ISO 27001. So we naturally look towards those. Because we use cards, we absolutely have to adhere to PCI DSS. But to be perfectly honest, those are not the frameworks and standards that we use to handle threats. Because handling threats is principally done by a risk based approach. So when you're a financial institution, you're required to actually assess threats, analyze threats, threat intelligence, you're also required to do risk analysis. So you're analyzing your risks, and you're building up controls and risk structures in accordance with both the regulation but also in accordance with the threats that are applicable for your organization. The answer is really, what are you using to handle progress, it is really in the risk assessment, to be perfectly honest, but then we use a lot of frameworks for governance, more for compliance reasons, we are also independently audited and our independent assurance reporting that is of the isa e 3000 and 42 3 standard.	T-SPO-SF
19	F.S	Alright. I actually think you answered basically all the questions we had on this slide. Because you mentioned that you had the foot in the ISO 27001 and that you must use the PCI DSS so unless I misheard something, you don't use BS 7799?	
20	M.S	I'm actually surprised that you young people even know what that is, because that's the one that I grew up with. But that one is so ancient, we don't use it much. And we use our own frameworks, which are much more modern and agile and COBIT. Our auditors sometimes can use COBIT, but not ourselves.	T-SPO-SF
21	F.S	Okay, okay. Do you use NIST?	
22	M.S	Yes, we are looking at NIST. More and more. So it's becoming more and more important for our business to look at NIST. So that is something that is a big up and comer, though there are some challenges with the NIST as well, because it is a rather extensive and wide framework.	T-SPO-SF

23	F.S	Yes, thank you. Okay. And for the next slide here, then what security practice do you use to ensure safe teleworking for your employees.	
24	M.S	So we have a mobile technology wise, we have a multi layered approach of multiple different measures. There's everything from encrypted traffic, VPN certificates on the devices, endpoint enforcement, encryption, there's a humongous amount of different capabilities technology wise. But one of the most important ones is actually the awareness training. So we have mandatory awareness training towards all our employees, that they have to go through and they also have to get that education when they're completely new, to get on board. And then they have to renew some of the education annually as well.	T-SPO-CP T-SPET S-T-ET S-SPO-CP RT-SPO-CP
25	F.S	Why is that so important for you with the education of employees?	
26	M.S	So basically, the single most important factor that influences security and actually contributes to compromise, especially when you're talking about teleworking is people's behavior. And as a security organization, working with technology to mitigate risks, that is one way. But handling people's behavior is significantly more important than the technology side because technology can never be perfect. Let me give you an example of data leakage prevention. Data leakage prevention is naturally a really good tool. It's there to detect whether or not you've done something that you shouldn't be doing, or someone is maliciously trying to do something. Hence, it's the cat and mouse game, but it is always a couple of steps behind. But if you can lead people towards doing the right things, then it's much easier to avoid the risks that you're faced with when teleworking. For example, teaching them to not to send emails containing personal data and not to send sensitive information. To remember, when you're sharing a document, how you should be sharing it, how you should be collaborating over those.	RT-SPO-CP S-SPO-CP T-SPO-CP
27	F.S	And when you're communicating inside or internally in the organization, do you have any kind of trust indicators when you're communicating over email or teams or whatever?	
28	M.S	How do you mean trust indicator?	
29	F.S	I mean, to ensure that it's not a phishing email or something like that? Do you have a set language to use?	

30	M.S	No, we don't have any set language we use. Our email infrastructure lends itself towards not easily being able to send as an internal sender. So that allows us to have some type of control. But also, inside of the business processes that we have, there's controls built into that. For example, the most common risk one, in most industries, is executive impersonation. If I am sending you an email saying, Hey, you know what, it's really urgent, I need to have this invoice paid very quickly, can you transfer X amount of money to this account, and then it is stated as it comes from our CEO or something like that, and it's sent to someone in accounting. This is a very, very common type of attack. That type of processes that we in our company have controls in place for are those types of transfers. So even if someone would receive something like that, that would still require them to have a sign off from the correct individual inside of the systems, so that they couldn't basically act upon something like that, without that being authorized by that individual. And here again, comes two factor authentication capabilities in and those things. So that allows us to avoid those risks.	RT-SPO-SF S-CS-SE RT-SPO-CP
31	F.S	All right. And you already mentioned some of the cyber security practices that you use to handle this. But you can see here also on the slide that we have listed a few. And you mentioned that you had educational employees and the multi factor authentication?	
32	M.S	So we can say firewalls check, documented security policies, check education of employees check. Plan for mobile devices, check. We only allow our own managed devices, we don't allow to Bring Your Own Device. And the reason for that is that we are moving towards zero trust infrastructure principle. If you read Googles beyond Corp, that is where we're headed. Enforce the safe password practices. Yeah, we take that even one step further, we use two factors. Regular backup of data? Yes. Most of our data and our infrastructure is not handled on devices themselves, it's handled in cloud environments. We are a 100 percent cloud based company. We don't have information that is just laying around. That is operationally significant. It's laying around in other factors. Installation of anti malware, yes, anti malware threat hunting and all those tools on endpoint protection is built in. And then multi factor identification. Yes, well, I mentioned it before.	T-SPO-CP T-SPET S-SPO-CP T-SPO-SF
33	F.S	And then I think you also mentioned that education of employees perhaps could be seen as an extra importance of these?	
34	M.S	We see that as one of the most important areas where we also invest a little bit extra. It also all starts and ends with employees. It's like technology is built by people, so unless you educate the people that build the technology or educate the people that use the technology, it's kind of useless to put a very complex and very advanced tool in	S-SPO-CP

		the hands of someone who doesn't understand why they should be using it. Instead, they will just bring out the hammer and bang away. I don't like that.	
35	F.S	Okay. I think we could move on. Because I think you also mentioned earlier, when you said you took it a step further with the enforced safe password practice. Or are there any others besides these that you have seen here that you use?	
36	M.S	So there is one more capability that we have, for example, we have a security operations center, we have a dedicated team that explicitly works with threat hunting, and threat protection and threat intelligence. So they are completely dedicated for this specific purpose. All right, that is one leverage that we also do properly.	T-SPO-CP
37	F.S	And then, moving on to the next slide. These are more specific cyber security practices, but perhaps to handle force teleworking. We're wondering if you're using any of these, for instance, like DNS filter VPN, BAS, or such?	
38	M.S	DNS filters, if that becomes a security tool. I'll change my job. We can see the use of VPNs. BAS what’s that?	
39	F.S	Breach attack simulation	
40	M.S	Oh, yes, we have a team. We call that the red team. Working with offensive security that is populated by penetration testers and that team that does continuous attacks against our environments and our processes. We have protocols in place for breaches and stuff like that, we have playbooks.	T-CS-MA T-SPO-CF
41	F.S	Alright. Do you see an increase in the use of these practices? Since more and more employees have started working with teleworking?	
42	M.S	We see an increase in all of these practices regardless, so Klarna is on a very, very large growth. So most of these areas are growing whether or not they are due to Covid or not, or forced teleworking, I would not say, because I couldn't really assess it. But I doubt that it would be that because we are capable of teleworking. We went from not teleworking, to teleworking 100 percent, in less than two days. And it wasn't even a hiccup in the organization. We just basically pushed a couple of buttons and ramped up. We multiplied our VPN capability with about 10 times in a matter of hours. So we just increased the capacity. Being cloud based has its advantages.	T-SPO-CP T-SPET S-T-ET S-T-FT
43	F.S	Impressive. And then moving on to the social aspects, which is another aspect that we use. For the first question, we wonder, what is your organizational take on social engineering? And I know you mentioned it a little bit earlier in the interview but we're still	

		wondering if it's a big problem, and how often perhaps hackers or activists or other threat actors are trying to use your employees to reach the internal data?	
44	M.S	But that is continually happening. So it is something that is in the price of doing business as a global company, the more famous and more known you become, the more attacks you have. It's not even something that we statistically even need to track because it's something that we just presume is always there and always is present, as being a bank. And having our customers social engineering is a large problem. But it is a problem for society in general, and dependent on the region where you are, that problem basically, like, is manifested in different ways. So for example, in Sweden, because of our openness, people are trying to convince others to use bank ID and validate things. Phishing attacks and those types of things, most in other countries, that attacks will be fairly different with regard to attacks against our company, that's just about our everyday business. It's nothing that we even concern ourselves with tracking, but we made sure that everyone is well trained to handle it.	RT-T-ET S-CS-SE T-CS-MA S-SPO-CP
45	F.S	And I know you also mentioned earlier that you gave or provided training and education to your employees. But you said that you do it annually. But we wonder if you have added perhaps an extra training due to the forced teleworking, since COVID-19?	
46	M.S	No. Oh, wait a second. Yes, we added some extra. We added some extra education and provided extra materials towards our customer services area because they were not doing teleworking prior to this. So that's where we added extra. Yes.	S-T-ET S-T-FT RT-SPO-CP
47	F.S	Right. And we also want to know, how has the evolution of teleworking been in the context of organization, you said that you went in a couple of days from some teleworking to 100 percent. But if you look back perhaps two, three years, like how has the evolution been? And what are the effects of this?	
48	M.S	If you look at it historically, Klarna has been mostly focused around working from the office in the very beginning. And then we gradually grew to more and more of a global company. And with the growth and with the expansion teleworking become more and more. You also see that post Covid, there are two phases that you could actually distinguish in changes. One where all our employees become teleworkers. And then the second phase, which is very shortly afterwards is basically where all our service providers, employees are then starting to telework. And because of them doing a change, we need to control that they are doing it in the correct manner. So in	S-T-TT

		those cases, we have to work with some of our vendors to ensure that they have good enough practices and good enough controls, and in some cases, actually switch vendors because they didn't have sufficient capabilities that were enough for us. And then we could move over the volume to another service provider.	
49	F.S	Okay. I think you actually answered all the questions here. So I think we can move on to the next slide. And that's our last aspect. It's two slides on this aspect, and it's called the Risk Tolerance. The first question here is if your organization were prepared for letting the employees telework, when Covid 19 came?	
50	M.S	They were fairly prepared. So all the basic aspects were there. There were some things that needed to be refreshed. We had to improvise a little bit and take our principles and apply them towards our service providers. But other than that, it felt like we were very well prepared. So even those things were quite easy to adopt.	RT-T-ET RT-SPET
51	F.S	And did you see any security risk when the scale up of teleworking happened?	
52	M.S	There is a marginal increase in security risk regardless, because you're moving from a well controlled, well defined physical space, especially with customer service agents, and those, to something that is more of a home environment. And where each individual employee needs to enforce the state and capabilities in their own environment, making sure that nobody overhears and making sure that nobody sees your screen and so on. So that becomes naturally a different risk. Whether or not that is a large risk, I would not say it's a large shift in risk. It's just a shift in how the risks are managed, and how the risks are manifested.	S-T-ET S-T-FT RT-T-ET
53	F.S	Okay. Next question, perhaps it's a product of the training and education that you provide, but we're wondering what level of understanding the employees or organization have of the threats that might occur when you're teleworking?	
54	M.S	I think most of them have a good understanding about the risks.	S-SPO-CP RT-SPO-CP
55	W.H	A question there. Would you say there is a difference of understanding depending on what generation the employees are from?	

56	M.S	I would definitely think that in most companies that have a generational diversity, you can see a difference. But at Klarna, we don't have a big generational diversity. At Klarna, I am considered old and I'm 46. And that may explain to you that the ones that are considered old at Klarna are employees that are very tech savvy that can fit in with the younger generation. At Klarna many of our employees grow up with the internet and are a part of the millennial generation. So no, at Klarna we don't have a big generational knowledge gap.	RT-SPO-CP RT-T-ET S-T-ET S-SPO-CP
57	F.S	And how well do the employees of your organization know about the security practices that you use?	
58	M.S	They know how we apply those frameworks. I would say it's a fool's errand to get all your employees to understand and follow a framework of a standard. Like if I tried to teach every employee an ISO 27000 standard, I would have to work on that task for the rest of my life without succeeding. But on the other hand it is very very important for the employees to understand the routines, the processes and the controls and structures that we have in place. Again, here comes the importance of the user training materials. We don't focus on training them in all the regulatory requirements, instead we boil them down into what we actually do and what you should be doing as a user in different circumstances. Because there's no point in training you about the governance structures or what to deal with, but there's a very good reason to tell you what to do if you get a phishing email, what button you should be clicking on and what not and who you should be asking about this.	RT-SPO-SF S-SPO-CP
59	F.S	I think all of us agree with you that it is impossible for everyone within the organization to know but it might however be important for them to know that you are working with a structured way on how to handle threats and risks. And now for the last slide here, we are wondering if you see a difference between different departments of the organization regarding the knowledge about security practices?	
60	M.S	No, I would honestly say that, of course there is a difference between security professionals and engineers, versus non professionals. There will somehow always be a technical knowledge gap. But we track all our awareness trainings and the results of those awareness trainings and to be perfectly honest we even do some test on that throughout the organization, with phishing campaign tests and stuff like that, and we don't see a significant difference in the level of understanding maturity among the different parts of the organization, so easily I don't think there is a difference. Technology people or engineers and security people have just a greater ability to understand those threats.	RT-SPO-CP S-SPO-CP

61	F.S	Okay, and what departments seem to be more likely to be attacked and which departments might actually suffer from more attacks?	
62	M.S	I think anything that is surrounding financial processes and executives are more likely to be attacked, threat actors have become more and more professional in directing their attacks towards the right targets, identifying the right individuals rather than the right groups, they don't send out phishing spams to a very large population, they direct them, they write them explicitly designed to you, sending you William an email saying "Hey William, this is Mark, really nice to have this conversation, here is a file that I put together with some of my thoughts and that would basically be it, all based on you, writing something just based on Facebook or LinkedIn or some other site from Social media that "I really had a good conversation with Mark earlier today". So that type of directed communication. But where you see that more and more is where they have identified their business functions, sending directed attacks to those people that have a relevant narrative and a relevant content towards what you are trying to address. So our CFO sending an email to our CEO saying here is the latest financial results or sending out to a manager saying, hey here is the promotion number in a spreadsheet. So those types of attacks we see more predominantly in the later couple of years but I cannot really say they are due to the Covid working from home kind of thing, but many people think so.	T-CS-MA RT-SPO-CP RT-T-ET
63	F.S	Unfortunately we have only a few minutes left before we have to run to another meeting actually but we will try to ask our last question here and that is if you see that employees with more knowledge about security practices within teleworking are more risk taking than those that are not.	
64	M.S	Difficult to say. Calculated risk taking, I would say that security people are a little bit more, they understand that just clicking a link does not always mean that you infect the computers but there are more steps to it but that could also lead to some kind of overconfidence. The difference is marginal, it is like very marginal, but I would imagine that some kind of overconfidence from some security people or engineers could exist.	RT-SPO-CP RT-SPET
65	F.S	Thank you so much for your time!	

Appendix 6

Email from Stora Enso:

“På detta tema kan jag redan nu dela med mig av en summering som jag gjorde till Combient tidigare.

==
Kort, ingen skillnad eller någon nämnvärd förändring i vår IT säkerhet. Bakgrunden är att vi hade redan före Corona en väl utvecklad modell för fjärrarbete framtagen från ett behov av att kunna ge en säker arbetsplats för alla av våra kollegor som reste mellan kontor, kunder eller leverantörer.

Som en teknisk bakgrund så krypterade vi alla våra laptops och installerade vid leverans programvaror för fjärranslutning till interna nätverket, avancerat skydd mot elakartad kod samt automatiska uppdateringar av alla programvaror. Så den fysiska platsen en Stora Enso dator befinner sig spelade ingen roll för vår IT säkerhet.

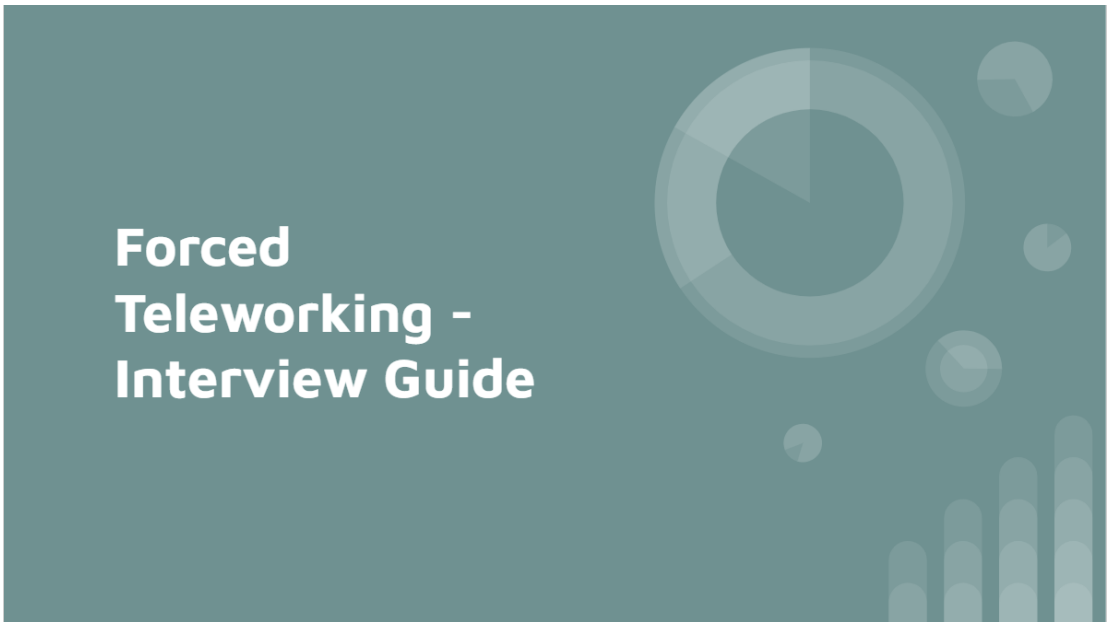
Ja, vi noterade fler säkerhetsincidenter från anslutna USB enheter när våra anställda satt i hemmiljön men de hoten spärrades och resulterade inte i störningar, och vi har sett en ökning av incidenter från phishing emails men processen för att spärra lösenordet och kommunicera nya via mobiltelefoni fungerade redan väl. Naturligtvis så spelar det roll att tjänsterna för fjärrarbete skalade upp från före Corona ett par tusen dagliga användare till över tio tusen på bara en vecka, utan driftstörningar.

Det finns en liten skillnad och det är att vi har ingen filtrering av Internet accessen i hemmiljön så det är nu möjligt att besöka tvivelaktiga websidor, men skyddet av länkar och bilagor till email samt nerladdade filer eller kod i webbsidor fungerar precis likadant oavsett var våra anställda befinner sig så det kompenserar för den oskyddade Internet accessen.

Det finns andra observationer som inte är säkerhetsrelaterade som kan noteras, att anställda känner en större stress från fler möten än före Corona och hemarbetet, detta beroende att tidigare förlorad arbetstid i olika fysiska möten eller resor, tid som nu istället används för både planerade och oplanerade möten. Eller att olika kreativa lösningar för teamutveckling testats som virtuella After work, eller virtuella kaffepauser.”

Appendix 7

The PowerPoint presentation that was used during the interviews.



Intro

- Permission to record the interview?
- Ok to use your name, role and organization in our transcription - it will be published on Lund's internet library
- Same goes for in the actual thesis
- *Our purpose with the thesis*
- Focus on the time frame from March 2020

- What is your name and role?
- Are your organization teleworking? When did it start? Is it forced? How many percent of the employees are teleworking?

Malware is a term combinated between the words, "malicious" and "software" to describe a software or code that criminals, often called hackers, use to infect and infiltrate computers, networks and data (Cisco, n.d).

Technical Aspect

- What challenges and threats do you see with forced teleworking in an IT-security perspective for your organization?
- Have you had any problems with some kind of malware attack towards your organization since March 2020?
  What happened? *How was it handled? What did it cost?*
  What kind of attack?
- Have you seen an increase in the number of malware attacks?

Technical Aspect

-Can you rank these types (from the most common to the least common) of malware attacks regarding threats for your organization when teleworking?

- **Viruses**
- **Ransomware**
- **Scareware**
- **Worms**
- **Phising**
- **Spyware**
- **Trojans**
- **Adware**
- **Fileless malware**

Technical Aspect

-Are you using any cybersecurity standards and frameworks to handle the threats from teleworking?

-Are you using any of these cybersecurity standards and frameworks to handle the threats from teleworking?

ISO27001
BS 7799
PCIDSS
ITIL
COBIT

-*Anyone you see as extra important?*

-Any other cybersecurity standards or frameworks you use?

Technical Aspect

-What security practices do you use to ensure safe teleworking for your employees?

-Do you use any of these cybersecurity practices to handle the threats from teleworking?

Firewalls
Document cybersecurity policies
Education of employees
Plan for mobile devices (BYOD)
Enforce safe password practice
Regularly back up data
Installation of anti-malware software
Multi-factor identification

-*Anyone you see as extra important?*

-Any other cybersecurity practices you use?

Technical Aspect

-Have you used any specific cybersecurity practices to handle the forced teleworking? For example DNS filters, VPNs, BAS, protocols or such.

-Do you see an increase in the use of these practices due to a growing number of teleworkers?

Social Aspect

-What is your organizational take on Social Engineering? Is it a big problem for your organization? Are hackers trying to use your employees to reach internal data and systems etc.?

-Do you give trainings and education to your employees to minimize the threat from social engineering?
-How often? Have you added extra training due to forced teleworking?

-Do you have policies for your employees on how to telework to minimize the threat from hackers?

-How has the evolution of teleworking been in the context of your organization? Is it many more employees teleworking now? Effects of this?

-How has the forced teleworking affected the employees of your organization?
-Do they have to work in a different way then before to keep devices and networks etc. secure?

Risk Tolerance

-Was your organization prepared for letting the employees telework when Covid-19 came?
-Did you see an increased security risk when an increased number of employees telework?
- What level of understanding does the employees of your organization have of the threats that might occur when teleworking?
- Do you consider they were/are prepared from an organizational point of view?

- How well do the employees of your organization know the security practices of your organization?

- Do the employees have an idea of what framework/standard your organization follows?
- How important do you think it is for employees to know about the standard that your organization follows?

Risk Tolerance

- Do you see a difference between departments of your organization about the knowledge of security practices?
What departments seem to be more likely to get attacked, and which departments suffer from more attacks?

- Do you see that employees with more knowledge about security practices in teleworking are more risk taking?

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3), 183-196.

Abukari, A. & Bankas, E. (2020). Some Cyber Security Hygienic Protocols for Teleworkers In Pandemic Period and Beyond. *International Journal of Scientific & Engineering Research* Volume 11, Issue 4, 1401 ISSN 2229-5518.

Babulak, E. (2009). Teleworking and next generation cyberpace. *In 2009 International Conference on Computational Intelligence, Modelling and Simulation* (pp. 142-146). *IEEE*

Bakac, C., Zyberaj, J., & Barela, J.C. (2020). PREDICTICTING TELECOMMUTING PREFERENCES AND JOB OUTCOMES AMID COVID-19 PANDEMIC: A LATENT PROFILE ANALYSIS. *CAFER BAKAÇ1*.

Baruch, Y. (2001). The status of research on teleworking and an agenda for future research. *Blackwell Publishers Ltd*.

Baruch, Y. (2002). Teleworking: benefits and pitfalls as perceived by professionals and managers. *New technology, work and employment*, 15(1), 34-49.

Bélanger, F & Allport, C. (2008). Collaborative technologies in knowledge telework: an exploratory study. *Information Systems Journal*, vol. 18, no. 1, pp. 101-121.

Belzunegui-Eraso, A., & Erro-Garcés, A. (2020). Teleworking in the Context of the Covid-19 Crisis. *Sustainability*, 12(9), 3662.

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices, *2nd edn, Tampa: A. Bhattacherjee*.

Binchus, C. (2021). Timeline of communication technology. Spie. Available online: https://spie.org/news/photonics-focus/janfeb-2021/a-timeline-of-communication-technology?SSO=1 (Accessed 01/04-2021).

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: a socio-technical perspective, part II: the application of socio-technical theory. *MIS quarterly*, 11-28.

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. *In Proceedings of the International Conference on Technology, Education and Development, Valencia, Spain* (pp. 6-8).

Brenner, J. (2007). ISO 27001 risk management and compliance. *Risk management*, *54*(1), 24-29.

Broderick, J. S. (2005). Firewalls–Are they enough protection for current networks?. *Information Security Technical Report*, *10*(4), 204-212.

Buchholz, K. (1995): CRITERIA FOR THE ANALYSIS OF SCIENTIFIC QUALITY, *Institute for Carbohydrate Technology at the Technical University Braunschwei, Scientometrics*, Vol. 32, No. 2, pp.195-218.

Burke Johnson, R., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come, *SAGE Journals*, vol. 33, no. 7, pp. 14-26.

Cambridge Dictionary (n.d). Meaning of Forced in English. Available online: https://dictionary.cambridge.org/dictionary/english/forced (Accessed 28/04-2021).

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44.

Cisco. (n.d-1). What is Malware? Cisco. Available online: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (Accessed 07/04-2021).

Cisco. (n.d-2). What is Phishing? Cisco. Available online: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works (Accessed 19/04-2021).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber security. *Technology Innovation Management Review*, 4(10).

Dery, K., Sebastian, I. & van der Meulen, N. (2017). The Digital Workplace. *MIS Quarterly Executive.*

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, pp. 1128-1133.

Efron, S.E. & Ravid, R. (2019). Writing the Literature Review: A practical guide. *New York : The Guilford Press*.

European Commision. (n.d). SME definition. Available online: https://ec.europa.eu/growth/smes/sme-definition_en (Accessed 30/03-2021).

Evangelakos, G. (2020). Keeping critical assets safe when teleworking is the new norm. *Network security, 2020* (6), 11-14.

Fairweather, N. (1999). Surveillance in Employment: The Case of Teleworking. *Journal of Business Ethics* 22: 39-49.

Firch, J. (2021). 10 Cyber Security Trends You Can't Ignore In 2021. PurpleSec. Available online: https://purplesec.us/cyber-security-trends-2021/ (Accessed 07/04-2021).

Gikas, C. (2010). A general comparison of fisma, hipaa, iso 27000 and pci-dss standards. *Information Security Journal: A Global Perspective*, *19*(3), 132-141.

Golden, T. (2007). Co-workers who telework and the impact on those in the office: Understanding the implications of virtual work for co-worker satisfaction and turnover intentions. *Human relations*, 60(11), 1641-1667.

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, 21(2), 135-146.

Gratton, L. (2004). The democratic enterprise: Liberating your business with freedom, flexibility and commitment. *Pearson Education*.

Greenhill, A., & Wilson, M. (2006). Haven or hell? Telework, flexibility and family in the e-society: A Marxist analysis. *European Journal of Information Systems*, 15(4), 379-388.

Griffith, T. & Dougherty, D. (2002). Beyond socio-technical systems: introduction to the special issue. *Journal of Engineering and Technology Management*, [online] 19(2), pp.205–216.

Gupta, M. & Sharman, R. (2009). Handbook of Research on Social and Organizational Liabilities in Information Security. *IGI Global.*

Harris, L. (2003). Home-based teleworking and the employment relationship: Managerial challenges and dilemmas. *Personnel Review*, Vol. 32 No. 4, pp. 422-437.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2019). Improving employees' intellectual capacity for cyber security through evidence-based malware training. *Journal of Intellectual Capital*.

Ingham, K., & Forrest, S. (2002). A history and survey of network firewalls. *University of New Mexico, Tech. Rep*.

Johnston, S. (2017). Meet the new Hangouts. *Google blog.* Available online: https://www.blog.google/products/g-suite/meet-the-new-enterprise-focused-hangouts/ (Accessed 01/04-2021).

Kearns, G. S. (2016). Countering mobile device threats: A mobile device security model. *Journal of Forensic & Investigative Accounting*, *8*(1), 36-48.

Kenning, M. J. (2001). Security management standard—iso 17799/bs 7799. *BT Technology Journal*, *19*(3), 132-136.

Klarna (n.d). Om Oss. Available online: https://www.klarna.com/se/om-oss/ (Accessed 28/04-2021).

Kilpi, A. (2020). Practical Factors of Successful Telecommuting. *Metropolia University of Applied Sciences.*

Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication. *Journal of Information Processing Systems*, *7*(1), 187-198.

Kowalski, K. & Swanson, J. (2005). Critical success factors in developing teleworking programs. Benchmarking: *An International Journal*.

Krishna, S., Nicholson, B. & Sahay, S. (2003) Global IT Outsourcing. Cambridge University Press. Lee, A.S., 1991. Integrating positivist and interpretive approaches to organizational research. *Organization science, 2(4),* pp.342-365.

Krisinformation (2021). Anställda, arbetsgivare och företag. *Myndigheten för samhällsskydd och beredskap.* Available online: https://www.krisinformation.se/detta-kan-handa/handelser-och-storningar/20192/myndigheterna-om-det-nya-coronaviruset/arbetsgivaretagare (Accessed 28/04-2021).

Kvale, S. (2008). Doing interviews. *Sage.*

Lee, A.S., 1991. Integrating positivist and interpretive approaches to organizational research. *Organization science*, 2(4), pp.342-365.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

Liu, Y., Zhong, Q., Chang, L., Xia, Z., He, D., & Cheng, C. (2017). A secure data backup scheme using multi-factor authentication. *IET Information Security*, *11*(5), 250-255.

Mann, S., & Holdsworth, L. (2003). The psychological impact of teleworking: stress, emotions and health. *New Technology, Work and Employment,* 18(3), 196-211.

Martínez-Sánchez, A., Pérez-Pérez, M., de-Luis-Carnicer, P., & Vela-Jiménez, M. J. (2006). Teleworking and New Product Development. *European Journal of Innovation Management.*

McAfee. (n.d). What is Malware? McAfee. Available online: https://www.mcafee.com/en-us/antivirus/malware.html (Accessed 07/04-2021).

McIntyre, A. (2018). Developing a Cyber security Protocol for Your Operational Environment. *Natural gas & electricity*, *34*(9), 23-27.

Mello, J. A. (2007). Managing telework programs effectively. *Employee Responsibilities and Rights Journal*, *19*(4), 247-261.

Morgan, S. (2020). Cybercrime To Cost The World 10.5 Trillion Annually By 2025. *Cybercrime Magazine.* Available online: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed 07/04-2021).

Nastase, P., & Ionescu, C. (2011). THE IMPACT OF TELEWORKING ON THE AUDIT MISSION. *Accounting & Management Information Systems/Contabilitate Si Informatica De Gestiune*, 10(3).

Nilles, J. (1991). Telecommuting and urban sprawl: mitigator or inciter? *Transportation, 18*(4).

Patton, M. Q. (2015). Qualitative Evaluation and Research Methods. *4th ed. SAGE, Thousand Oaks (CA),* ISBN 9781412972123.

Pearce, J. A. (2009). Successful Corporate Telecommuting with Technology Considerations for Late Adopters. *Organizational Dynamics 38*(1):16-25.

Pyöriä, P. (2011). Managing telework: risks, fears and rules. *Management Research Review*.

Randolph, J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research, and Evaluation*, *14*(1), 13.

Qvortrup, L. (1998). From teleworking to networking: definitions and trends. *Teleworking: international perspectives. from telecommuting to the virtual organisation*, 21-39.

Rathore, H., Agarwal, S., Sahay, S. K., & Sewak, M. (2018, December). Malware detection using machine learning and deep learning. *In International Conference on Big Data Analytics (pp. 402-411)*.

Recker, J. (2013). Scientific Research in Information Systems: A Beginner's Guide. *Springer, Berlin Heidelberg, E-book*, ISBN 9783642300486.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cyber security: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 21582440211000049.

Review, C. and Brumma, F. (2016). DigitalCommons@ILR DigitalCommons@ILR Telework is Work: Navigating the New Normal Telework is Work: Navigating the New Normal. *Cornell HR Review*.

Rikitake, K., Kikuchi, T., Nagata, H., Hamai, T., & Asami, T. (2001). Security Issues on Home Teleworking over Internet. *IEICE Technical Report IA2001-20*, 101(440), 9-16.

Roig, M. (2006). Ethical writing should be taught. *BMJ, 333* (7568), pp.596–597.

Ruoti, S., Andersen, J., & Seamons, K. (2016). Strengthening password-based authentication. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS}).*

Ryan, F., Coughlan, M. & Cronin, P. (2009). Interviewing in qualitative research: The one-to-one interview, Research methodology series. *International Journal of Therapy and Rehabilitation, EBSC*, Vol 16, No 6, pp.309–314.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In *2008 Second Asia International Conference on Modelling & Simulation (AMS)* (pp. 749-753). IEEE.

Salomon, I. and Salomon, M. (1984). Telecommuting: The employee's perspective. *Technological Forecasting and Social Change*, 25(1), pp.15–28.

Scania (n.d). Om oss på Scania. Available online: https://www.scania.com/se/sv/home/experience-scania/about-us.html (Accessed 28/04-2021).

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research, *Information and Organization*, vol. 21, no. 1.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian journal of science and technology*, *5*(2), 2170-2176.

Sica, G.T. (2006). Bias in research studies. *Radiology*, 238(3), pp.780–9.

Skype (2012). Skype Timeline. Available online: https://blogs.skype.com/wp-content/uploads/2012/08/skype-timeline-v5-2.pdf (Accessed 01/04-2021).

Souppaya, M., & Scarfone, K. (2016). Guide to enterprise telework, remote access, and bring your own device (BYOD) security. *NIST Special Publication*, *800*, 46.

Stora Enso (n.d). About us. Available online: https://www.storaenso.com/en/about-stora-enso (Accessed 28/04-2021).

Sturges, J. E., & Hanrahan, K. J. (2004). Comparing telephone and face-to-face qualitative interviewing: a research note. *Sage Journals*, 4(1), 107-118.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

SVT (n.d). About SVT - SVT Om oss. Available online: https://omoss.svt.se/about-svt.html (Accessed 28/04-2021).

Timmins, F., & McCabe, C. (2005). How to conduct an effective literature search. *Nursing standard*, *20*(11), 41-47.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.

Von Solms, B., & von Solms, R. (2018). Cyber security and information security–what goes where? *Information & Computer Security*.

Vrchota, J., Maříková, M., & Řehoř, P. (2020). Teleworking in SMEs before the onset of coronavirus infection in the Czech Republic. *Management: Journal of Contemporary Management Issues*, *25*(2), 151-164.

Waboba (n.d). About Us - Waboba. Available Online: https://www.waboba.com/pages/about-us (Accessed 28/04-2021).

Walsham, G. (2006. Doing interpretive research. *European journal of information systems*, 15(3), pp.320-330.

Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, M. (2013). Security risks in teleworking: a review and analysis. *The University of Melbourne.*