'Working from home increases the chance of infection'

Understanding organizations' approaches to managing cybersecurity challenges related to high levels of teleworking: a multi-actor perspective

by

Tim van Veen

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on Wednesday August 24, 2022

Student number:	4469895	
Project duration:	February 1, 2022 – August 24, 2022	
Thesis committee:	dr. S.E. Parkin,	TU Delft, First supervisor
	K.L.L. van Nunen,	TU Delft, Second supervisor
	Prof. dr. M.J.G. van Eeten,	Chair

An electronic version of this thesis is available at
http://repository.tudelft.nl/to-be-continued.

TU Delft

Acknowledgements

Dear reader,

This thesis in front of you started seven months ago and would not be here without the tremendous help of a few of you. First of all, my graduation committee: I am very grateful for the constant feedback Simon Parkin provided, the fruitful discussions we had and especially his patience. Although I sometimes struggled with this study, I not only learned a lot from his experience and knowledge regarding research in the cybersecurity field, but he also made me aware of the importance of relevance. Furthermore, I would like to thank the other members of the committee Karolien van Nunen and Michel van Eeten for the provided feedback and suggestions during our meetings. It was a pleasure to work under the supervision of this committee.

Without the respondents that took their time to participate in an interview, writing this thesis would not have been possible. Many thanks to all the participants and the individuals that brought me into contact with the interviewees. I wrote this thesis during my internship at PwC where I have met a lot of new people that supported me, especially the weekly meetings were very helpful with my coach Reyer Sikkel. As this has been a great experience, I will stay at PwC after graduation, which I am very excited about.

Last but not least, I would like to thank my family and friends. I must admit that this has been one of the most challenging phases of my time in Delft. The setbacks were much more bearable with your support and encouraging words.

Overall it has been an exciting project where I've learned a lot and spoke to some very interesting people. I hope that for some of you who will be reading this paper, the findings are helpful in any way.

Tim van Veen
Delft, August 2022

Executive Summary

This study investigates organizations' approaches to managing cybersecurity challenges that are associated with high levels of teleworking. Over the last two and a half years the pandemic forced organizations to implement teleworking models that resulted in a large share of the workforce working from home. Organizations were not prepared for such unpredictable event. The time constraint and pressure to adjust to this new environment and change their IT infrastructure led to organizations being exposed to more security vulnerabilities that led to an increase in cyberattacks. Organizations were more worried than ever about their ability to handle cyberthreats, while at the same time they sidestepped on their cybersecurity to implement a proper teleworking model. There is a large body of literature showing what the security risks and practices are related to these high levels of teleworking, while it is not clear what the related security challenges are and how organizations are approaching these. So there is a gap in the literature regarding the understanding of the current cybersecurity challenges and approaches that are associated with these high levels of teleworking. Furthermore, there is a clear need to support organizations to improve their cybersecurity, which led to the following question:

> *"How did the increasing use of teleworking affect organizations' approaches to managing cybersecurity challenges?"*

To gain a deeper understanding of this problem, a more qualitative exploratory approach seemed the best fit for this study due to the combination of this topic being highly complex and the current literature suffering severe limitations due to the lack of known challenges and responses. A literature review has been conducted to understand the security risks related to high levels of teleworking and available practices. More important, data has been gathered from sources that possess up-to-date information regarding the cybersecurity challenges of organizations and their approaches. Therefore, the decision has been made to conduct semi-structured interviews with individuals that have this knowledge. These actors were split into two categories to obtain different perspectives. Consultants from various organizations that support other organizations managing their cybersecurity and individuals that fulfill certain roles that make them responsible for the cybersecurity management of their own organization. Both groups are expected to have a different perspective given their interests and responsibilities.

The interview protocol derived from the identified sub-questions and theory that contribute to answering the main research question. After the introductory questions, the first questions focused on the phase of teleworking and how organizations were affected by these high levels of teleworking. Secondly, questions were asked regarding the organization's cybersecurity risks and threats and what challenges they are experiencing in managing such risks and threats. The last questions focused on how organizations are approaching these challenges. Four consultants and five individuals with relevant roles in organizations were interviewed. Subsequently, transcripts were made from these recorded interviews. Thematic analysis has been chosen as the method to analyse the interview transcripts since this allows the researcher to identify patterns in the data that are deemed important. The thematic analysis and literature review resulted in four identified main security challenges organizations are facing and four approaches used to manage these challenges.

The first identified cybersecurity challenge is 'Privacy vs. security' which shows how organizations struggle with securing the private environments of their employees without invading their privacy. As with these high levels of teleworking, a large share of employees' private environments became part of the organizations' infrastructures. The second challenge is 'Control vs. awareness', which addresses the balance between control and awareness. More restrictions can lead to less security if there is a lack of awareness and knowledge among employees. Due to the high levels of teleworking, organizations lack the ability to fully monitor and control the private environment, which made them more dependent on the awareness of their employees. Thirdly, the 'Lack of resources' challenge, not all organizations have the monetary resources to achieve the desired level of security. More importantly, the current labour shortage and the extra attention towards cybersecurity has received the last years resulted in a lack of skilled people, especially for smaller organizations. The increase in teleworking strengthened

this demand, since it made organizations more vulnerable. Finally, the 'Priorities' challenge shows how according to the consultants cybersecurity is still seen as a burden and is being neglected by organizations, regardless of the increase in cybersecurity attention and the increased risks related to high levels of teleworking.

The identified approaches started with 'Technology & Processes', as this is often the first choice of organization to manage cybersecurity. A distinction is made between mature an less mature organizations, more mature organizations use proper device management systems to guarantee a high level of security without invading employees' privacy. While for organizations that use BYOD there is a possibility to use an enclave that give them the possibility to secure private devices, without breaches employees' privacy and requiring too many monetary resources. However, the physical private environment remains out of the reach of organizations. Secondly, the 'Education of the workforce' which is deemed to be one of the most successful approaches, especially since awareness plays a significant role in the second identified challenge, since the private physical environment is hard to secure, education can provide the required knowledge and awareness for proper cyber hygiene. Furthermore, 'Establishing security culture' is a counter-intuitive approach that describes how it is not possible to reach the desired level of security without culture. Organizations are integrating security into the daily roles of all individuals in the organization, giving responsibilities and nudging them with discussions instead of forcing them by too many controls. Such an approach might be especially effective to counter the 'control & awareness' challenge, since too many controls can be counterproductive. The last approach 'Pandemic as a priority trigger' is not a specific approach, but shows how organizations currently have the desire to become more mature although it lacked effort in the past. Despite this still being challenge, organizations are currently giving cybersecurity a higher priority. However, since every organization is different, it depends how high is how enough and consultants might think it can never be high enough. Some organizations also started exchanging treat information with other companies and making it public information, this benefits less mature organizations that do not have the resources and in the end the organizations that share this information benefit from their improved security since they are often part of the supply chain as well.

Since the data sources were two different groups of actors, it is important to understand the differences between these groups in the findings. The 'Priority' challenge has not been addressed by the organizations. The reason can be that they do not want to disclose their organization not prioritizing cybersecurity or given the positions, it shows that these organizations have security as a high priority. There is also the possibility that organizations are prioritizing the improvement of cybersecurity, but can not achieve their desired level due to other challenges. Another possibility is that progress is being made due to prioritizing, but the results are not yet visible to the consultants as this takes time to show. Furthermore, consultants did not address the 'Establishing security culture' approach. It could be that since such culture takes years to develop, consultants are not heavily involved in such-long term goals.

This study created an overview and understanding of the main cybersecurity challenges related to the increasing use of teleworking and the approaches taken by organizations to manage these challenges. These challenges show the difficulties organizations are perceiving when managing related security risks and threats. Furthermore, this research reveals how organizations are responding to these challenges and how improving cybersecurity is not always possible. This knowledge is not only an addition to the current body of literature, but can also support organizations by helping them improve their cybersecurity with the provided understanding. This research can be especially helpful for smaller organizations that do not have the ability to allocate a lot of resources to cybersecurity. Not only organizations benefit from improved cybersecurity, in the end society as a whole benefits from secure organizations, especially critical infrastructure.

With such broad scope, there are also limitations and possible future research that should be addressed. This study focused on organizations in general, while the findings also indicate that the identified challenges and approaches differ between various types of organizations. Future similar research can focus on one specific industry or on a maturity level to avoid these limitations. Additionally, the order of the interviews could have affected the outcome, since data from previous interviews was used during the upcoming interviews. Also, since the fact that the thematic analysis was performed by only one researcher, the performed analysis depended on the judgement and interpretation of only one interviewer. Future research can focus on specific identified challenges like 'Security vs. Privacy and study how employees perceive this challenge. Or the 'Control & Awareness' challenge and identify

motives to comply or not comply with certain security controls.

Lastly, despite the pandemic being an important part of the reason why teleworking levels have rapidly increased over the years, the main focus of this research was not to show the impact of the pandemic or the restrictions imposed by the government. At the moment this study started, organizations had two years to adjust to this new environment, which might have made the 'shock of the pandemic' a less valid argument and might have resulted in different security challenges and approaches. Just after the start of this research, the environment changed again as the restrictions that forced organizations to let their employees work from home dropped. This research found that the levels of teleworking are still relatively high and there is likely a shift going on from the use of a crisis-induced teleworking model to a more conventional teleworking model, but this is a limitation of this research. Future research can possibly look into the impact of the dropped restrictions on cybersecurity related to teleworking.

Contents

List of Figures

List of Tables

1 Introduction

1.1. Background

Over the past two years the COVID-19 pandemic left a global trail of destruction. While a lot of businesses and societies have suffered during this period given the 3.6 % fall of global GDP, the pandemic seems to act as a catalyst for the digital transformation as worldwide IT spending is projected to rise by 8.4 % in 2021 [1] [2]. For the sake of protecting public health, the pandemic pushes large-scale adoption of work-from-home technologies and overall greater IT service management. There are currently a lot of organizations that carefully try to bring employees back to the office. Although in some capacity people moved back to working in the office, not the full-time as we are used to pre-covid. According to a survey done in the US 39% of the employers require employees to be back in office full-time, while only 29 % of the employees actually want this. There also have been made a lot of changes in the physical offices, more than 1 in 5 offices reduced space since the start of the pandemic and a lot of tech upgrades have been made [3]. So it seems that these high levels of teleworking will not dissapear in the near future and will likely become the new norm. Unfortunately, as most organizations and individuals shifted their former physical activities into the 'safe' digital world, another virus was lurking around the corner.

A significant increase in cyberrisks was the result of the alternation of socioeconomic systems caused by the pandemic [4]. The first quarter of 2021 showed a 17% increase in the number of attacks compared to Q1 of 2020 [5]. Moreover, according to IT giant IBM, the cost of an average data breach has risen to 4.24 million dollars, the highest cost in history. Another interesting finding from this report is that organizations that have 60% or more employees working remotely have a higher average cost of a breach than the overall average [6]. As the number of attacks and the costs rise, it is clear that the partially forced digital transformation results in challenges regarding cybersecurity. While this transformation keeps progressing, it is of vital importance to reduce cyberrisks to ensure digital security and stop the ongoing uptrend of cyberthreats while protecting business continuity.

Unfortunately, there is not one predefined solution to solve this problem, just as there is none for physical crime. How cyberrisks can be effectively minimized could differ for each organization in various industries. Moreover, the chief information-security officers of certain organizations do not have experience with this unusual and uncertain pandemic that could be used as guidance [4]. This is especially important these years compared to other years, given the combination of the negative economic impact of the pandemic and the increase in cyberrisks. Cybersecurity can be an immense expense for an organization and during such pandemic there might not be enough resources nor priority to identify, prevent and mitigate all the critical risks. Not considering cybersecurity risks as an organization, especially organizations that have already suffered from the pandemics effects, might cause more vulnerabilities to be exploited which could lead to a financial catastrophe.

1.2. Problem statement & Knowledge gap

Given the fact that currently there is a significant increase in cyberrisks and the number of attacks, combined with increasing costs of data breaches, there is a great need for reversing this trend [5]. Due

to the unusual and uncertain characteristics of the pandemic, there is not one pre-defined playbook to solve this security threat in a rapidly growing digital world. Despite the widespread consensus that there currently are currently several cybersecurity challenges related to teleworking, there does seem to be a lack of consensus regarding what the main challenges currently are.

According to Wang and Alexander who conducted research in April 2021, employees are expected to work at home only with the use of VPNs, which provide limited security. This forced teleworking is not only a problem for existing organizations, but as well for the increasing number of work-from-home companies [7]. As there is an urge to ensure security improvements at home, the costly pandemic may have caused certain organizations to have a lack of resources for such solutions. Although not all the organizations have a lack of resources due to the pandemic, some organizations were actually able to prosper financially. Research conducted in the beginning of June last year in Montenegro concluded that the degree of resilience to cyberrisks will in the future become one of the key factors determining the efficiency of an organization. So not investing to reduce cyber risks does not seem like a valuable option. The authors have proposed several actions, like developing innovative defence mechanisms in organizations and educating the employees to improve their digital skills [8].

Even earlier in late November 2020, research was conducted at a University in Virginia. Analysis of the interviews shows that employees do trust cybersecurity protocols laid out by the organization during the pandemic, yet they believe the protocols are not as secure as in-person and still feel vulnerable [9]. This supports the proposed action of the researchers in Montenegro concerning the improvement of digital skills, as experiencing a lack of security and feeling vulnerable might be the result of these skills being underdeveloped. A European study published in February 2021 evaluated the cybersecurity culture readiness of organizations by using surveys. Among other things, they found that 53 % of the respondents did not receive any cybersecurity guidelines from their organization regarding teleworking during the pandemic. This article recommends scientific researchers to emphasize the importance of security adjustments in businesses as teleworking becomes the norm. Moreover, research' focus should be more on all security characteristics as the human factor is key to ensuring information security but often seems to be untouched [10]

Multiple articles propose various solutions for the worsening cyber security issue, while the statistics do not seem to report many effective solutions being used. It might be that budget is one of the main reasons for organizations to hold back on investing in cybersecurity. However, there could be another important factor that is playing a role in this complex multi-actor system.

Last year in August 2021 Ernst & Young released a security survey with 1000 security leaders worldwide. According to this survey, more than half (56%) of the leaders say they sidestepped their cyber processes to facilitate remote and flexible working. This is an interesting statistic, given that simultaneously these leaders have never been more concerned about their ability to handle cyber threats [13].

This February, only a few months ago PwC published a report regarding the global digital trust insights from the Netherlands. The increase in organizational complexity makes it more difficult to identify all the risks. Which is especially true for risks stemming from hybrid working due to the relatively young character of this socio-economic change. Also, according to the report fewer than 1 in 3 organizations are using data and intelligence when making cybersecurity decisions. It might be possible that not all organizations have the ability or financial resources to use data and intelligence. However, this makes it even more difficult to determine cybersecurity challenges [14]. A report from the same firm that came out in January 2022 shows that out of the 4446 CEO's 58% identify cyberrisks as the largest threat for their businesses. In contrast to the only 33% of organizations that think climate change is a major threat or the 26% that think health risks are a major threat to their organization. This shows that organizations are feeling the need to properly secure their organization in the cyberspace [15].

It is essential to understand the companies' cybersecurity challenges and approaches to tackle these in order to analyze this complex system. A study from Eijkelenboom & Nieuwesteeg last year analyzed the disclosure of cybersecurity information of 75 listed companies in the Netherlands. According to this research 94 % of these listed companies only mentioned cybersecurity or just a few measures in their annual report. Although they are not legally obligated to do so, the analysis shows that total openness creates the highest surplus for society and companies [17]. As these companies are not obligated to disclose specific cybersecurity information, it can easily be left out to avoid possible reputation damage. However, this makes it even more difficult to analyze possible solutions for the security challenges.

More research shows that due to the pandemic, a great amount of organizations were not prepared for these changes in the work environment [18]. Preparation takes time and such world-changing event as a pandemic is hard to predict. Given the fact that we are now entering our third year of the pandemic, the magnitude of Covid's surprise might have worn off. The aforementioned literature showed that for organizations that have implemented teleworking a lot can change in a short period of time. Despite that only month old studies show that organizations are facing severe cybersecurity challenges, it is unknown what the current main challenges are and how they are being handled. There is the possibility that organizations already managed these challenges or that the uptrend in cyberattacks is even accelerating. Furthermore, there exists a gap in literature regarding the organization's current cybersecurity challenges that are the result of the increased use teleworking. Which seems to be essential knowledge as these high levels of teleworking are believed to be the new normal.

Furthermore, what is essential to note and to take away any confusion later in the research is that this research does not focus on the impact of pandemic measures taken by the government on the cybersecurity of organizations, but on the security challenges that derive from the increasing use of teleworking. These measures being a significant reason for the teleworking levels to be at their current levels, so throughout the research the relationship between teleworking and the pandemic will be often discussed. However, these pandemic measures such as lockdowns caused a lot more than just an increase of teleworking. A large number of organizations do not even exist anymore due to the effects of the lockdown. So this phenomenon will not be studied, but since the pandemic has such an huge impact on society at this moment, it might be that some of the organizations' security challenges related to the increase use of teleworking also indirectly relate to the pandemic.

1.3. Research approach & Objective

1.3.1. Research approach

As discussed in the introduction, this problem exists in a specific period that has never been seen before. Organizations being forced by the pandemic to introduce or heavily increase teleworking employees, while continuing all other processes, even with possible shrinking resources. Before being able to answer this question one should understand how this complex system is currently working. It is important to acquire knowledge regarding what cybersecurity challenges organizations are currently experiencing. Furthermore, how these organizations are responding to these certain challenges. In addition to the experiences of organizations, the view of consultants that support organizations is indispensable since they have a different perspective given their responsibility and interests. Considering all these characteristics of this research, a well fit approach would be a qualitative research [20].

These knowledge gaps will be transformed into several sub-questions that will contribute to answering the main research question. As the knowledge gaps can not be sufficiently filled by only using literature as the specific view of both organizations and consultants is likely not widely available nor up to date. The required information can be acquired by interviewing individuals that are fulfilling a role inside a company where they are responsible for the organization's cybersecurity and consultants that are supporting organizations with their cybersecurity management. The combination of these interviews and literature review will contribute to gaining a deeper understanding of this complex issue in a specific context and help answer the research questions. What is important to note is that the view of the consultants might significantly differ from that of the organizations. Not only because of local expertise and experience, but also because of their interests. For organizations there might be numerous aspects that might have a higher priority than cybersecurity [21]. So there is a conflict of interest between the consultants and the organizations. The main goal of the cybersecurity consultants is to mainly focus on achieving the best possible security for a organization, while organizations have to focus on business continuity and other business risks as well. It seems feasible to arrange several interviews with both consultants and organizations. Research shows that 9 to 16 participants reached saturation, which in this case with the time schedule seems feasible and a good fit for this research [22].

1.3.2. Objective

Besides filling in this knowledge gap to provide scientific relevance, the literature and statistics show that there is a need to support organizations to improve their cybersecurity. This research can provide this support by gaining a deeper understanding of the current challenges in organizations. What differentiates this research from prior research into this topic is that it does not solely advise organizations

to 'do more security' as this does not seem to provide any support to organizations as they seem to be aware that cybersecurity is a threat. As shown in the introduction, prior research and data show that there is a need for organizations to improve their cybersecurity, but the important question this research should answer is not 'what is the solution?', but to take a step back and start by 'what are the current challenges?'. It is important to first start by gaining a deeper understanding of the current challenges organizations are facing in the continuously changing environment. What makes this research more valuable and unique is the combination of the view of both consultants and security managers of organizations to get multiple perspectives on this complex problem.

1.4. Research questions

The reviewed articles show the knowledge gap regarding the understanding of current and future cybersecurity challenges caused by high levels of teleworking. Considering the uncertain and unique character of this problem, research is required to understand and analyze this complex system. The answer to the following main research question should fill in the knowledge gap:

"How did the increasing use of teleworking affect organizations' approaches to managing cybersecurity challenges?"

In order to give a well-founded answer to this question, five sub-questions are formulated. Before being able to answer the main question, it is important to fully understand what the current organizations' cybersecurity challenges related to the high levels of teleworking and organizations' approaches to manage these. It is important to acquire information that comes directly from organizations and consultants to answer the following subquestions.

1. To what extent are organizations using teleworking and how did the increasing use of teleworking affect organizations?
2. What cybersecurity risks and threats are related to high levels of teleworking?
3. What are the main cybersecurity challenges that are related to the high levels of teleworking?
4. How are organizations approaching these identified challenges?
5. How do the challenges and approaches stated by the organizations differ from those stated by the consultants?

1.5. Relevance

One of the main purposes of this thesis is to have scientific relevance and provide a meaningful contribution to the current literature. In addition to scientific relevance, this research aims to make a positive impact on society. This section will discuss how this research will contribute to both society and science. At the end of this report in chapter 5 the relevance of this research will again be discussed using the results from this research.

1.5.1. Scientific relevance

Multiple scientific articles are presented in the introduction that show that cybersecurity is a growing threat for organizations and how high levels of teleworking increase the security risks. However, there is a lack of research regarding the current security challenges related to the increase use of teleworking and organizations' approaches to managing those challenges. So there is a need to uncover these challenges and approaches taken by organizations. This gives future researchers the possibility to focus their research of specific parts of cybersecurity or one particular worrying challenge. Besides only examining the challenges, what is especially interesting to add to the scientific literature is showing how organizations are responding to these challenges. Given the characteristics of this complex problem, this research can support the literature by creating an overview and understanding of the main security challenges related to high levels of teleworking and the approaches taken by organizations to manage these challenges.

1.5.2. Societal relevance

There is a very clear reason this research provide societal relevance. According to the objective of this research there is a need to support organizations to improve their cybersecurity to account for the differences in the current pandemic-related situation. As this research will provide this support by gaining a deeper understanding of the current challenges in organizations and their approach of handling them. This will not only support organizations given the fact that society as a whole has interest in improvement of organizations' cybersecurity. Data breaches can for example harm the privacy of citizens or can have an negative economic impact given the costs of these breaches. So organizations can use the knowledge that will derive from this research to improve their cybersecurity, knowing how organizations are responding to the identified challenges.

2

Literature study

2.1. Teleworking

The concept of teleworking is an significant part of the research, so this concept should be well defined. The literature presented in the introduction shows some of the effects of teleworking and how the pandemic resulted in high levels of teleworking within organizations. However, the implications of teleworking are dependent on what definition of teleworking this research uses. Therefore, this section will provide an in-depth discussion of teleworking.

2.1.1. Definition of teleworking

Before showing how teleworking made its way into organizations and how it is affecting them, it should be clear what the definition of teleworking is, as there are multiple terms floating around. According to the Cambridge Dictionary teleworking is a new synonym for telecommuting and has the following definition: 'The activity of working at home, while communicating with your office by phone or email, or using the internet' [23]. One can argue that a teleworking employee is an employee that is working from home and does not go to the office. In the early '70s when the term telecommuting was used for the first time and did indeed meant that telecommuting employees did not work at the office [24]. Since then, the term has evolved and a teleworking employee refers to an employee who combines working from home or an alternate location and in-person at the organization's office. A term that is widely used among organizations is hybrid working. Every organization has their own approach and uses a different hybrid models, but the aspect that all these models have in common is that they consist of both working remotely and at the organization's premise.

An important note for this research is that the term teleworking will be used instead of hybrid working due to the literature seems to prefer the use of teleworking. However, especially for this research the terms are fairly similar, given that if an organization has high levels of teleworking, this means that they use a hybrid working approach with a high share of teleworking employees. In addition to the evolution of the definition, the rates of teleworking employees have surged in recent years [25]. In the next sub-section, the timeline of teleworking in organizations will be discussed.

2.1.2. Teleworking's history

As mentioned in the previous sub-section, teleworking was already introduced in the '70s. However, for the sake of this research, there is no need to look into the the specifics of teleworking before 2000's as mostly entrepreneurs used this instead of employees of organizations. In 2001, around 28 million people in the United States of America worked from home in some capacity, at the same time in the United Kingdom two million employees were working remote [26][27]. In the 2000s teleworking started gaining popularity for high-qualified work with higher payments instead of the negative reputation it had before. Nevertheless, in Europe the share of employees that are to some extent teleworking increased from 5.2% to 9% in the period between 2009-2019. So in a decade there was only a slight increase in this share. The share of teleworking employees in organizations before the start of the pandemic also seems to be very sector and occupation dependent. Knowledge-and ICT-intensive services were already

very familiar with teleworking, while obviously sectors that require physical manipulation had very low levels of teleworking [47].

After the start of the pandemic in 2020 the share of employees that were working remotely experienced a steep increase. In the second half of 2020 an average of 48% of all employees in Europe either completely worked from home or a combination of teleworking and on the employer's premise [30]. The results of a survey among world-wide businesses even show that 88 percent of the businesses mandated or encouraged their employees to work remotely at the start of the pandemic. While his research states that the businesses mandated this measure, governments worldwide did not allow organizations to have their employees working on premise [29]. Two years of pandemic with a lot of restrictions later in February 2022, Gallup published a survey based report. Most employees that were able to work from home continued to work remote at least to some extent. In the future, a hybrid work schedule will most likely be the most common workplace setup. Compared to pre-pandemic numbers the share of employees that are subject to an hybrid working model is expected to double. Both workers and leaders and managers prefer a hybrid working model, while only teleworking employees are not organizations' first choice [31].

2.1.3. Implications of teleworking

The forced shift of hybrid working models in organizations did not only brought a list of challenges, there were also a lot of opportunities. However, there is no need to focus on the positive impact teleworking has on organizations as this will not result in any relevant challenges. Teleworking has been around for decades, which means that teleworking has already made an impact on organizations. What makes this current post-/peri-Covid-19 period different is the share of employees that are partly working remotely and the short time period in which this change occurred. This has never been seen before and has resulted in even more implications. Teleworking did not only affect organizations' directly, other components of an organizations could have been hurt due to the introduction of the high levels of teleworking that eventually led to amplified or different cybersecurity challenges. So the impact is not only of a technical nature and the purpose of this section is to give a description of the implications of teleworking, without specifically focusing on the cybersecurity challenges that are related to the high levels of teleworking. These will be discussed in the next section, as the concept of cybersecurity requires more attention.

The implications that will be discussed are divided by the period before the sudden IT-change and the current situation to provide a clear overview of both situations.

Pre-Covid

Even before the introduction of work-related restrictions, a large body of research related to the impact of teleworking has been conducted. Research from 2009 shows that human interaction like eye contact and body language have a more significant effect on the understanding than the words being said. It was only until 2012 and forward that more developed communication technologies allowed employees to see each other during online meetings which helps with bringing over information. Even earlier in 2004 R. Morgan made an assessment of the teleworking challenges. According to this research coordinating teleworking arrangements can be difficult. In addition, the perceived costs to implement and manage a teleworking model could be too high. This paper also mentions a challenge that is in line with the one mentioned earlier, information access and exchange are a constraint. Controlling and coordinating the working activities of employees that are teleworking is considered an obstacle [32]. These problems seem to be solely focused on the organization's management. However, the well-being and satisfaction of employees is also in the interest of organizations as this will also impact the organization. Teleworking resulted in several mental health conditions for the employees of organizations. Social isolation is one of the most frequently stated disadvantages of teleworking that causes such condition.

Presenteeism is another reason for the mental health conditions of employees. The loss in productivity is due to not fully functioning ill employees. Teleworking employees do not seem to take a whole day off and return faster than non-remote workers. Organizations might think this is an advantage of teleworking, it is not in their interest to have employees work through illness. This report also reports a problem that is more in line with the other papers. A lack of support given by the organization to the organization. Teleworkers experience difficulties in the technical support provided by the organization. As remote workers become 'out of flow' they have a political disadvantage that expresses itself in the absence or delay in career progression, which can also result in mental health condition of the employee

in question. Overall this research suggests a negative emotional impact of teleworking on employees that results in loneliness,irritability, worry and guilt of teleworkers [33]. More technological issues are found in research conducted in 2013. Unauthorized people will more easily get access to the network through the devices of a teleworking employee. An employee can forget to lock their device which results in this problem, while this would not happen in an office as there is more physical security to enter the premise. In addition, in 2009 the majority of small enterprises used the cloud to store data and use WiFi. These connections are not secure and give hackers the possibility to access the system through the unsecured internet connection. Moreover, in this period employees are expected to use their own devices that they also use for private activities, which increases the risk of a breach [34].

There are also issues focused more on personnel security, research shows that many teleworkers lack the feeling of responsibility required to adhere to management objectives, and they can easily jeopardize teleworking's success. Employees are changing the security settings to unlock restricted websites without considering the security policies of the organization [35].

Peri-Covid

Before discussing the implications of teleworking since the pandemic that forced organizations to introducing high levels of teleworking, it is important to note several limitations. As the moment the pandemic started in early 2020 is only around two years away from the moment of writing this research, it is possible that not all implications are researched in the literature. So it is not possible to be completely certain that some implications have changed or do not exist anymore. The assumption has to be made that there is a possibility that a lack of literature regarding the implications of the high levels of teleworking during the pandemic.

Let's start by addressing the first implication mentioned by R. Morgan in 2004, since the start of the pandemic several sophisticated communication technologies were already widely available. A huge majority of organizations use the video conferencing tools that led to speed up decision-making processes and even more than half of the employees seem to be more likely to contribute to a meeting and it effectively increased employee engagement. One can say that this implication that existed before the rise of online meeting platforms has now become less significant [36]. Spanish researchers make the distinction between the conventional telework and crisis-induced telework. Figure 2.1, shows the characteristics of the different versions of teleworking.

Telework characteristics	
Conventional telework	Crisis-induced telework
• Voluntary	• Mandatory
• All or part of the working hours	• Full-time
• Preparation and Training (digital content and cybersecurity)	• No Preparation
• Adaptation of physical work environment at home, technology access and ICT tools	• (Potential) lack of ICT tools (hard/software, access to internet or intranet)
• Workplace flexibility (somewhere outside the office, not only at home)	• At home
• Children at school	• Children at home
• Social relations	• Social isolation

Figure 2.1: Characteristics of conventional vs crisis-induced teleworking during COVID-19 lockdown (source: [37])

The last characteristic of the crisis-induced telework seems to be similar to one of the implications mentioned in the previous subsection. Social isolation was a serious problem during the pandemic which has caused harm to the mental health of teleworking employees. The Spanish researchers used a well-being score to assess the well being of teleworking employees and results show that these scores have decreased during the pandemic-induced lockdown, in comparison to earlier data. No preparation also caused organizations to not have proper virtual working conditions at home which resulted in limited availability of technical resources, accessibility to data or files. Having children at home while teleworking could alleviate the effects of social isolation, but could also cause more stress and distraction [37].

Furthermore, a recent study looked at the benefits and drawbacks of working from home for knowledge workers in 29 European nations during COVID-19. They mention three main disadvantages of

working from home during the pandemic. The first main disadvantage is again focused on the employees, there are several home office constraints. Because of the crisis-induced teleworking model, employees get less social interactions and get out of home less. Secondly, employees also report work uncertainties, they feel that the work situation is unclear and have a hard time focusing on the work that is less interesting. Lastly, a reoccurring problem, accessibility to facilities, data and valuable work tools is one of the main problems [38].

The Organisation for Economic Co-operation and Development published a report in December 2021 that shows what the majority of the managers of organizations perceived as the main negative implications of teleworking. Starting with the managers feeling that working as a team is more difficult due to teleworking. Secondly, managers believe that the corporate culture and the identification of workers with the company's beliefs may be harmed. They also believe that training is more difficult and that on-the-job learning an creativity is limited. Lastly, according to the managers teleworking resulted in a higher risk of cyberattacks [39].

'Post-Covid'

Of course it is hard to discuss the implications of teleworking after the pandemic as there is a lot of discussion about the pandemic being over [40]. Furthermore, this also varies among countries and even within countries. However, what is particularly interesting and is unfortunately hardly supported by literature given the fact that this is a phenomenon that is happening while writing this research, is a new shift. All the implications mentioned in the previous section were mostly researched during the crisis-induced phase of teleworking. These same papers often mention advantages of a hybrid working model, which means that employees are both working remote and working on the organization's premise. A helpful illustration can be found in Figure 2.2 from the OECD, this shows how employee's efficiency increases while teleworking to some extent and decrease when completely working remote.

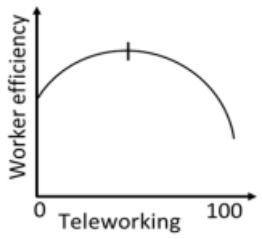

Figure 2.2: Relationship with percentage of working from home and employee's efficiency (source: [39])

Figure 2.1 also helps explaining the current shift. After discussing the teleworking's history, the model that was mainly used before the start of the pandemic was the conventional teleworking model. The pandemic resulted in a relatively long period of the crisis-induced telework and it can be argued that organizations are now in the transition of moving back to using conventional teleworking. A global survey from WFH show that employees prefer working on average 2 days a week from home, while employers are planning on allowing employees to work an average on 1 day a week from home. In the beginning of the pandemic the government forced organizations to let their employees work from home, at this moment employees are 'forcing' their organizations to let them work from home despite organizations having a preference for working at the premise. The employees are 'forcing' this given the 15% of global respondents quitting or considering quitting if their employees force them back to work full time at the organizations' premise [41].

2.2. Cybersecurity

2.2.1. Types of cybersecurity

As a great part of this research is to examine the cybersecurity challenges, it is important to completely understand what cybersecurity in an organization is. Merging several definitions from different papers, cybersecurity aims at protecting the cyberspace from any cyberthreats. A few examples in the long list of cyberthreats are: phishing attacks, DoS attack or eavesdropping [42]. These threats will be discussed in more detail later in this chapter. Cybersecurity can be divided into different components as cybersecurity on its own is a broad term. To get a better understanding of this operation of securing

information systems and protecting information assets, the main elements will be discussed in this section [43].

Application security

Application security is the process of protecting software application data against cyber threats. The aim of application security is to improve the security practices related to the applications, which covers the entire application life cycle. The application security consists of both hardware, software and procedures that can identify and mitigate vulnerabilities. Several well-known types of application security are: authentication, authorization, encryption and logging [44].

Network security

Network security is the process of protecting the network from unwanted users, attacks and intrusions. Most of the time network security has three different layers: physical, technical and administrative. Controlling the physical layer should prevent unauthorized subjects from gaining access to network components such as cables or routers. Data that is stored on the network or is in transit out of or into the network should be protected in the technical layer. The administrative security controls include network access control, so how users are authenticated and who can access certain data [45].

Cloud security

Cloud security refers to the process of securing the cloud computing environments from internal and external threats. Network security can be described as a branch of cloud security, so the measures taken to protect the network are also part of a cloud security setup. Cloud security is composed of multiple categories such as identity and access management (IAM) and data retention and business continuity [46].

Critical infrastructure

This part of cybersecurity relates to the critical infrastructure that organizations and society rely upon. Organizations that are responsible for this infrastructure should consistently identify, assess and manage the cybersecurity risks. Most of the time critical infrastructure organizations are more vulnerable to cyber threats as supervisory control and data acquisition system rely on older (less secure) software. For example the rapid digitization resulted in a great need for improving the critical energy infrastructure cybersecurity. Different critical infrastructures require sector specific attention [47].

IoT security

IoT security is the process of securing the physical smart devices and networks, processes, and technologies that are connected to the IoT environment. So this component includes both physical and network security. Examples of smart devices are for example security cameras industrial machines or entertainment devices. The main goals of IoT security are to maintain the privacy of the users, confidentiality of the data and ensure the security of the devices and the IoT infrastructure [48].

2.2.2. Threats

Classification of threats

Especially in this digital era, organizations are exposed to multiple types of security threats that can cause harm to organizations. These threats can affect the confidentiality and integrity of the data or the availability of the system. Which can be linked to the CIA Triad which is a common model that forms the foundation for the development of security systems. The confidentiality, integrity, and availability of information are as vital parts of any organization [49]. In 2014 computer science researchers defined a classification model of threats in information systems [50]. The classification starts with the source of the threat. A threat can be caused by both internal and external entities. An internal threat to an organization can occur when an entity has authorized access to the IT systems. Individuals or organizations working outside of the concerning organization that do not have authorized access to the network can pose an external threat.

Secondly, the threat agent is the agent that imposes the threat. The agent can be environmental, human or technological. Environmental threats can come from natural disasters like an earthquake or a flood, but also a war or a riot can be an environmental threat. This type of threat is not the type that will be focused on in this research, high levels of teleworking will not increase the likelihood

or impact of such an event. Human threats are threats caused by the actions of humans such as an hacker attacking certain systems. This seems to be the most relevant type of threat for this research as teleworking increased the amount of cyberattacks. The last type of threat is the technological threat, which are caused by physical processes on materials. For example the use of physical actions means to enter a compound and steal certain hardware.

After determining the source and agent of the threat, one can determine if the result of the threat is malicious or not. This only applies to the human threats. Malicious threats are caused by inside or outside agents that aim to harm and disrupt an organization. Non-malicious on the other hand are caused by poor security and can be caused for example by ignorant employees that do not intend to harm the system.

Finally the intention of the human threat is important. This might seem similar to the malicious and non-malicious classifications, but that is more focused on the result and not the intention. Unintentional threats are introduced without the awareness of the agent. Accidental modification of software for example is an unintentional threat. The intentional threats are caused by agents that make harmful decisions. Purposely steal confidential data of an organization through accessing their network is an example of an intentional threat.

Type of threats

According to the threat classification model and the discussed literature so far, teleworking resulted in mainly more human and some technological threats. This subsection will discuss the various of these human and technological threats. The goal of this section is to get a better understanding of specific type of threats that currently exist. This will be helpful for the discussion of the teleworking cybersecurity risks. The next section shows that indeed the human threats seem to become more and more relevant. This section will start with the unintentional malicious threat that are imposed by employees of organizations that is one of the most used by attackers.

Social engineering is a manipulative method used by an attack to exploit a human vulnerability through social interaction to breach cyberspace security. The victim has an asymmetric knowledge-relation to the attacker, the victim does not know he or she is interacting with an attacker. As large parts of IT systems rely on humans, the vulnerabilities of the innocent human can be exploited by any skilled attacker [58]. The goal of the social engineering attacker is to access sensitive information or money.

One of the most famous and relevant forms of social engineering is phishing. According to the FBI, phishing is the most common type of cybercrime at this moment, given that 3 of the 4 companies around the world experienced an form of a phishing attack in 2020. There are a lot of variations of variations of phishing. However, as phishing is the most used form of cybersecurity and provides a better understanding of what social engineering is, there is no need to discuss the extended list of variations in detail [59].

A phishing attacker sends fraudulent messages through various electronic communication channels, claiming to be from a reputable and trusted source. So a phishing is a type of attack that communicates socially engineered messages to persuade the victims to perform certain actions in favor of the attacker. Most of the communication goes through emails, the attacker for example sends an email that at first glance seems to be from a trusted source with a request. The email can ask the victim to urgently change their password credentials and will lead them to a website that looks like the website from the trusted source, but is a fake website that the attacker uses to steal the victim's credentials. As the security measures to prevent these developed and got more profound, the phishing techniques developed along with them. As two-factor authentication (2FA) is often required to complete transactions for example, the attackers use a dynamic form of phishing. The victim will be led to a fake website and is required to fill in their 2FA code to 'change their password', while this 2FA code will actually be used by the attacker real time to complete a transaction.

As stated, there are more variations of social engineering, but the essence is the same. The attacker exploits the vulnerabilities of system processes caused by the system users [60]. Social engineering attacks also occur in combination with the not less relevant threat: malware. This threat has as the name suggests a malicious character and can be classified as an human threat as well. Malware can be described as software or code that attackers use to infect and infiltrate IT systems. The goal of the attacker is similar to social engineering, to steal data or do harm to a system. Victims' devices can get infected with a lot of variations of malware. One of the well-known types of malware is a virus, which

is self-replicate and can insert itself into healthy files on the system. Another good example that has gained a lot in popularity is ransomware, the digital variation of taking a victim hostage. This piece of software encrypts all the files and or control of the system and only unlocks the decryption after the victim made the requested payment. A problem with some variations of malware is that this piece of software can easily spread to other devices connected to the network.

As already mentioned, a combination of both social engineering and malware is possible and often used. Not only are they combined, some types of malware consists of a social engineering aspect. A proper example is a Trojan, these applications are advertised by the attacker as harmless and helpful software programs. However, while running this program, it can steal information and data, just like other malware. This concept is similar to that of social engineering, the attacker exploits vulnerabilities of system processes caused by the system user, by making the victim think the program is useful. Another example of a combined attack is an attacker that could send a phishing mail or text to a victim with malware attached.

There is a large list of different variations of malware, such as scareware, worms, ransomware or adware. Not all variations have to be discussed in great detail, as for this research the discussed type threats seems to be the most relevant for this research [61]. More specific risks that are related to the high levels of teleworking will be discussed in the following section after which cybersecurity management will be looked into to understand how these threats are being dealt with inside organizations.

2.2.3. Teleworking related risks

After discussing the elements of cybersecurity and acquiring a better understanding of this operation of protecting information systems and information assets. This knowledge supports the understanding of the risks identified by the literature. As the aim of this research is to show what cybersecurity challenges organizations are facing and what their approach is to managing these since the pandemic, literature can help with identifying a part of the challenges. As the pandemic resulted in a continuously changing IT environment, literature might lag behind the current situation. Similar research that focused on the effects of the pandemic on cybersecurity that is for example published in 2020/2021, can show different results as managing and researching changes in organizations requires time. However, as this research does not have the resources to acquire data from various sectors and a large number of organizations, literature will be a valuable addition.

The introduction of this research already stated several teleworking related risks that are occurring within organizations according to literature, this section will describe them in more detail. High levels of teleworking in an organization means that a large part of the employees are working form home. For this reason the following challenges will be categorized based on their characteristics into employee-related or technology-related risks. In addition, over the past years multiple studies show that human errors are one of the main causes of causes, which now might even is the number one cause since the recent introduction of high levels of teleworking in organizations[62] [51]. Employee-related risks are associated to employees working from home, while the technology-related risks focus on the technologies that are used during the period with high levels of teleworking.

Employee-related risks

- Lack of concentration or distraction results an increased likelihood becoming a victim of a cyberattack such as phishing that can require a sharp eye to notice. Working from home can lead to various distractions related to the responsibilities an employee has at home or the household situation. Furthermore, according to the SHRM, a significant share of employees feel tired and have little energy when working from home. This is particularly the case for the crisis-induced teleworking model, as this probably requires the possible family members to stay at home as well which causes distractions [52].

- As a lot of organizations were not properly prepared for the forced high levels of teleworking, organizations were not able to provide sufficient training programs to all employees in time. Employees did not know what the possible risks are and how to reduce these risks. This resulted in poor cyber hygiene of the employees that resulted in a higher risk of cyber attacks.

- The reduced access to knowledge and information also did not contribute to a better cyber hygiene. Organizations could have restricted certain high-risk websites or platforms and employees will try

to find ways around this by for example changing the security settings. This will result in an increase in various security risks [35].

- One can assume that also the teleworking environment of the employees has less physical security. Whether this is at home or another teleworking location, there is a higher chance of unauthorized people being present. Family or roommates might be able to hear confidential information when they are in the same room. Furthermore, if employees do not lock their devices, there is a higher risk of the unauthorized roommates getting access to the organization's network and data. In addition to the present individuals at the remote working location, there is a new category of threats in the remote working environment. The IoT devices inside the room of the employee have a history of security vulnerabilities that led to eavesdropping and spying. So the IoT devices that have a microphone and/or camera in the same room as the employee increases the risk of cyberattacks [53].

- Until this moment only risks have been discussed that were not the result of intentional wrongdoing of employees. However, there is also the possibility that certain employees do not have good intentions. The lack of management monitoring enables employees to steal confidential information from their employer or misuse corporate services [54].

Technology-related risks

- The pandemic forced organizations to implement a teleworking model in a short period of time resulting in rushed technology adoption. Employees and managers not being familiar with the new remote-technologies led to security related mistakes. If the technologies in the remote working environment did not work properly, employees would try to find a way around this. For example not using VPN or connecting to a public WiFi network that is not secured. Despite the fact that there are employees that are complying to the security guidelines, their WiFi might still be less secure than at the office environment. Organizations can not control and manage the security of all the employees WiFi networks [55].

- The use of external communication and data sharing channels increases the risk of data breaches. A few of most used services are Microsoft Teams, Zoom, and Google Meet. Over the last years Zoom has been a target of many attacks which results in a higher cybersecurity risk for organizations [56].

- A large part of organizations use the concept BYOD (Bring Your Own Device). This causes a lack of control and visibility over the activities and behaviour of employees. Furthermore, employees might use the device for activities that involve downloading applications or visiting unsecured websites. So the use of unsecured personal devices for work related means results in a higher risk of data leakage, stolen or lost devices, unauthorised access and malware infections [57].

- Not only the personal devices that are used for business can be lost or stolen, also company devices may be stolen from home or any other remote-working environment. Especially if these devices are not properly secured, this imposes a high risk of unauthorized people gaining access to the organization's network and data. Attackers are aware that more people are teleworking and they have more mobile technology at home [54].

2.2.4. Cybersecurity practices

The rapid digitization over the past years resulted in multiple frameworks that lays out guidance and standards for organizations to secure their data from these threats. Despite not all organizations using these forms of guidance to manage their cybersecurity challenges, they provide a greater insight regarding the range of predefined options organizations have to approach their cybersecurity. Research conducted a few years ago shows by using surveys that 44% of organizations along all sectors are using at least one security framework. However, the frameworks do not name specific cybersecurity practices that are part of the guidance and standards. Last year the Information Technology Laboratory published a press bulletin reiterating the NIST teleworking standards. The following five security measures were outlined in the news bulletin [75]:

- Developing and enforcing a telework security policy, such as having tiered levels of remote access
- Requiring multi-factor authentication for enterprise access
- Using validated encryption technologies to protect communications and data stored on the client devices
- Ensuring that remote access servers are secured effectively and kept fully patched
- Securing all types of telework client devicesincluding desktop and laptop computers, smartphones, and tabletsagainst common threats

Despite the NIST standards, a part of the discussed teleworking related risks are still identified as concerns by organizations. So far, there is no extensive security policy that protect teleworkers, BYOD and remote access for a majority of the organizations. This subsection will discuss the security practices that are related to the earlier discussed security threats.

Practices assuming external environments contain malicious threats

To start with the fact that an organization should assume that using services, networks or devices from external parties will contain hostile threats. These threats can be mitigated by encrypting the device's storage or not storing sensitive data on clients devices. Furthermore, strong authentication such as 2FA, which is also related to the second bulletin, should be used. Communication through these external network outside of the organization's control are also vulnerable. In this case both encryption and authentication should be used to ensure secure communication. In addition, keeping software like network tools, Network-based Intrusion Detection Systems (NIDS), phishing identification and firewalls up to date is of utter importance.

Finally, organizations should also assume that the devices of telework clients are or will eventually become infected with malware. In order to mitigate this threat, teleworkers should use anti-malware software and there should be a separate network at the organization for clients bringing in their own devices. Furthermore implementation of Network Access Control (NAC) solutions helps checking the security status of the client before giving access [76].

Building a security policy

This concept refers to the bulletin point, developing a IT policy document to support their cyber security measures against social engineering and malware attacks. First of all, such policy should contain which types of teleworking devices have various forms of remote access. Also, which type of access each teleworker has and to keep this administered and updated.

Furthermore, the tiered levels of remote access as mentioned in the first bullet, the policy should contain what levels a of remote access are granted to certain type of devices. For example, organization owned devices can under conditions have access to all systems, while BYOD devices only have access to low risk levels. Having these remote access levels helps organizations limit the risks as the most controlled devices will have the most access and the least controlled devices, will have less access.

Server security

As remote access servers provide external actors access to internal resources. So properly securing these remote access servers is vital to preventing unauthorized access to the organizations' resources. Organizations should place their network server at the organizations' perimeter.

Employee education

Subsection 2.2.3 show that a great part of threats and risks are related to employees. So despite this not being a part of the practices to reiterate the NIST standards, educating employees is seen as one of the most important security measures by Chief Information Officers (CISOs). Especially since the introduction of the crisis-induced hybrid working models among organizations as teleworkers are being targeted more often. Too much training and education does not seem to be effective and could even result in employees understanding less of how important proper cybersecurity knowledge is in organizations. In order to reduce the risk of social engineering attacks, organizations could provide their employees cybersecurity awareness training. Having cybersecurity policies combined with the cybersecurity awareness training will help learning employees on how to act with various types of attacks [77].

3

Methodology

In this chapter, the research approach together with its used research methods to answer the research questions will be discussed. Subsequently, a discussion of the ways of collecting data for each sub-question and the data preparation for data analysis will be provided.

3.1. Research approach

The goal of this research is to provide a better understanding of organizations' cybersecurity challenges related to the high levels of teleworking and their approach to manage these challenges. In order the answer the main research question, various sub-questions have been stated in section 1.4 that each focus on a different part of the answer. Each question requires a different method that will be discussed in the following section. However, it is important to first look into the approach of this research.

Given the knowledge gap of this research and the complexity of this problem, a more exploratory approach seems to be the best fit for this research. Exploratory research is suitable for research fields where the topic is highly complex or the existing research results are unclear or consists of severe limitations, but also if there is not much known about the concerning phenomenon [84]. Such high-levels of teleworking due to the crisis-induced hybrid working model have never been seen before. In addition to the share of teleworkers, organizations are also in a rapidly changing environment since the pandemic. Both the phenomenon of crisis-induced teleworking in combination with the implications of the pandemic resulted in various cybersecurity challenges. There seems to be a need to support organizations to improve their cybersecurity. Therefore, performing an exploratory research that helps understanding what the current cybersecurity challenges of organizations are and their approach to managing these, is given all the characteristics the best fit.

Only scientific literature and reports do not seem to be sufficient to answer the research questions. Especially as the organizations' environments are constantly changing and the current scientific literature might lack behind to the situation of today. Given the exploratory nature of the approach and the given goal of the research, conducting interviews is likely the best method to choose. So this research has a an interpretive qualitative approach using interviews without any testable hypothesis. The interviews should be held with participants that posses up to date information regarding the cybersecurity challenges of organizations and their management approaches.

For this research, interviews with two different type of actors that possess the required information are arranged. Starting with the organizations, there are certain roles within organizations that are responsible for managing the current cybersecurity challenges related to the high levels of teleworking. Acquiring this information is vital to this research, so interviews with for example CISOs, IT/Security managers, or a similar role should be conducted. Although they are responsible for the data and information security of the organizations, their goals and actions have to align with the organization's goals. For this reason it is important to speak to parties that do have the required information, but do not directly work in such an organization. Cybersecurity consultants that work with organizations on these matters could provide a alternative perspective on this topic.

3.2. Research methods & sub-questions

How this approach and certain research methods will contribute to answering the various sub-questions will be discussed in this section. Subsequently, the last part of this section will discuss how the answers of the sub-questions will be able to answer the main research question.

3.2.1. Research methods

In the previous section, arguments have been made regarding the choice for the combination of interviews and literature. However, it is important to specify what type of literature and interviews will be used before relating them to the specific sub-questions.

Desk research

The previous chapter 2 is devoted to the theoretical background that consists of relatively large share of organizations' reports next to the scientific literature. While a great effort has been made to select mostly proper scientific articles, as this research is looking into the current cybersecurity challenges, there is need to also use very recent reports of companies. A significant part of the used literature are reports that were published even after the start of this research, to establish an theoretical background that is as accurate as possible. The provided literature review is a good basis, as it discusses all the key concepts in the current context which is necessary to understand before conducting any interviews. How exactly the desk research will contribute to answering each sub-question will become clear in the upcoming subsections.

Semi-structured interviews

The most important source of the data is the interviews. Aforementioned, this research is focusing the current cybersecurity challenges and organizations' approach to managing these challenges, so in-dept information originating from the actor that is in need of support is indispensable. Furthermore, interviews with consultants will provide another perspective on the issue that might give other insights.

There are multiple types of interviews that were taking into consideration. Choosing the hybrid form semi-structured interviews will enable you to both gain new insights like with unstructured interviews and be able to compare the responses of the candidates as with structured interview [85]. This type of interviewing enables the researcher to formulate both open and structured questions with follow-up questions. Furthermore, semi-structured interviews tend to be more suitable for this research as it allows a more personal and conversational discussion. This is important to consider as the goal of the interviews is to understand the challenges of organizations and their vulnerabilities, which can be quite sensitive [86].

Despite these advantages of interviewing, there are some disadvantages that should be mentioned as the quality of the results. One of the disadvantages is that the interviewer could respond with what the respondent thinks the the interviewer would like to hear. So the possible absence of objectivity can be troubling for this research. Section 3.3 will discuss the research design and show how effort is made to obtain high quality data.

3.2.2. Sub-question 1 - Implications & phase

"To what extent are organizations using teleworking and how did the increasing use of teleworking affect organizations?"

First of all it is very important to start by having a clear definition of teleworking. Of course teleworking did already exist before the start of the pandemic which also brought various types of cybersecurity challenges. However, it is important to understand what teleworking is and what the implications are to get a consensus with the interviewees regarding these concepts. There is a large body of literature regarding the definition of teleworking and its history. Although there are some variations to the definition, so the most suitable for this research should be chosen.

Additionally, the used literature both reports on the implications of teleworking in both pre-pandemic and during the pandemic. However, as this work environment is constantly changing, so there is a lack of information regarding the current and possible future implications and in what state teleworking is in specific organizations. Due to the exploratory character of this research, the decision has been made to not focus solely on one specific industry. So in order to understand what the current

state of teleworking is in organizations, interviews with both consultants and organizations should be conducted. So it is essential to conduct both desk research and interviews to get an proper answer to this question. For the sake of the quality of the interview, the literature study should be (partly) finished before creating a interview design.

The answer to this question will contribute to answering the main research question as the implications of teleworking can be part of the cybersecurity challenges. Moreover, the answer will establish a understanding of the current context.

3.2.3. Sub-question 2 - Risks & Threats

"What cybersecurity risks and threats are related to high levels of teleworking?"

Despite this question seeming similar to first question, this question is only focusing on the cybersecurity risks and threats of organizations instead of other implications as well. Once the current situation of organizations is well understood, one can dive deeper into the cybersecurity risk and threats that are the result of this situation. Academic literature and reports are very useful for answering at least a part of this question. As since at least 2 years ago a lot more organizations were forced to implement a crisis-induced hybrid working model. So at this moment there are a significant amount of articles that report the cybersecurity risks and threats that are related to the high levels of teleworking.

Regardless of the information retrieved from literature, there is still a need to conduct interviews with both consultants and organizations to complement the literature and show different perspectives as the situation for each party can differ a lot. It could be for example that the literature report a lot of risks and threats in organizations that are not recognized by certain organizations or lack behind as the current situation already uncovered new risks and threats. So in order to prevent this, different perspectives and sources of data seem to be necessary to give a proper answer to this question.

Similar to the contribution made by the first question's answer to answering the main research question, it is likely that certain risks and threats are part of the cybersecurity challenges related to the crisis induced hybrid working model.

3.2.4. Sub-question 3 - Challenges

"What are the main cybersecurity challenges that are related to the high levels of teleworking?"

Challenges & Risks differences

This question might seem similar to the second question. However, for this research a challenge is not the same as a risk or a threat. Therefore, this difference is important to understand since the main focus of this research is to understand the cybersecurity challenges. A risk can be part of a cybersecurity challenge that an organization has, but this does not have to be the case. An organization can possibly have several main cybersecurity challenges that are not related to specific threats or risks, there are more factors that play a role in a challenges.

Another reason this distinction has been made is to not only understand what risks and threats are associated with teleworking, but also what makes it difficult to manage some of these risks. In this case the risks and threats are external and the organizations' perceived difficulties in responding to them can be described as a challenge. For example, resources or privacy of the employees limits organizations in improving their cybersecurity and controlling certain security risks that are the result of increased teleworking. There are also security risks and threats that are more easily controlled, so these are not part of a challenge.

Although data regarding security risks and threats associated with high levels of teleworking is available, data regarding the challenges is not, so the main source of data that will be used to answer this question will be the interviews. The answer to this sub-question shows the organizations' cybersecurity challenges, which is required for answering the next sub-question and the main research question.

3.2.5. Sub-question 4 - Approach

"How are organizations approaching these identified challenges"

The next step is to obtain information on how organizations manage the identified challenges. As the main research question requires information regarding the organizations' approach to manage cybersecurity challenges, the answer to this question should focus on this management as well.

More importantly, the cybersecurity practices used by organizations should be understood. Especially the practices used to counter the threats and risks that are included in the answer of the second question. The literature can only provide limited information as organizations can differ a lot, so can their cybersecurity management. It will be very valuable to obtain information about an organizations' specific risks and threats and their response, as this can not be found in the literature.

This question will contribute to answering the main research question as the answer to this question can help establishing a clear view of how organizations manage these cybersecurity challenges mentioned in answer of sub-question 3. Which is important as a part of the goal of this research is to understand how organizations manage the cybersecurity challenges they have. As mentioned in the previous subsection, challenges are difficulties in handling certain risk and threats. This sub-question will mainly focus on how organizations are responding to these difficulties. So for example, organizations have identified certain risks and threats related to teleworking and are not able to effectively manage these. Although this is considered a challenge, organizations are likely to approach such challenges in order to improve their security. The answer to this question will be how organizations currently approach these identified challenges.

This question builds upon the answer of the last question. After obtaining enough information regarding the organizations' context, the risks and the challenges, the last part that is necessary to answer the main research question is the answer to this question. As the main source of data from the previous question is the interviews, it seems best to use mainly the interviews to answer this question as well. Especially as the challenges and their approach to managing them are different for each organization, so it does not make sense to use a significant amount of literature to help answering this question. Furthermore, the appropriate literature is might not even available at this moment.

Although this is not the last sub-question, this is the last sub-question that is deemed necessary to give an complete answer to the main research question.

3.2.6. Sub-question 5 - Consultants vs. Organizations

"How do the challenges and approaches stated by the organizations differ from those stated by the consultants?"

The combination of the perspective of both consultants and organizations will shine light on the problem from two different angles. There is a possibility that due to the fact that the interests of both actors are not the same, that the identified challenges are not either. Aforementioned, organizations also differ a lot, this research does not select on for example industry, size or maturity, so this could also be a reason that these challenges differ. For this reason, the required data should derive only from the interviews. Despite being able to answer the research question without this question, the answer to this question will still complement this goal of this research by providing an opening for future research that support organizations in improving their cybersecurity. Moreover, the answer to this question might also help understanding why these challenges are different.

3.3. Research design

This section of the paper will focus on the respondent selection, the interview protocol and the validity & reliability of this research. Furthermore, the selected consultants and organizations are anonymized are presented in the upcoming section.

3.3.1. Selection of respondents

The process of choosing the right respondents started very early in the process. The first thing to think about is who is able to provide the data that is required to answer the research questions. Aforementioned, individuals that are responsible for the cybersecurity inside an organization have insight in

the organizations' security challenges and risks, so this actor should be targeted. Furthermore, consultants that work with their clients on cybersecurity challenges also have insights in the cybersecurity management of organizations. The goal is to find a mix of both individuals at organizations that are responsible for protecting their organization from cyber threats and consultants given their different perspectives. As doing this research at PwC which enables interns to interview colleagues that have an expertise in various fields, it seems a good decision to also select consultants from PwC. The consultants that are working at the Cybersecurity & Privacy department are supporting organizations with their cybersecurity challenges, so this is a good match given the goal of this research. These colleagues should be contacted first to find out if the person is eligible for the interview. As this research is focusing on a phenomenon that started in the beginning of 2020, it is preferred that the candidate is working in this field for more than three years, so it has experienced organizations switching to the crisis-induced hybrid working model. However, the consultants are not selected based on relevant experience with organizations in specific industries or other characteristics.

As the consultants within this same company do probably not have very diverse perspectives, so it is not deemed necessary to conduct interviews with more than a handful of these consultants. Therefore the decision has been made to only interview two colleagues and find two consultants outside of PwC with relevant expertise. So the interviewed consultants work at three different organizations to provide a mixed view and prevent a saturated perspective from only PwC consultants. The names of other two organizations will not be mentioned due to ethical considerations. Aforementioned, organizations are not selected based on a lot of their characteristics. However, being large enough to have a IT manager, CISO or at least someone that is responsible for their cybersecurity management and is eligible for answering the questions, is required. Otherwise, it is possible that the person that will be interviewed is not able to answer a significant amount of the questions due to lack of knowledge. Of course, the fact that some organizations are not able to answer certain questions might be an interesting finding as well. However, that is not the goal of this research, so this should not be aimed at. Furthermore, organizations that for example did not have experienced an abrupt shift to hybrid working as they were excluded from the general restrictions due to their vital role in society, it becomes less interesting to hear their experience. In contrast to the consultants, organizations do probably have diverse perspective given all their characteristics. It would be possible to contact organizations through the internship company PwC. However, since already two consultants from PwC are interviewed, selecting organizations that are clients of these consultants could result in similar or biased answers. For this reason, none of the selected organizations are direct clients of PwC. Organizations are selected from the researcher's own network based upon the previously mentioned characteristics. Interview invitations with the corresponding TU Delft ethics consent form were sent to the respondents. The invitations did contain a summary of the research goal and some context, but without the interview questions to prevent bias. The possibility has been given to do physical interviews and given the research area, it seems appropriate to also be open to online interviews using a communication service that is preferred by the respondent.

Table 3.1 will show the respondents that were interviewed for this research. Their name and company name are not provided given ethical considerations that are discussed in more detail in subsection 3.3.4. Furthermore, a summary with the interview details containing the length, date and duration of the interviews is provided in the same table. The duration of the interviews refers to the duration of the recording, not the whole meeting. All meetings were in finished around one hour. A similar table 3.2 show this information related to the interview respondents from organizations. Section 4.1 provides a more in-dept discussion of the professions of both the interviewed consultants and organizations.

Table 3.1: Consultant respondents

Interview date	Position	Communication channel	Duration
10-6-'22	SOC Analyst	Microsoft Teams	32 min
10-6-'22	Cybersecurity & Privacy Consultant	Google Meet	38 min
23-6-'22	Principal Consultant	Microsoft Teams	53 min
28-6-'22	Cybersecurity & Privacy Consultant	Google Meet	37 min

Table 3.2: Organization respondents

Interview date	Position	Communication channel	Duration
23-6-'22	Security Officer	Microsoft Teams	32 min
23-6-'22	CISO	Microsoft Teams	31 min
26-6-'22	Cybersecurity Project manager	Microsoft Teams	36 min
27-6-'22	CISO	Microsoft Teams	33 min
29-6-'22	CISO	Microsoft Teams	46 min

3.3.2. Interview protocol

Section 3.2 shows what information is required to be able to answer the sub-questions. So this is used to build an interview protocol that helps obtaining this data. This interview protocols can be found in Appendix 7.1, this appendix also elaborates on the reason each question is part of this protocol. The protocols for consultants and organization are different, but still very similar. The first few questions are general questions to understand the role and the experience of the interviewee. Subsequently, questions will be asked that are related to the levels of teleworking in the concerning organization or clients and how this has affected their organizations. Afterwards the questions aim to get an answer to the sub-questions related to the cybersecurity risks and challenges related to this IT change. Ending with several questions to uncover how organizations are approaching such challenges. Looking at these questions, they do follow the same order as the sub-questions and have similarities. However, since this protocol is used for a semi-structured interviews, there is possibility to ask additional questions and aim to uncover specific challenges. Especially, since the questions that will be asked can be interpreted in various ways. For example understanding the difference between risks and challenges is very important, but without discussing this difference, the respondent might be confused. So during the interviews, further explanations will be given and all concepts will be discussed in great detail.

The order of the interviews is deemed important given the interest to use the information from the interviews with the consultants in the interviews with the organizations.

3.3.3. Data processing method

Each of the participants were questioned for up to one hour. A great advantage of this qualitative research method is the large amount of data that is gathered that can be used for the analysis [86]. However, the downside is that hours of recorded interviews should be processed, which can be very time consuming. The conducted interviews are recorded using among other communication services, Microsoft Teams or Google Meets. These recordings are saved in a video file or M4A audio file. The length of the interviews vary between 30 minutes and one hour, which is shown in table 3.1.

The first step to take processing this data is to start with transcribing which enables one to study the data in more detail once it is coded [87]. There are several online transcription tools available that is able to turn a audio file into notes. Despite not being completely accurate, this software is very helpful and saves a lot of time.All the interviews were held in the same language as this report is written in, so there is no need to translate any of the text.

Subsequently, to further prepare the data for analysis, coding will reduce the large amount of data and turn this into useful information [86]. Coding allows the researcher to organize, structure and interpreted the data in the transcriptions. There are three different coding concepts; open, axial and selective coding. Starting with open coding, where the transcripts are broken into discrete parts that are labeled by codes. The codes developed in open coding are linked together during the axial coding process and are put into several categories. The final phase is selective coding, the researcher identifies one core category and looks for relations between the categories, but also to remove codes that can not find enough support [88].

Given the pre-defined sub-questions and the semi-structured interview protocol that is derived from these questions, there will be several themes that will be focused on. For this reason the decision was made to use 'Codebook Thematic Analysis'. Codebook TA allows the researcher to use initially developed themes, but also new themes can be identified through inductive data engagement and analysis [89]. The used codes are data-driven although theory was used to formulate the interview protocol which aims to support the research goals. The data-driven codes and the themes are defined according to the steps described by Braun & Clarke [90]. These codes will form several codebooks that will contribute to answering the sub-questions in chapter 4.

3.3.4. Ethical considerations

As mentioned before in the research design, the data will be anonymized. Publishment of this paper is required according to the TU Delft's graduation rules. Although there is no need to process very sensitive data, the organizations and consultants might not want to have their name and company name published in this report. They do share information regarding their cybersecurity approach to manage their specific challenges and it does make sense that these actors do not want this information to be linked to the organization the are working for or what the clients of the consultants are, as this might even be confidential.

In addition, the consent from the interviewees is very important. To be sure of the interviewees' consent in partaking in this research, a form was used that the interviewees have signed. Furthermore, the obtained research data, like the audio files and transcripts with the data that can be linked to actors or actors' company will be deleted after the anonymized transcripts are finalized. Also the respondents can request their transcription that is used in this research to check for sensitive information. During the research process having high ethical standards was considered an essential part. This is in particular important given the goal to support organizations improving their cybersecurity, so possibly harming participants helping to achieve to this goal would be unacceptable. To make sure there is as less risk as possible, even the anonymized transcripts will not be included in the final product that will become public. However, these will be discussed with the supervisors and are saved until the end this research.

4

Results

This section will present the findings of both the interviews and the literature review. In order to remain a clear structure, the findings will be presented in the order of the formulated sub-questions and the themes identified during the thematic analysis of the transcripts. Certain findings or quotes of the interviewees will be specifically discussed.

In the final part of this chapter, the sub-questions will be answered using the literature review and the discussed findings of the interviews with both the consultants and organizations. The main research question will be answered in chapter 6 as this requires all the answers of the sub-questions.

4.1. Profession and expertise

Before starting with the first section that analyzes the data retrieved from literature and interviews it is important to understand what the professions and the expertise of the interviewees are as this is important for the credibility of the data.

4.1.1. Experienced specialists

Starting with the consultants that already have been shortly introduced in table 3.1. In the following subsection these consultants will be assigned E1 to E4 according to the order of the table.

The first consultant (E1) works as an Security Operations Center analyst for an organization that provides several services to clients. E1 works in the department that monitors the network and infrastructure of the client in order to detect possible cybersecurity threats. If one or more are detected, the client will be notified immediately. The organization also offers other services like pen testing, but he mostly focuses on the defense aspect. In addition to monitoring and detecting, they do the investigation of the data that is behind the alerts and advise the clients on future steps. The consultant is also involved in daily monitoring of customers regarding any possible incidents. The clients he is working are is various industries but mainly critical infrastructure, so universities, government agencies, power companies, airports. The sort of clients that if they get hacked there would be an significant impact to society. They are currently monitoring around 160 clients.

The next consultant (E2) is mainly focusing on tasks like, ISO27001 certifications, security assessments, but also privacy assessments, work related to GDPR and crisis work. The organization E2 is working at also have a crisis department in which they among other things develop, simulations and tabletops for clients. But E2 is mainly involved with cybersecurity projects since he started at the organization. The clients of E2 are in various industries, like tech, financial, healthcare, retail sector and lately also the entertainment industry.

The third consultant (E3) has worked for almost 20 years in different IT roles at a organization in the industrial infrastructure industry, where the last few years as IT and Operational Technology (OT) manager. The reason this interviewee is categorized as 'expert' and not as 'organization' is because of E3's current role as principal consultant in a cybersecurity company for the OT environment. E3 started this role a few months into the pandemic, so the decision is made to use his perspective as an consultant and expert. In the role E3 if fulfilling security assessments, pen tests are conducting at

clients. Furthermore, they do remediation sessions to follow up on the findings and recommendations given to the clients, to ensure improvements.

Although the last consultant (E4) does not yet have multiple years of experience, E4 is currently a cybersecurity consultant that is also involved in privacy and risk assessments. On a daily basis a great part of the responsibilities is the legwork, so E4 is learning a lot of information along the way. The clients the interviewee is working with are in very different industries, so public organizations, semi-public organizations and a lot of private organizations.

4.1.2. Relevant roles in organizations

Secondly, the respondents that currently are working and were working during the pandemic. They all have a function inside an organization that enables them to answer the interview questions stated in the interview protocol in table 7.2.The roles and expertise of these interviewees will be discussed in this subsection similar to how the consultants were discussed in the previous subsection and are named O1 to O5. So why they are able to give a proper answer to these questions will become clear as well.

The first organization interviewee (O1) is currently a security officer at an organization that is working in different business units and from the headquarters there is Global IT that provides IT services throughout the business unit. O1 is a security officer within the security team and has colleagues in various countries. This interviewee is often performing business impact assessments and making process improvements like automation. Furthermore O1 is also defining the privacy impact assessment process and has implemented cybersecurity e-learnings related to for example phishing. But also privacy e-learnings. The business assessments they perform sometimes also include privacy risks although this is not their department's formal responsibility, but is one of the projects O1 is working on.

The next candidate (O2) is currently fulfilling a relevant role in a organization that is operating in the financial service industry. The organization among other things creates applications and web front ends in a local platform. They can create applications far quicker than having a own development team and can be changed easier. It is a rapidly growing company which is based in America and have tens of millions clients using their applications with billions of USD being managed through their services. Before being closely involved with the growth of this company, O2 worked in large businesses in the payment industry as CISO. Currently O2 is head of Information Security, but O2 is combining information security with business continuity management in one function. The team that this candidate is managing looks at IT risks, cybersecurity, information security and also physical activity management. Everything is done from a resilience perspective, where there is a risk involved that cannot provide the continuity of the service to their clients, they are combining that in one function at the organization.

Despite the recording of the third interview with an organization not being complete as the introduction is missing, a small introduction can be given based on the rest of the interview. O3 is currently working in a cybersecurity program as a Project manager and has been with the organization for more than 20 years. The program they are working on is divided into an IT and OT program. Among other things they developed modules in their HR system that were mandatory to follow to understand the cybersecurity risks. For example how one can recognize certain phishing emails.

The fourth interviewee is fulfilling the role of CISO at a municipality. O4 is working to get the organization into the cybersecurity mindset and making sure that the organization is growing in the cyber resilience. There are also departments that are responsible for these goals, but O4 translates everything in an understandable language to the board. Before working at the current, O4 had experiences in IT project management and quality assurance manager that supported the IT management by helping to understand the IT audits.

The fifth interviewee (O5) is CISO of an organization that is basically an ecosystem of smaller It companies in various maturity stages. The ecosystem consists of companies specialized in Business Intelligence, creating applications, ERP systems, and more. All these companies have their own security officer that report to O5. O5 provides the corporate policy and translates the mission and vision of the company to their security strategy. Furthermore O5 provides basic services for the companies in the ecosystem which they can use in their security landscape, for example standardized awareness training. The individual companies have their own security policies as well, but these must comply to the corporate policy.

4.2. Phase and implications

As the literature study suggests, teleworking has been around for quite a while. It is since the start of the pandemic that the majority of the organizations were forced to implement a variation of a crisis-induced hybrid working model. Since most employees that were teleworking during the pandemic kept doing this even after most restrictions dropped, high levels of teleworking are believed to be the new normal. However, despite the high levels of teleworking, one can argue that the crisis-induced hybrid working is no longer in place in most organizations as it has more characteristics of the conventional teleworking model. Like for example being voluntary, part of the working hours and adaption of physical working environment, also shown in figure 2.1. Not only employees but also managers prefer a type of hybrid working model but not fully remote, which seems like there is a preference for a conventional teleworking model, so there will likely be a shift from the crisis-induced teleworking model to the conventional model.

Given that the implementation of these crisis-induced hybrid working model resulted in employees being kept inside their own homes, this caused several implications aside from the cybersecurity aspect. Implications like lack of social interaction, working as a team being more difficult, lack of access to data, are reported. Although literature provides this information, the interviews with the respondents can show how their organizations are affected by the increase use of teleworking.

Both consultants and organizations were asked questions during the interviews to acquire this knowledge. Starting with the consultants that have been working with multiple international clients and are able to provide their insights. Organizations were able to provide a more detailed answer as they have better access to this information, but they do lack the ability to make statements regarding other organizations. However, this does not apply to all interviewees from organizations as some of the candidates were able to provide information that is related to other organizations.

4.2.1. Phase

As a starting point it is important to understand the presence of teleworking of teleworking among the organizations and the clients of the consultants. The scope of this research has been kept broad on purpose, this requires extra attention to certain aspects. Despite the fact that almost all organizations had to deal with the restrictions imposed by the government, there are always exceptions. Given the goal of this research, it would not be valuable nor make sense to acquire data of organizations that have not implemented a teleworking model that resulted in an significant share of the workforce working remote. This has been taken into account during the selection of the respondents, but the more detailed picture will be discussed in this subsection. Table 4.1 shows the theme and sub-themes that were identified during the thematic analysis

Table 4.1: Theme and sub-themes of teleworking phase

Current levels of teleworking
Dominant teleworking levels
Mixed levels
Shift back

The levels of teleworking among organizations vary a lot. Not all respondents were able to give a very detailed answers to what extent their clients or their are subject to high levels of teleworking, but could give a proper indication.

Dominant teleworking levels

Even within organizations it can vary a lot between departments of the organizations. O1 states that half of their office population is working from home, while there is also a section of the office that is still working completely from home. Also a large share of the organization is working in operations and were not forced to work from home, which is more than half of the organization.

O2 already shows a different situation where they currently have around 30% of the teleworking levels before the start of the pandemic, so most of the employees are working from home. Similar to the situation of O1, it varies a lot among departments, finance are almost always at the office, while other departments are completely working remote. O2 even states that there are employees that do not want

to come back to the office at all. According to the respondent that has a technology company, this can be explained by the fact that developers tend to appreciate to appreciate to work in their own time and environment. Given that the company is very innovate and they like to do things differently, O2 does not think that they are going back to where they were in the past.

Also O3 notices hands-on that before the pandemic it was hard to find a spot at the office while you are now able to sit everywhere. Although the organization do asks its employees to work at the office certain days, this request seems to stay unanswered.

At the organization O4 is working for there are no policies that enforces their workforce to come back to the office. O4 estimates that only around 20 % of the time employees are back to the office.

All the employees of O5's organization are currently working 3 days at home and 2 days at the office. However, just like O1 and O2 already mentioned, it varies from role to role. While most of the employees are programmers and consultants, this type of work can easily be done from home.

Mixed levels

Although E1 does not have a clear picture the working models implemented at the clients, E1 would say that maybe 50% of the clients are subject to high levels of teleworking and to his knowledge, they do not have clients that are completely working on site.

E2 saw that the Nordic countries moved back their workforce relatively faster than the Netherlands, but almost all clients are now about 50% working from home and working at the office. Most of E2's clients in the Netherlands are in the public sector and according to E2 the public sector is a bit more hesitant in coming back to office in contrast to other industries. Since the pandemic they started doing site visits virtually, which also shows that a lot of the office personnel is working from home: "I mean somebody walking around with the camera and going to the office. So that is when you can see that there are not that many people at the office. In some case clients even have to go to the office as the only one to perform the site visit when no one is around.".

At E3's clients it is also still a mixture of both working remotely and at the office. A lot of tasks can not be performed remotely, there is remote access for emergency support, but the service engineers that conduct maintenance activities are required on site as it is too large and cumbersome to do that type of work from a workstation. This also applies to the employees that work with the suppliers, so the logistics can be managed properly.

Shift back

Although E4 does believe that there is currently is a shift in progress of the workforce going back to the office, a lot of clients and E4's organization have adopted a hyrbid working model. Again it is mentioned that desk jobs can easily be done from home, while the industrial jobs, such as maintenance are really hard to do from home. So some organizations moved back to the office, but still a lot are almost completely working remote. According to E4, especially the small and medium sized companies try to get their people back in the office. Despite the efforts, the respondent is confident that the pre-covid levels will not return.

O2 believes that their innovative company will not go back to how things were in the past. However, this might not apply to the other companies in his area. Visibility and making a lot of hours in the office used to be a very important aspect in the working culture of the country the organization is operating in, while work-life balance is not (yet). The offices in the Netherlands for example are already set up a little bit for remote working, because of the working culture and the way they work part time.

4.2.2. Implications

At first glance the implications that the increase in use of teleworking have on an organization might not be related to the cybersecurity challenges and the approach of organizations. However, the cybersecurity challenges are more than just the risks and it is possible that these implications have become part of an organizations cybersecurity challenge. Or at least show more context of the High levels levels of teleworking could have affected or will affect the organization in such way that this will also result in related cybersecurity challenge. Or if it does not, it would at least help to better understand the challenge.

Table 4.2: Theme and sub-themes of implications

Well being of employees	Benefits	Not affected	Communication
Higher work pressure	No physical presence		Challenge to connect
Private vs work	More productive / efficient		Threshold to communicate
Less productive	Less travel time		

Three main themes were identified during the thematic analysis. As shown in table 4.2 a lot of the implications refer to the well being of the employees instead of processes or technology. Of course these themes will be touched upon in the upcoming sections, but it is quite interesting that they are not frequently mentioned during the interviews.

Well being of employees

The literature study softly touched upon this topic, but it did not seemed to be the main subject the respondents would come up with. Starting with the higher work pressure, E2 often experiences a large amount of meetings without any breaks throughout the day. A lot of the meetings end in another meeting starting in just a few minutes. This is not only internal, but also happens at E2's clients, which significantly increased the stress during the day. E2 explained this as follows:

> *"Normally if you have physical meetings, you would have a few minutes that you would physically walk to a meeting or grab a coffee with everyone and have purposely long meetings with built in breaks. But now we have clients actually request to go on without breaks....*

Breaks are not taken into account anymore which has increased stress during the day. This slowly slips in and is noticed once the pressure is very high.

Besides the back-to-back meetings, E4 states that the working hours are longer. At the office one would just work their standard 9-5 hours, while at home you would make up for the hours you are having lunch or a private call later in the evening to make up for the lost time. This statement is similar to what O3 experiences, who is tempted to work longer hours each day till late in the evening when working from home. O4 links this higher working pressure due to high levels of teleworking to the merged work and private environment. Although the respondent was able to focus more at home, the private environment also became the 24/7 working environment.

The organization of O5 was very successful during the pandemic, so the working pressure was high regardless of the large share of employees working from home. However, according to O5 it is harder to enforce your own boundaries when people are working from home. Normally you would for example have to catch the train or leave before traffic jam, but once you are already at home, this boundary is gone. So O5 sees a lot of people putting in more hours than is healthy for them. This applies to O1 as well saying that once it is time to stop working at home, it is easy to confess just one more hour, which you would not have at organization's premise.

Not only the clear line between the private and working environment broke down, team cohesion suffered as well. E4 states that you now have to plan moments to talk to certain people and that just does not happen that often, which results in less team cohesion. O1 shares this experience. Once a lot of the employees are working from home often and you occasionally come to the office, you have to make use of the moment to speak to this colleague. According to O5 once such situation of extremely high levels of teleworking last too long, people start to become disconnected and bubbles are formed. Bubbles within companies of people that think something of the company for example and become unhappy as group. Now you have to plan these social moments outside the bubbles.

Furthermore, O1 mentions that there are a significant amount of people that would say that they have not been as productive at home because they get distracted. The reason why is not clear, but O1 thinks that some people do need people around them.

Benefits

The question asked regarding the implications of the pandemic were fairly open. Despite the expectation being that the respondent would mention negative implications, there were respondent mentioning benefits to the organization. E4 for example mentioned that not being forced to be physically present all the time is experienced as an advantage. Also O1 states that the large majority of people have said

that they do work more productive at home. Although O3 earlier mentioned that the working pressure increased, some of the tasks are getting more efficient once you have the right tooling.

Furthermore, you do not have to travel to the office that often which saves time, as well as not having to settle in which requires time. So not being required to do everything from one central point while complying with all the standards saves a lot of time. The role of O4 normally requires the respondent to travel to other cities, so the less travel time is a major advantage.

Not affected

As earlier mentioned the majority of E3's clients' employees are not all working at the office in cubicles, but at in large operation rooms. So E3 did not report any implications to their clients as a result of the high levels of teleworking. According to O2 there are always complaints that the work pressure is too high, but this does not have anything to do with the levels of teleworking. Despite the comments made by O5 regarding the employees', O5 do not thinks the high levels had very adverse effect on the organization

Limited Communication

The points made might sound similar to the statements made regarding the team cohesion, but the following points are not directly related to the well-being of the employees. E1 mentioned that due to high levels of teleworking there are a limited number of incident respondent at the client's side and it was more difficult to contact them. Furthermore, once contact was established it was harder for the respondents to investigate certain alerts as everyone is working remote. So the whole response chain was slower. Internally there are also communication challenges related to high levels of teleworking given that according to O4, it is difficult to have big sessions or new ideas without being at the office. O5 also realizes that some communication works better in person than at home and even says that a lot of security is done at the coffee machine.

In the experience of O1, this is not only with big groups or new ideas, O1 mentions that sometimes communication on smaller topics does not happen anymore. This only happens once you meet each other at the office, but not when you are working from home and even mentions that there is a threshold for people to start communicating:

> *"That this very simple communication that you would normally have in the office is not really something you would do through a message in chat or an e-mail. So I would say there is a real high threshold for people to start communicating."*

Despite it being 'simple' communication, according to O1, this can be a question that might enable you to proceed with certain activities while working from home.

Also O3 agrees that you hear conversations of other colleagues at the office and you get a lot of updates that you would not get at home. There is also specific relevant information that only comes up when you are getting coffee with colleagues.

4.3. Related cybersecurity risks

Moving on the the next part of this research topic, the main risks that are the result of the high levels of teleworking. It is important at this point to again understand that a lot of the risks related to teleworking already existed before the pandemic and the start of organizations implementing such crisis-induced teleworking models. It is possible that before this start these risks were negligible or at least not of great importance to organizations. However, some of these risks got amplified since the volume and frequency of employees working remote increased. How the high levels of teleworking affected these cybersecurity risks will be discussed in this section. In subsection 2.2.3 of the literature study, the distinction is made between employee-related risks and technology-related risks. As it does not seem particularly useful to repeat this list of risks before the analysis of the interviews, these risks will be discussed in combination with the findings of the interviews.

Starting with the themes and sub-themes identified during the thematic analysis of the interviews. Table 4.3 shows the themes and sub-themes identified during the thematic analysis. One can notice that these themes do seem to differ a lot from the two groups of risks in the literature study, during the discussion of these themes it will become clear that a lot of risks mentioned in the literature study will be addressed under these themes.

Table 4.3: Theme and sub-themes of risks

Controlled environment	Behaviour of the workforce
Physical security & IoT risks	Knowledge & awareness
Control & monitoring	Bypassing policies
Information exchange	Corrective behaviour
Device & patch management	
Access management	

4.3.1. Controlled environment

Physical security & IoT risks

Although this theme is interconnected with access management, there are some distinctions that can be made. Consultant E2 states that organizations can control the physical security of the work place at the office by for example security gates, or floors with restricted areas. These security guarantees are not present at home, it is easier for an somebody to for example look through a window to look at your screen or go trough the trash to find notes with classified information. Especially since a lot of employees might not have their own shredder at home. The only thing an attacker has to do is look up who is working for the organization and find out where this person lives. This would also apply to friends or roommates, they would not easily access the office, but looking around an employee's house, finding interesting information or listening in is a lot easier.

E4 describes a similar situation as follows:

> *"...if your neighbour is a malicious actor and is checking your screen the whole day while your handling sensitive data. That is not even technical, but that is a real weakness and a vulnerability."*

This respondent uses the Evil maid attack as an example to describe the last point made by E2. The employee's partner, family member or even the delivery guy can all easily access the corporate. That corporate security is not the same at employees' private environments and that imposes a lot of security vulnerabilities. Although one would assume your own home is a safe environment. This might seem like a risk with a low likelihood, but E4 defends this by saying that :

> *"You would say "what are the chances", but once everybody is working from home and you have one malicious actor trying to gain access, cracking into a office building is a lot harder than some random employee at home."*

Although O1 acknowledges that it is best practice to always lock your devices at home, O1 does not believe it is a larger risk to leave your laptop unguarded in your home for a short period than in the office and feels a bit safer at home as nobody is around. However, O1 always locks all valuables away and properly hides it once the interviewee leaves the house.

The physical security is even more important at the organization of O2, since housing in that country is more expensive compared to Europe. While people in Europe often have their own private room to work in, people working at O2's organization do not have mortgages and live and work at home for a long time. In meetings O2 sees a lot of people in the background, working, or sharing rooms. So the physical security you would normally have in the office, does not exist at the employees home anymore.

O3 does not feel concerned about this risk and mentions that during meetings O3's partner for example might be able to listen, but will not do anything with the information. O4 also mentions that in one way it is also less of a risk since the employees home is a small environment instead of the office.

Consultant E2 emphasized the importance of IoT security, IoT devices can impose a risk as well:

> *"Any IoT device for example a security camera at home can be tapped into or just your router can be tapped into by an attacker to propagate throughout your own network."*

Despite that the attacker might not be able to directly enter the corporate network, it could possible pick up information using the microphone of any of the IoT devices connected to the personal network and steal sensitive information from clients. Or for example access a camera and being able to read such information.

Again E4 mentions this risk as well giving the example of the AliExpress light bulbs the respondent has in the private working environment. These IoT devices are very insecure, which means that the WiFi network is very vulnerable as well. According to this expert, VPN fixes this risk for the most part by encrypting the data, but it is not fail prove. VPNs also have vulnerabilities and is dependent on the provider and the third parties managing the cybersecurity as a whole.

O5 even has an example of such attack happening and gives another example describing this risk:

> *"I've encountered an example of a hacked home router which was captured by some Russian speaking group who took over the cameras in the house, depending on where they are they could have been looking at your keyboard...Also for example wireless keyboards, if you buy a cheap one, I can see your key strokes down the street."*

Control & monitoring

Organizations are able to control who comes in and out of the office, like discussed in the previous sub-theme regarding the physical security. However, this sub-theme dives deeper into the lack of control and ability to monitor the security once their employees are working from home.

E2 brings up the example of the clear desk and screen policy. Once employees are working at home it is harder to control the cyber hygiene of the employees and monitor if the security policies are being properly followed. Even when there is a perfectly working device management solution in place, this does not cover everything.

It is not possible for organizations to check if employees all have safe routers or no IoT devices, that is basically out of the control of organizations, according to E4. As an organization you can also not ask to work in a room without windows for example. Furthermore, despite maybe being able to monitor systems and applications of the employees, an organization can not see if the laptop is being used for example by another member of the family for doing private business

O3 agrees that it is hard for managers to monitor the employees since they are working from home. According to O4, it is not possible for organizations to search for example to local drives of the employees as this is their private environment. The same applies to the clear desk policy that is mentioned earlier in this section, O4 gave the following example:

> *"For example keeping a clean desk, you can not see my desk and I should keep it clean, but it is my private environment."*

So it is a risk that as an organization you are not able to completely monitor the employees.

Information exchange

The moment a large share of the workforce started working remote, the amount of people using third party communication increased as well. According to E1, once the amount of users of software like Teams and Zoom started to exponentially increase, it became more interesting for adversaries to find vulnerabilities in this software and exploit these. Evert software always has vulnerabilities, but even earlier in the pandemic critical bugs were found in Zoom as well as vulnerabilities in Citrix in the last few years. So once you increase the volume, you make it more interesting to attack this kind of software. Furthermore, since the levels of teleworking are so high, people can not exchange information physically anymore, more information will be shared through unsecured channels. Especially if people start to use for example the free version of Google Drive. E1 further explains this:

> *"If you've ever read the terms and conditions of Google Drive. If you're using the free version, you accept the fact that Google can read all your documents and use them to improve their service because it is free. So it's not so nice if you're sharing company secret documents that way, because Google now also knows that is in these documents."*

E3 gives a similar example of using these types of free software:

> *"If you work remotely and still want to have the working in a team experience there are so many tools around on the internet where you can work as a team like Slack or Jabber, you must realize that there is no such thing as free software."*

Despite the efforts made by the organization to have a controlled environment, O3 receives invitations to meetings from Teams or other tooling that O3 has never heard about. O3 also mentions the example

of Zoom not being secure, so that is a point of attention. However, O3 does not believe information exchange risks are related to high levels of teleworking, since this has been in place before the pandemic. Sharing documents with someone from or with someone from the office, or at home, stays the same.

According to O4, since everyone is working online, more documents are being shared online, more collaboration online, with the increased possibility of downloading documents onto private environments. So there was a increased amount of document sharing, which could have an effect on data breaches. O4 adds that it is also a risk that big brother is watching you and where your data is stored due to new way of information exchange.

The following risk is related what is discussed in sub-section 4.2.2 regarding the limited communication among colleagues. According to E1 the result of this lack of communication among colleagues is an increase in phishing risks. Not only the standard phishing messages, but more sophisticated and targeted as well. An example given by E1:

> *"So what you would see for example is someone would imitate your manager or your CEO and they would send an email like "Hi, I'm in a busy meeting right now, can you please pay this bill".*

Such message would be send to one of the employees in finance that would regularly do transactions like this to legitimate parties. This so called CEO fraud is much harder to detect and E1 explains that they do not have a specific detection system in place for this type of phishing.

O1 did see a spike in phishing as well since the introduction of the crisis-induced teleworking model and has seen some quite significant breaches at the competitors of the company O1 is working for. Although O3 did not recognize this increase in phishing, O3 can understand that the risk has increased. However, O4 did notice that the amount of phishing attempts has increased due to people sharing more links and documents. Furthermore, O4 sees that the phishing attacks are more advanced. Recently they received an e-mail from an attacker that used an e-mail address that was similar to one of O4's colleagues and almost no differences were spotted. According to O4 this phishing attack was hard to recognize and adds the following to this statement:

> *"For me this is a sign that the phishing attacks evolved during the pandemic due to the way of file transferring."*

Device & Patch management

According to E1 companies were usually not able to quickly supply company managed devices to all the employees, so these employees started using private devices that were not managed by the company. Furthermore, it is harder to manage devices that are inside of the company's network, but spread among many employees. That is not the only problem, when the devices used for corporate purposes are not restricted properly, it is harder to manage these as well. E3 also sees that people are mixing up their business apps with their private apps on the devices, so business data and private data are not properly separated.Not only access control is important, also the additional security controls on these devices has to be more secured than before everyone started working from home. So if employees can use the devices without any restrictions, this can impose a serious security risk.

O1 mentions that during his time at the previous employer O1 was able to download all kinds of software, which at O1's current organization is not possible. However, at O1's organization employees are using unmanaged personal devices, which was already a problem before the start of the pandemic. O2 states that since the introduction of high levels of teleworking, they started to allow devices that they do not manage anymore, so they have to secure these endpoints which is a point of concern.

Similar to the point made by E3, O4 describes that despite having proper access control, the device could contain viruses because it was used for personal business for example. O5 has seen such event as well, with a BYOD from a colleague that let his kid play with the device resulted in an incident. E2 sees that especially the small immature clients often do not yet have a device management system in place despite this being included in several of the security standards as ISO or NIST that they are working with.

What is often mentioned during the interviews is patch management. This also related to software vulnerability, but seems to fit in this sub-theme as well. If organizations do not patch the software that is running on the device, the vulnerabilities can be exploited by attackers. E1 uses an example

of zero-day vulnerabilities, so vulnerabilities that have not been discovered yet. These can be hard to detect and are worth a lot of money to malicious actors to attack the targets. Especially if it is a critical vulnerability, all the software on the devices should be patched in a short period of time before it gets exploited. If a lot more devices now are using a large range of software tools, this might result in the devices not being secured on time. According to E1, the volume of attacks using this increased exponentially.

At the previous employer of O1, the device had to make a connection with a VPN to allow the device to update the configurations. There were people that did not connect to the VPN for a significant amount of time that resulted in a device that did not install the patches and was therefore unsecured. Even at his current employer in the past, the patching only happened once the employees were at the office, so once everybody started working from home, the patching of the devices stopped. O5 does mention a similar example of an attacker that just waits till the next Microsoft bug to claim access to the device.

Access management

According to E1, if employees are able to access the corporate network with for example a personal device, the company suddenly has a device on the network that is unfamiliar which can impose a risk to the network. A major risk described by E3 for example allowing only single-sign on or a poorly password policy and access control and supports the claim of E1 that if you allow remote access to you internal network from unsecured devices this would be significant risk. Furthermore, E4 states that there is a lot of stress on VPN networks which are not fail proof as well. E4 agrees that if employees are able to access the corporate environment through a VPN with their personal device, this would result in a serious risk.

O1 reports this the be one of the major cybersecurity risks of high levels of teleworking, employees using VPN connections on their private devices to log into the corporate network. At the current company O1 is working for this is not possible, but O1 still hears that this is happening a lot. Although O1 this was already a problem before the pandemic, O1 believes this is a larger problem right now. Moreover, employees being able to log into their private e-mail accounts that might not the same controls to detect for example phishing, could impose a risk as well despite the efforts made as an organization. Having a proper access management is one of the main concerns of O2 as well, using measures like Multi Factor Authentication (MFA). Also E4 sees that a lot of organizations that have not yet enabled MFA.

The same applies for O4, not knowing which devices are connected and how is a risk. Before managed devices were provided by the organization and despite the MFA that was already enabled, people were able to log into the central environment with their own private devices that might contain viruses.

4.3.2. Behaviour of the workforce

Knowledge & Awareness

This sub-theme is the most frequently mentioned among all the interviews. So knowledge and awareness seems to be an important risk factor regarding organizations' cybersecurity.

Starting with E1 that describes that most users do not have the required knowledge or awareness to properly manage their computer, especially in big companies. This relates to the previous discussed topics as well for example information exchange. A company can have a secure system to share files among other colleagues of the organization, but this is not enough according to E1:

> *"You can have this fancy file sharing service. But if your employees don't know about it, they'll just still use e-mail or Google Drive etc., and you will have the same problem"*

But also employees not knowing what the risks related to teleworking are is a risk. Not knowing how to for example share company documents, recognize phishing mails or don't leave anything on the personal laptop. What E1 saw especially in the beginning of the pandemic was that people often used private e-mails as they did not know how to set up their company email etc..

E3 confirms this by stating that people might not be aware of the fact that business data and private data should be separated. In addition, referring back to the example made by E3 related to information exchange, that here is no such thing as free software. If employees are working from home a lot and still want to have the 'colleague experience' and they are not aware of the security risks, they will seek for such unsecured collaboration tools if these are not blocked. According to E3 a lot of business data

is leaked because certain documents are uploaded to those environments and shared with other teams. Furthermore, in this situation, if the employee is also not aware of the need to use different passwords for the business and private environments, it is quite easy for a hacker to access the business environment.

O1 agrees that it is a huge risk to your device and network if people are not aware of the risks related to visiting Facebook, go to strange websites and submitting credentials to see funny videos. Related to the aforementioned risks that are the result of IoT devices, organizations need to depend a lot on the awareness of their employee that they have a proper cyber hygiene, according to O2.

One of the main risks state by O4 is indeed that documents are downloaded or sent to the private environments for printing purposes for example. If employees are not aware of the risks behind this practice, this will keep happening. O4 believes this risk will not just disappear and also sees that in his organization employees are meeting outside of the organization, not being aware of the risks working outside the controlled environment like discussed in subsection 4.3.1 can impose a significant risk as well.

Bypassing policies

In the subsection that discussed the device management, the risks that are the result of not restricting and managing devices properly were mentioned by the interviewees. However, restricting devices can also lead to other risks.

To start of, E3 mentioned an interesting example of such risk that is the result of restricting devices:

> *"You saw with Rutte as well, they'll say: 'My business email is too much restricted and it is too cumbersome to access, so I forward it to my personal email ... if you make it too difficult for your employees, people are creative, they will find a way out and browse the internet for solutions"*

This might not have anything to do with knowledge or awareness, but is mainly due to the convenience of the employees. A similar example is given by E1, if organizations block everything to mitigate risks, employees tend to just use their own laptop. They would for example send all the necessary information or emails to the private environment, to work from there. E3 uses the CEO fraud as an example as well, in the start of the pandemic a lot of processes were bypassed to implement such teleworking model, so in the beginning of the pandemic the risk of such incident happening is higher. A client of E3 restricted the file size of emails to mitigate risks, but this increased the risk of employees bypassing this control and sharing it through unsecured information exchange channels like discussed in subsection 4.3.1.

E4 connects this risk to the knowledge and awareness. Security measures often makes work harder, by for example implementing MFA methods, this takes time. However, if there is no security awareness, employees would see this as an obstacle for their work and might try to bypass this control.

The first interviewee to mention this risk was actually O1, this interviewee noticed that a lot of people automatically forward the corporate e-mails to their private e-mails so they can go through the e-mails on their private devices as well. Although O1 believes that this was already a problem, O1 believes that this has happened more often due to the high levels of teleworking and became a bigger problem. This also applies to the higher volume of people sharing their Google Drive folders with their private Google accounts, so they would have access in their private environments. O1 believes that the main drive for such behaviour is convenience and not being aware of possible consequences.

This can also possibly be linked to the implications mentioned by the respondents discussed in subsection 4.2.2. Although this is not studied nor discussed with the respondents, there is a possibility that the discussed implications have an impact on the behaviour of the workforce. For example, the implications: an higher working pressure or a threshold to communicate, might be an incentive for employees to bypass certain policies that are seen as obstacles to complete their tasks.

Corrective behaviour

This sub-theme is also very related to the controlled environment theme that is discussed earlier in this chapter. Once employees are not complying to the security policies at the office, colleagues will notice this and correct you, according to E2. Besides the inability to monitor and recognize this behaviour when employees are working from home, there are also no colleagues that would correct you. Even O3 describes one of his experiences that backs this statement:

"I think that 10 years ago I once forgot it and someone put everything that was on my screen upside down, so it took me almost half an hour to fix this, which resulted in me never doing that again"

O5 mentions the morality and integrity that is enforced as a group in terms of security. If employees are working at home and do not have much contact which each other, the integrity boundaries might start to shift. What was not acceptable at the office, suddenly becomes acceptable. Furthermore O5 gives an example that employees are easier to influence outside of the view of the organization, a bad actor has e larger chance of success turning an employee into being a bad actor as well:

"Well for instance there is a lot of news going around which is fake news, and fake news is often debunked in the conversation, when people talking about it. If you leave a person in isolation, it becomes harder and harder to discern the fake news from the real news. As soon as this actor starts to act on the fake news you have a problem"

4.4. The Challenges

Moving on to the identified themes that are related to the relevant cybersecurity challenges. A lot of the themes and sub themes identified closely relate to the challenges and some are even a combination of the risks that discussed in that section. This section will discuss these themes that describe the main cybersecurity challenges that are related to the high levels of teleworking.

4.4.1. Security vs. Privacy

The previous section regarding the cybersecurity risks related to the high levels of teleworking resulted in a discussion of several very interesting risks. With 'Controlled environment' as one of the two main themes and sub-themes that discussed the risks related to IoT devices, monitoring, device management and more. According to the interviews one of the reasons why these risks are a serious challenge to control is privacy. This is not particularly new, security versus privacy has always been an challenge for organization. But this cybersecurity challenge is especially related to the high levels of teleworking.

A large share of the workforce made their private infrastructure part of the corporate infrastructure by working from home. E2 states that as an organization you need to respect the employees privacy and the environment, while at the same time guarantee a certain level of security that they are performing. Coming back to the clear screen & desk policy discussed in the previous section, organizations want to ensure that employees are complying to such policy but are not able to due to privacy regulations. The same applies to the IoT devices in their home, that these devices in a certain way meet the company's standards.

E2 also adds an example explaining why this is, according to this interviewee one of the biggest hurdles to overcome:

"What you could do, theoretically is have somebody come over from the office, to work at your location or have IT set up your device. But, if these are their devices then you're already kind of disrespecting the employees' privacy. Because you are forcing somebody to get into their private home, forcing them to touch private equipment and mandating how they should design their private rooms."

E3 can agree on this topic, mentioning that there are certain measures as an organization you can take at the office that you can not take at the employees' homes.

"I can not ask you to pickup your laptop and do a 360 so I can see how tidy your room is, because that is privacy. So security shift a little bit from the office to the personal space and that is difficult..."

Moreover, O1 identifies privacy risks in the business impact assessment as well, but since privacy is not the formal responsibility, these risks are very hard for them to threat. So they need to think of handing this over to HR which is the responsible function within the organization to handle privacy risks.

For the organization of O2, privacy is a challenge as well. Especially since they want to enter major markets like Europe where privacy is far more important than it used to be in the O2's country. So it is

really a concern that they are responsible for, but for the employees themselves it is not, privacy is just not that well established as it is in Europe. According to O2, people still do not care that much about privacy as they think that they already know everything about them since they have lived under certain circumstances that they got used to the idea that the governments knows a lot about its citizens.

Furthermore, O4 points out as well that there is a line until where you as an organization can search or block certain things. When it is going to local drives, it is their private environments and sometimes it is technically difficult to not cross that line. According to O5 if and how you as an organization can actually check how employees deal with the security is hard as you are squarely in the privacy domain.

4.4.2. Control & Awareness

This challenge has already been discussed to some extent in sub-section 4.3.2, but this challenge does require more to completely understand. For controls to be effective, awareness of the practitioners is vital. The related risks to both individual topics were mentioned and during the thematic analysis it was clear that these topics were often discussed together. Without a doubt technical controls are important to keep your data and network secured. However, as E1 mentioned an interesting quote:

> *"The problem is between the chair and the keyboard."*

O2 also mentions that their biggest cybersecurity challenge is security awareness:

> *"We can do a lot with technology and processes. But the human behavior... I always put 'people' very big and 'processes' a little smaller and then really small 'technology'. A lot of security people think you can solve everything with technology, well in the end it is people work.*

Lastly O5 complements these statements by saying

> *"Technology, that is what everybody is looking at, but that is the easy part"*

Besides from these intriguing quotes and statements, what is also discussed in the previous section is that there are controls that are not effective if the workforce has no or little security awareness or knowledge. Just like E3 mentioned, O3 has a similar thought:

> *"If you impose a lot of restrictions, more people get creative and look for new solutions which makes it less secure."*

This almost supports the suggestion that implementing more controls to increase the security of the company might in the end decrease the security due to employees bypassing policies that might lead to even more risks, as a result of the lack of the employees' awareness. Of course the security awareness and knowledge of the officers implementing these measures is important. E3 was able to provide an interesting example illustrating how this challenge can manifests itself in practice:

> *"For example a client of mine on put a limit on the size of attachment their email service, so admitting above a few MB is blocked. So that is completely stupid because any malware dropper is like 20kB or something like that, so it is a completely false sense of security that they give themselves ... so employees go to Dropbox or go to WeTransfer, that is an example of thinking you're doing the right thing but actually doing the complete opposite."*

It must be understood that this is of course an extreme example where the control is not even effective on its own and this resulting in employees bypassing this control. However, this practical example also shows the importance of the knowledge and awareness of the officers implementing the controls and not only of those who have to work with them. In the last sub-section regarding the priorities of organizations, this will also be discussed.

This challenge also grew as a result of the increased importance due to the high levels of teleworking of the previous mentioned challenge regarding privacy. Without the organizations ability to fully monitor and control the private environment, they now need to depend a lot of their security on the awareness of the employees, according to E3.

4.4.3. Lack of resources

Until this point, most of the challenges were related to technology, knowledge or processes, but resources has not been mentioned yet. The introduction of this research touched upon the economic impact of the pandemic to illustrate the different environment organizations are in. However, as stated by several consultants and organizations during the interviews, there are also organizations that grew a lot during the pandemic. This sub-section will explain how the lack of resources is a challenge that is related to the high levels of teleworking.

Starting with E1, that earlier mentioned how important for example patch management is since a large share of the workforce started working from home and how time matters:

> *"You can't afford to wait a week ... You have to jump on it immediately and if your cyber-security team is not up to scratch then you might be late. You have to stay on top of your game."*

Additionally E1 states that it is not only the question how an organization can protect itself, but also how it can protect itself without costing too much. Cybersecurity is expensive and requires specialized people that mostly work all day as cybersecurity attacks do not follow follow hours. Cybersecurity is not an one time expense, organizations need skilled people and a proper up-to-date infrastructure.

> *"Tomorrow the world can change again and you'll have to start over and this costs you money as well."*

Once E1 was asked how the interviewee thinks the respondents from organizations would respond to the question what their main cybersecurity challenges related to high levels of teleworking, E1 describes this as follows. E1 believes that they would probably say the same, however expects to hear more challenges related to budget and lack of skilled people. Especially in this period with a huge shortage in the labor market.

According to E4 employees themselves often do not have the budget to fully secure their private environments as well. E4 adds that as an organization you can try to fortify your organization as much as possible, but this is very costly and again the more secure often means it is less accessible or user friendly:

> *"For example if you have a very secure VPN that would probably have a lot more lag and latency, so that would also mean slower work time for people and that is also gonna cost you."*

Furthermore, E4 builds upon the point made by E1 regarding the labor shortage. According to E4 they now have too much work to handle and there are not a lot of people in the cybersecurity field yet. Besides E4's organization, E4 describes an example of the problem with getting a CISO as an organization:

> *"Of course that needs to be filled in by a very senior individual with a lot of experience in the field, and the only way to get these people is to steal these people away from other organizations that also need them. So it is really a game of tug-of-war. So that's is really the problem right now."*

O2 experiences the shortage of skilled people hands-on. In the organization's country there are a lot of security professionals that make exploits. So there is a large pool of skilled and capable people who are making exploits that want to have remote work, but still live where there are currently living. O2 has lost somebody because O2 can not cope with the offers they are giving to O2's people at the moment. So the large demand on experienced professionals is a serious challenge. Especially with high levels of teleworking:

> *"The way that people are embracing remote working, it also means that these nomads are becoming much more accepted, that people are working outside the country, in another country far away and still do the job. That makes it a little bit more complicated for me"*

The organization of O4 is currently moving from BYOD to CYOD (Choose your own device), which will also be discussed in the next section. However, these laptops costs between 2 or 3 thousand euros and since the organization is very large, they are currently doing this department by department. This

example shows how expensive investing in cybersecurity can be for an organization. Not only expensive, but it is also the large scale that which makes this difficult. E1 for example mentions as in the past teleworking already existed, higher management would usually take the company laptop home as they are working all the time. They would get specific security awareness courses of a few hours, but suddenly you have to educate for example 10 thousand people.

O5 also makes a distinction between smaller and bigger companies:

> *"Knowledge is money. The big corporate can afford it and if you have a properly trained security officer, a really good one,you need to pay at least 100k per year. If you are a smaller company that is completely out of proportion with what you are earning as a company, so for them it is not doable, so smaller companies need standardized services which help them at a affordable price."*

However, according to O5 the security market is not there yet, those affordable services for smaller companies do not exist yet. The security services are still very expensive and as an organization you need highly skilled people to make use of these advanced tools. O5 made a similar statement to E4's statement regarding currently getting a CISO as an organization, saying that is easier to lose a security office at the moment than to hire a new one.

4.4.4. Priorities

Starting with a note to understand this sub-section in relation to the next section. The next section of this chapter will focus on the approaches taken by organizations to manage these cybersecurity challenge and go deeper into the effects of the pandemic's shock. This sub-section will only briefly discuss these.

Given that two years ago, all of the sudden a large share of the workforce had to work remote and everything had to be set up quickly. According to E1, once there is a time constraint or pressure, as an organization you are tempted to forget security only to found out a few months later that you were hacked as you forgot to configure it properly. Since this is due to the shock of the pandemic and the sudden introduction of the crisis-induced teleworking model, this problem is likely to not exist anymore since the pandemic started 2.5 years ago at the moment of writing this, or at least the effects have worn off.

However, E1 explains that they see customers that are fairly big companies that you would expect to have their security in order. They would call E1 once they have an incident and afterwards the investigation, E1 founds out that they just overlooked cybersecurity. It was not a priority for them. E1 adds that this is also related to awareness and knowledge saying that:

> *"They were not aware that cybersecurity could affect their business continuity. They were just focusing on production or other business processes, so it's just simply forgot."*

Furthermore, speaking of lack of resources. E1 explains that cybersecurity is very easy to safe money, as organizations have to invest now to prevent a potential loss of money later. At the organization of E3, they also see that organizations introduce remote access solutions that were not as configured and secure as E3 would advise. But also E3 mentions the time constraint and says that you could regard it as emergency changes that are carried out in a short period of time and afterwards you would configure them properly. However, E3 describes even after having the time constraint, security is often forgotten:

> *"Especially in the beginning when pressure is high you and your manager want a teleworking solution and you implement it, it must work and security comes after. But there is always more work to be done, so security becomes after again and at one point it is forgotten and you get hacked."*

E3 adds that security is often seen as a burden and additional costs, but an incident results in an even bigger burden and costs. This also comes down to the lack of awareness and knowledge of the management layer, given that cybersecurity requirements are not included in the whole picture. However, according to E3 a good CEO will see that business continuity is the number 1 priority for an organization.

Furthermore, looking back at the E4's statement about employees not having the budget to fully secure their private environment. E4 also believes that fully securing their home is just simply not in the employees' interest.

4.5. Managing approaches

The identified risks and challenges are closely related since some of the risks are involved in the cybersecurity challenges. So it might not be a surprise that the themes identified in the thematic analysis regarding the approaches in managing these challenges are similar as well. However, it most be noted that despite the fact that the identified cybersecurity challenges are based on the codes that were applied over multiple interviews, not all interviewees mentioned the same challenges, so some approaches do not completely match the challenge, but the same identification process has been used for the management approaches, so there is a proper fit.

4.5.1. Technology & Processes

According to E1 organizations are currently deciding what software they will use for their infrastructure. For example Microsoft Office 365, they will start doing everything with Office 365. Other applications will be blocked and not allowed to use. E1 states this is easier to manage as it solves a part of the patch management problem, since you only have one tool to patch and also on tool to explain to the employees. E1 does not see this everywhere, but they are thinking about it. However, according to what is discussed in sub-section 4.4.2, this could result in that identified cybersecurity challenge.

Regarding both the aforementioned resources and privacy challenge, E2 mentions that there are organizations allow employees to use their own device, but use an enclave which is basically a sandbox environment, so the business environment and the private environment are separated on the private device. However, this does not apply to the physical environment of the employees. E2 adds that all the mature clients of E2 have a proper device management in place and less mature clients are either in the process of establishing such system or are advised to do by E2. This has also been a requirement in the security standard ISO 27001 as teleworking is not completely new and was already covered. However, there have not been made a lot of changes or upgrades in these standards since the introduction of the crisis-induced teleworking models among a lot of organizations.

For the clients of E3, the facilitation of corporate devices was a just little investment and already had either a Citrix or cloud environment. E3 mentions a similar approach to manage the privacy challenge:

> *"I know there are solutions that you can have a sandbox environment on their private device, so you have a business layer, or sandbox, on top of their normal environment and then you wipe it and provide security controls on that environment without touching their private space."*

E3 believes that organizations are approaching the mentioned challenges in the interview mainly through technology. E3 provides several examples of the clients E3 is working with. One of the clients focused on the application of the Microsoft defender security suite which enables them to do more enhance security logging and protection. Additionally, business laptops are provided on which installation of software is not possible. Another client provided business laptops with a Citrix client and did not allow external software as well. However, E3 was provided a laptop that enables users to install software, but with a very strict security protection and detection software. So according to E3, everyone with a little bit of privacy sense would not use the device for private purposes.

The statement that there is always a balance between security and privacy is acknowledged by E4. However, according to E4 a privacy breach is allowed to some extent if it otherwise would result in corporate loss. E4 mentions the example of the take-at-home exams, some universities required students to have several cameras on to monitor the room where the student is taking the exam. This is a serious breach of privacy, but still legal as there is no alternative, a judge has to decide if it is accepted. How this actually translates to managing the challenge discussed in sub-section 4.4.1 is not clear.

Aforementioned, the organization of O4 is currently providing their employees with standard secured devices instead of them using their private devices. This allows them to have more control without crossing the privacy boundaries.

According to O5 there is the possibility to provide employees that are managing their own devices with tools like Windows Defender or FireEye, so as an organization you can make sure that they can only work from home if such tool is installed. With Windows Defender, you can not even access your account if you do not have the tool installed.

> *"So you get your goal of monitoring the device, respecting a persons privacy and not having to not managing all those laptops. Because one screw up of a system administrator*

can compromise for example a few thousand laptops."

Furthermore, regarding processes and organizations viewing cybersecurity as an hindrance. Keeping things simple for organizations results in less chance of making mistakes, which in the end helps security. O5 describes security as business enabler as O5 tries to make processes as efficient as possible, so there is a smaller chance of error and this helps the customer as well. Once that is the first step, organizations come to the discovery that there are very few additional controls needed.

4.5.2. Education of the workforce

Starting with what already has been mentioned by E1 is that organizations already had security awareness programs related to teleworking in place for higher management, but not on such large scale to educate all the employees at once. However, according to E1, teleworking is getting more mature now and companies are aware how it works and had time to properly think about it.

Responding to the 'security vs privacy' challenge discussed in the previous section, E2 believes that on of the only measures organization can take is making the employees aware of the relevant security risks. So mainly through awareness campaigns, to ensure that people are aware of the policies and through for example e-learnings or security information weeks. Repetition of these campaigns could increase the security at the employee's private environment. After being asked if E2 thinks this approach is successful, E2 responds that at the clients it is usually discussed, but can be improved. Especially the repetition of making the their employees aware. This again differs at each maturity level, immature organizations can improve a lot more compared to mature organizations. According to E2 bigger organizations usually use e-learning initiatives and make use of their governance structures and ends with the following proposal:

"So a good combination would be to have mandatory e-learnings at a certain interval, so that they are repeated and that you keep them being aware. At the same time, you use the governance structure at each department to check up on that, but also maybe give a few more departments specific requirements or courses to smaller groups".

As E3 already mentioned, most of the organizations E3 has as clients are managing the mentioned challenges through technology. However, despite E3 stating that technology helps a lot, it does not help against administrators with additional privileges, when they bypass their own policies, you as an organization would have a problem. So this is why according to E3, it is especially important that these employees are given additional attention regarding awareness. Furthermore E3 states that incident simulation exercises is a really good method to raise security awareness, especially among the managers. They will go through a scenario where for example an incident that is triggered by teleworking resulted into an ransomware attack and outage of the IT and OT environment, so productions stops as well.

There have been several statements made by some of the interviewees regarding the lack of skilled people. E4 sees that organizations are currently getting many people in the cybersecurity field and pay for upskilling as this is cheaper than waiting. Furthermore, E4 states that security training is a very large part of cybersecurity as a whole.

The organization of O1 now provide e-learnings that are mainly focused on Shadow IT and cybersecurity in the house environment. This also involves sharing and automatic forwarding to private accounts. Furthermore, they have a detection mechanism in place and are requesting the employees to stop forwarding these business e-mails to the private environment or sharing folders with external accounts. This is also a approach to increase awareness by addressing the people that are bypassing the policies. Lastly, they recently implemented a renewed phishing e-learning that is recommended once they failed the phishing test done by the organization. Looking at the identified challenges, these could be an helpful approaches managing the 'control & awareness' challenge.

Also O2 is currently putting a lot of effort in awareness sessions, phishing simulations and a lot of online training. This is similar to what O3 mentions, they started with an additional project for end-user awareness such as courses and phishing campaigns. They even developed modules in their HR system that are required to follow in order to understand and recognize cybersecurity risks.

Early on in the pandemic O4 started communication campaigns to show their employees how to send data in a controlled way to their private environment, or how they can print from the corporate environment. Additionally, they have an awareness program that is dedicated to the board and management and a dedicated version for the other employees.

4.5.3. Establishing security culture

The organization of O2 is currently working on integrating security in the organization, so that resilience is part of the whole workforce, making it part of the culture, instead of only the security team focusing on security.

> *"The same as in Y, where I was the CISO, where you have the safety culture. That is what I love about oil and gas industry. You learn safety is very important, every meeting you have the executives talk about the safety rules, it is part of the company's culture. What we are also trying to with having such a cyber resilience culture in our organization, from our CEO to our ladies at the desk that are registering the people who are entering the offices."*

Everyone in the organization has an important role to play, this is why O5 is focusing on integrating that cyber resilience into everybody's daily role. According to O5 they are able to completely manage technology, but establishing such culture takes a lot of time and repetition.

Despite a lot of interviewees mentioning that the human aspect is one of the main security challenges and it is not possible to control everything, O4 believes that the human being is also effective. O4 as the CISO of the organization together with a large group of employees are helping the organization to become aware of the risks and the measures they can take. However, instead of ensuring security by forcing and blocking certain actions, O4 tries to provide a standard and try to nudge the employees in using that. So this approach is focused on empowering and nudging the employees into a different way of working instead using restrictions. According to O4, this works best for the organization.

In sub-section 4.3.1 O5 mentioned an security incident as a result of poor cyber hygiene in combination with BYOD. However, there is more to this story:

> *"I've been in IT for 30 years I have seen 1 incident with a BYOD, that was from a colleague who let his kid play with this device. And I have seen a lot of incidents on corporate regulated devices. Why? When a strange thing happens and you are responsible for your own device, you will investigate. When a strange thing happens on a completely buttoned down device they will think "Well they know about it, they have seen it and I do not have to do anything".".*

Although it might be counter-intuitive, if you give employees these responsibilities and talk about them and challenge them, will in practice lead to less incidents.

Furthermore, the automated awareness courses do have some value, but not as much as people believe. These make people aware only for a few days until it is forgotten. What O5 believes works is both making the employees aware of the risks, controls and what you expect from them. Furthermore, discussion about why some controls are being ignored instead of sanctioning. Organizations started worrying and thinking about cybersecurity, but similar to O2, O5 states that changing a culture takes a couple of years. Most focus on technology, but without the security knowledge of the employees and the culture, the controls become less effective over time because of the challenge discussed in sub-section 4.4.2. The only way to stop this is security culture.

4.5.4. Pandemic as a priority trigger

According to E1, awareness among organizations themselves is getting better since the amount of attacks and companies getting attacked are rising every day:

> *"So imagine if you're CEO of company X and you see in the news that Company Y was hacked and their production was stopped for a whole month. Then maybe that would trigger some kind of awareness. Within company X they would think "If that company can get hacked, maybe I should check if my company can get hacked."."*

Since E1 is also asked what E1 would think organizations would say if they are asked what their challenges are. E1 believes that higher management would say that cybersecurity is their priority and they do everything they can, while lower management would say they know what to do, but they do not get the budget. Furthermore, this respondent thinks the overall quality of cybersecurity in organizations decreased due to business continuity having the number one priority, but expects it to increase again. However, although it depends on the company, E1 sees companies that were not aware of anything before, suddenly confronted it.

Furthermore, E3 sees that there is currently a lot of attention towards the subject of this research. So E3 thinks that the pandemic has triggered quite some improvements, also with software and solution providers, mainly from the better vendors like Microsoft, Google or Cisco.

Especially during and 'after' the pandemic there is an increase in understanding of cybersecurity being a very important topic within organizations, according to E4. Which E4 also believes to be due to the increase in successful ransomware attacks and media attention that also reached CEOs and management. the The years before, cybersecurity was often seen as the black sheep of the family. E4 says that all organizations now want to be really mature all of the sudden, while the work to achieve this has not been done for years.

According to O5, organizations are also starting to work together and exchange threat information in collaboration with ISACS and the National center of cybersecurity. Most companies make their security policy confidential and classified information, but with this information being confidential, you make it impossible for suppliers or other businesses you closely work with to meet this policy. As O5 made the security policy of the organization public information, smaller companies can use this as best practice. O5 adds that the controls are not public information as this makes it easier for attackers. In the past half year O5 got a few requests from other non-client companies to receive their security policy. This shows how cybersecurity is becoming a larger priority among organizations.

4.6. Sub-question Answers

The findings have been discussed in great detail which might made it difficult to see the bigger picture at this moment. Therefore, the aim of this section is to give an adequate and brief answer to the sub-questions defined in the first chapter 1.

4.6.1. Sub-question 1 - Phase and implications

The question is defined as follows:

> *"To what extent are organizations using teleworking and how did the increasing use of teleworking affect organizations?"*

Phase

Starting with the phase, before being able to discuss how increased use of teleworking is affecting organizations, the current levels of teleworking should be determined. The first thing to note is that this highly depends on the industry and it is likely that the respondents are not able to know all the organizations' teleworking statistics. This was expected and has been mentioned several times during the interviews. However, the levels of teleworking are also varying within organizations between departments. Although it was difficult for the respondent to give exact numbers, some of them were able to give an estimate like for example O4 that estimates that only around 20 % of the time employees are back in office. The goal of this part of the question is not to show the exact number, but to see if organizations are starting the process to move their workforce back to the office since organizations are not forced to keep the implemented crisis-induced teleworking model.

Only one of the interviewees believes that there currently is a shift in progress of the workforce moving back to office, especially small and medium sized companies. However, the rest of the respondents are, or see that around 50 % or more of the time employees that can be perform their tasks from home are still working remote. Furthermore, given the view of the respondents, including the view of the respondent that noticed a shift back, it is likely that organizations will not move back to pre-covid teleworking levels.

This is in line with the literature that suggests that organizations are currently using a more conventional teleworking model instead of the forced crisis induced teleworking model [37]. Also several papers discussed in the literature indicate that we will not move back to pre-pandemic teleworking levels [41].

Implications

Table 4.2 shows the identified themes and sub-themes related to this subject. More than half of the respondents mentioned implications related to the high levels of teleworking that involved the well-being of employees ranging from employees being less productive, no clear line between private life and work and a higher work pressure. Despite the aim for negative implications as these could be part of later identified challenges, a little less than half of the interviewees discussed some beneficial implications

like less travel time, being more productive and not being forced to be physically present. This also shows that there is no consensus among the interviewees regarding the relation between teleworking and productivity. Figure 2.2 also suggests that low levels of teleworking is less efficient than a mixture, while this also applies to high levels of teleworking [39].

Only 2 of the respondents reported that they did not see or experience any implications related to the high levels of teleworking. Furthermore, implication related to communication were discussed by some of the respondents , it would be harder to connect clients and both simple communication and big sessions are suggested to be harder due to these levels of teleworking. This seems to be similar to what is described in the literature study, that exchanging information can be constraint as well as the possibility that teleworking harms the well being of employees [32] [33]. In the literature study, more implications are discussed that are directly connected to security risks, these will be addressed in the next sub-question.

4.6.2. Sub-question 2 - Risks & Threats

Moving on to the second defined sub-question:

"What cybersecurity risks and threats are related to high levels of teleworking?

As shown in table 4.3 there are two themes that were identified during the thematic analysis: controlled environment and behaviour of the workforce.

Controlled environment

Starting with the 'Controlled environment'. The majority of the respondents addressed how the fact that there is less physical security in the private environment or that vulnerable IoT devices that employees have at home impose a larger security risk on the organization. Several arguments have been made by respondents explaining why there is less physical security in the private environment. For example there are no security gates, having roommates or other unauthorized people in the same room or house, this is not the case for most organizations' premises. Also vulnerable IoT devices like cheap light bulbs, keyboards or security cameras at home could be tapped into that are connected to the personal network of the employee. According to these interviewees these risks have become more significant as a result of the high levels of teleworking, which makes sense as these risks are related to the private environment that becomes part of the organizations' infrastructure. The use of vulnerable IoT devices inside the room and the high chance of unauthorized people being present has been mentioned in the literature as well [53]. Furthermore the risk of corporate managed devices being stolen is higher according to the literature, which even happened to one of the respondents [54].

Furthermore, according to almost half of the respondents high levels of teleworking make it harder to control the cyber hygiene of employees and monitor if certain security policies are being followed. Relating to the previous mentioned risks, organizations do not have the ability to check the vulnerable IoT devices or if there are unauthorized people in the room of the employee, which increases these security risks as well.

The amount of people using vulnerable third party software to exchange information and communicate increase along with the levels of teleworking. Three respondents addressed using unsecured or free software which gives third parties the right to look at the data, increased the risk of a data breach. Also three of the respondents stated that the way of file transferring and the facts that more links are being shared or the lack of physical communication with colleagues due to high levels of teleworking, resulted in more phishing attacks and the attacks being more sophisticated. Again, this risk regarding the use of external software is mentioned as well in the literature [56]. There has been made a connection between the increase in phishing and teleworking in the literature study as well. However, according to the researchers this is due to the employees being distracted at home, not that more links are being shared and the lack of physical communication led to more sophisticated and frequent attacks [52].

Since the crisis-induced teleworking model has been widely implemented among organizations, a lot of organizations let employees use their own devices. According to nearly half of the respondents, the private devices of employees are harder to manage and without proper restrictions or access management this could impose serious security risks as these devices are also used for personal purposes while not taking into account the organizations' expected cyber hygiene. Although this exact risk has been addressed in the literature, even if a proper device management system is place, there are respondents that pointed out that if organizations do not patch the software running on the devices, the software

vulnerabilities can be exploited [57]. Sometimes the patches were only made possible at the organizations' premise for example or devices with multiple tools that required patches, these devices might not be secured on time. This is a larger risk since a large share of the workforce is working remote.

Lastly, six of the respondents agree that the high levels of teleworking put more pressure on access management. Not knowing which devices are connected and how these are connected is a serious security risk. This also relates to the use of private and unmanaged devices that are able to connect to the corporate network. Having a VPN in place seems safe at first glance, but if an unsecured device is able to access the network through the VPN, this is still a risk. Also other bad practices have been named like, poor password policy or no MFA.

Behaviour of the workforce

A lot of the increased risks have already been discussed that these can be linked to this topic as well. The majority of the respondents address that employees not being aware of some of the aforementioned risks related to remote working and how to deal with these risks only amplifies these risks. Some examples of situations that occur once employees lack certain knowledge and awareness like: not being aware that free software imposes a security risk or having a lot of vulnerable IoT devices in the private environment. Since a large share of the workforce is working from home, more security depends on the awareness and knowledge of the employees.

According to several respondents employees are bypassing security policies out of convenience, for example if the device is too restricted and they want to use other (vulnerable) software or send information to their private environment to work from there. Without the necessary knowledge and awareness these security policies are only seen as a obstacle. Which is in line what has been found in the literature, that employees will try to change security settings once certain websites are blocked [35].

Besides the absence of physical security and to a certain level control as well, there is also no more corrective behaviour according to three of the respondents. At the office colleagues would correct each other once not complying to the security policies, while at home this corrective behaviour is not present and not complying becomes more acceptable.

4.6.3. Sub-question 3 - Challenges

The third sub-question focuses on the main cybersecurity challenges and is defined as follows:

> *"What are the main cybersecurity challenges that are related to the high levels of teleworking?"*

Although the literature study supported the results derived from the thematic analysis regarding the risks related to the high levels of teleworking, the conducted literature study did not succeed in providing enough information to answer this question as this is part of the identified knowledge gap.

Security vs Privacy

Firstly, according to the majority of the respondents, due to these high levels of teleworking organizations' security shifted from the office to the personal space. As this personal space became part of the organizations' infrastructure, organizations want to guarantee the same level of security as at the office, but organizations do have to comply with privacy & ethics regulations which limits organizations in implementing certain controls, this makes achieving the desired security level very challenging.

Control & Awareness

The second challenge relates to the risk regarding employees bypassing policies that has been discussed in the answer of the second sub-question. Six of the respondents emphasized the importance of the security awareness and how this one of the main challenges for organizations, since a lot of organizations are mainly focusing on technology. If an organization imposes a lot of controls and these are the risks these are managing are not understood by the employees, employees will find new solutions and bypass these controls, which in the end harms the organizations level of security.

Lack of resources

The third challenge concerns organizations' lack of resources. Although cybersecurity can be a huge monetary expense given that it requires constant attention and for example providing the whole organization with a secure setup and managed devices, seven of the respondents that addressed lack of

resources as on the main challenges focused more on the lack of resources in the form of skilled people. The increase among organizations in security awareness and the acknowledgement of cybersecurity's importance, resulted in a higher demand which is very challenging given the already significant shortage in the labour market. Furthermore, especially for small less mature organizations as they need affordable standardized services, but these are not yet widely available. Additionally, employees probably do not have the budget to completely secure their private environments as well.

Priorities

Lastly, three of the four consultants addressed the priorities of organization as one of the main challenges as well. Despite the time constraint and the shock of the pandemic that forced organizations to make some decisions to guarantee business continuity that not always involved security, currently 2.5 years after the start of the pandemic this challenge has not been solved. According to these consultants cybersecurity is still often forgotten by organizations and often see it as a burden, regardless of the attention it got the last years. Furthermore, this also applies to employees, that do not have the interest to secure their private environment to the same extent as the organization secures its environment.

4.6.4. Sub-question 4 - Approaches

The fourth sub-question that goes into organizations' approaches to manage these identified challenges.

"How are organizations approaching these identified challenges?"

The literature study provided some security measures and practices to manage a part of the risks identified in sub-question 2. However, it is not able to describe the current approaches of organizations to solve these identified challenges in the last sub-question. Nevertheless, the literature is able to complement these approaches since part of the approaches of organizations involve earlier mentioned practices.

Technology & Processes

Several respondents have stated that organizations are currently deciding which software they want to build their infrastructure on or have chosen already. This results in lowering the patch management risk, but might result the discussed challenge 'control & awareness' if other software is blocked. All except one of the respondents currently have managed corporate devices' and one of them is moving from BYOD to CYOD, while it is noted that less mature clients do not have proper device management systems in place.

Given the 'lack of resources' and 'security vs privacy' challenge, there are organizations that allow their employees to use their own device, but they have to use an enclave which separates the business and private environment on the personal device. This enable organizations to secure private devices, without breaching their privacy or providing managed devices. However, securing physical private environment remains an unsolved part of the challenge. Furthermore, currently more tools like Windows Defender or FireEye are provided and required by organizations, which enables them to monitor the device, respect the employee's privacy and do not have to manage all the devices.

The updated NIST teleworking standards discussed in the literature study outlined several measures [75]. One of these is 'Requiring multi-factor authentication for enterprise access', although not having MFA enabled has been mentioned as risk, this does not seem to be part of the main identified challenges. Furthermore recommendations include, using validated encryption technologies, ensuring that the remote access servers are secured and patched, and secure all types of devices. These standards are certainly helpful for organizations and have been discussed at length, but these points do not provide a clear approach to manage the identified challenges. Especially given the 'control & awareness' challenge, that could even become more prominent after implementing all these measures.

Education of the workforce

The education of the employees is mentioned as one of the most important approaches to manage the identified challenges. This also applies to what is found in the literature, that CISOs believe educating employees is seen as on of the most important security measures [77]. This makes sense given the characteristics of the challenges and technology does not seem to be the aspect that makes these challenges challenging. Although technology can do a lot, organizations tend to stop there, which is also one of the reasons these challenges exist. However, regarding the identified challenges, according

to some of the respondents organizations are currently improving the awareness & knowledge of the workforce by repeating awareness campaigns, security information weeks, e-learnings and simulation exercises. Where at some of these organizations these are specifically focused on teleworking security risks as well. Furthermore organizations have detection mechanisms in place that for example request to comply to certain policies once an employee fails to comply to this policy or once an employee fails a phishing tests they will be automatically recommend a phishing e-learning. This could be a very helpful approach to manage the 'security vs privacy' challenge, or at least decrease its importance as employees are more aware. This approach is expected to be the most effective countering the 'control & awareness' challenge, since controls are more effective with more awareness, while as discussed, implementing more controls without proper security awareness might even be counterproductive. Furthermore an increase in awareness of the workforce and management might start a shift in priorities as well, which addresses the 'priorities' challenge. Given the lack of skilled people in the field, organizations are currently upskilling as many people as possible, instead of waiting for the supply to grow.

Establishing security culture

Another approach that has been discussed is the establishment of a security culture that involves more than just proper technology, processes and awareness. As mentioned in the challenges organizations can never control everything, even through education it is not possible to achieve the desired security level concerning the human aspect of the challenges. Organizations are making cyber resilience part of the organizations' culture, so to involve security into the daily role of the whole workforce. Not approaching the given challenges with solely technology, processes and education, but a combination and giving employees responsibilities and nudging them. So not using a lot of restrictions to force the employees that can result in the 'control & awareness' challenge, but empowering them and have discussions about their responsibilities. Despite sounding counter-intuitive, this can be an effective approach to manage challenges as without such culture, education is forgotten and controls become less effective over time. However, establishing such culture can take multiple years.

Another interesting point from the literature study is the recommendation to develop and enforce a telework security policy, given what has been discussed in this and the 'control & awareness' section, enforcement might not always be the most effective approach [76].

Pandemic as a priority trigger

Although this is not particularly a managing approach, since one of the identified challenges concerns organizations' and employees' priorities, this should be discussed here. The large increase in cyberattacks due to the implementation of crisis-induced teleworking models resulted in a lot of media attention that also reached organizations. Organizations have recently become more aware of the importance of cybersecurity and want to become mature as well while the work has not been done for years since this was not a priority. However, it seems that the pandemic resulted in cybersecurity being a larger priority among organizations. The literature does back this statement, while there is also research that addresses that there is a difference between organization stating that cybersecurity is their priority and acting upon it [15] [21].

Furthermore, organizations also started exchanging information regarding threat information. Although still a large share of the companies keep their security policy confidential, there are organizations that make this public information so these can be discussed. Also smaller companies can use these security policies as best practice, as they often do not have the resources, mature organizations have, like discussed in the challenges. This also shows how over the past few years cybersecurity is becoming a larger priority.

4.6.5. Sub-question 5 - Consultants vs. Organizations

The last sub-question is defined as follows:

> *"How do the challenges and approaches stated by the organizations differ from those stated by the consultants?""*

Although one might expect to see significant differences in mentioned challenges since they both have different interests and perspectives. However, they were very similar except from one of the challenges that has only been addressed by the consultants and not by the organizations. This is the 'priorities' challenge, this actually was already expected by one of the respondents that organizations would not

disclose that cybersecurity is not one of their main priorities. Nevertheless consultants do address the lack of resources as on the of the main challenges for organizations, which is closely connected to the challenge regarding priorities. An consultant can comfortably state that organizations are not prioritizing cybersecurity enough, while it can be that organizations are in fact prioritizing cybersecurity more, but are not able to reach the desired level due to lack of skilled people or monetary resources. Or that the efforts made by organizations are not visible for the consultants yet.

Looking at the approaches there is a balanced mixture of both consultants and organizations addressing the approaches taken to manage the identified challenges. At least for two of the identified approaches. Specifically establishing a security culture has not been addressed by any of the consultants. Furthermore, again organizations also do not state that their cybersecurity is now a more higher priority for them. This makes sense, since they also did not mention this to be a challenge in the first place. However, they make various statements that show that security is an important priority in their organization.

This answer highly depends on the organizations and the research design, which will be discussed in more detail in chapter 5.

5

Discussion

This chapter will focus specifically on the differences between the consultants and organizations, the implications and the limitations of this study will be addressed in this chapter, ending with recommendations for future research.

5.1. Consultants vs. organizations

Given the goal of this research to gain a deeper understanding of organizations cybersecurity challenges and approaches, the decision has been made to interview both consultants in the cybersecurity field and individuals that are responsible for their organizations' cybersecurity. This decision was supported by the idea that these different actors would have a different perspective on these challenges given their role and interests. The reason for the lack of difference between the identified phase of teleworking and risks between these two actor categories, can be that there is no relation between the perspective and these factors. The share of the workforce that is currently working remote is rather objective and it was not expected to identify a clear difference regarding this aspect. However, the findings also show the absence of a clear difference between the consultants' and organizations' identified security risks. This can be due to the fact that in the process of conducting the interviews, data from earlier interviews has been used during the later interviews to start a discussion. A respondent could have confirmed and elaborated on this risk that was addressed in an earlier interview, while this risk might not have been addressed without the use of an earlier interview. Nevertheless, all respondents had the ability to disagree with the presented statements, which also happened. For example in the interview with O4 regarding physical security of the private environment, O4 mentioned that at home there is also less risk since it is a small environment or O3 not being concerned about roommates in the private environment.

During the identification of the security challenges, it was expected to find a distinction between the two actors, given the different perspectives and interests. One of the identified challenges has only been addressed by the consultants and not by the organization. There seems to be a logical explanation for this difference. The concerning challenge is 'priorities', according to some consultants, organizations still often forget cybersecurity or see it as a burden. As an expert that supports organizations managing their cybersecurity with their priority to help organizations to achieve a certain level of security, they are often able to make an assessment of their security management. One can understand that individuals who are responsible for the organizations' cybersecurity would not address specifically their priority to be a challenge for the organization. Of course it would have been possible that the respondents stated that other departments or for example the CEO is not prioritizing cybersecurity. Although this might even be the case, it is not hard to imagine that disclosing this information in a recorded interview is not preferred.

Furthermore, it is also possible that organizations are prioritizing cybersecurity, but are not able to translate this in practice due to the other discussed challenge 'lack of resources'. The 'lack of resource' might be organizations' reason for the lack of security, while consultants only see that they have not done enough and assume that the organizations in question did not prioritize cybersecurity. It has been discussed that the consultants that are interviewed all support their clients' cybersecurity in various ways. So these clients already have support to a certain extent and the resources to use the services

that the consultants provide. However, one can assume that especially smaller organizations do not have the resources to use these consultants' services while in the meantime prioritizing and improving their cybersecurity, but can not reach their desired level due to the lack of resources, which might in the consultants view be a case of 'not prioritizing'.

One can say that organizations did have time to properly adjust to a crisis-induced teleworking model, but for example O4 just started this year moving to CYOD instead of BYOD and since they are a large organization they are doing this department by department. So it can take a significant amount of time to roll out changes in the infrastructure. This could also result in organizations putting in the effort to manage the security challenges, but the results are not visible to the consultants yet. This lag might make consultants believe that organizations are forgetting security, while it just takes time before consultants see this progress.

There is also another challenge that shows how the security of an organizations also depends on other processes and departments. Given the 'Privacy vs. Security' challenge, one of the organizations O1 stated that in fact the security team want to implement a certain measure, but they have to deal with the opinion of the Human Resources department as well. Also O3 mentions that they have developed modules in their HR system, which shows that there are other departments in organizations that can limit the cybersecurity team in their actions. Such limitations have not been addressed by the consultants, which might suggests that consultants do not take this into account.

Given the identified approaches, another interesting distinction between these two actors have been found, the establishment of a security culture. In contrast to the previous finding, this has only been addressed by the organizations. Although this identified approach contains aspects of the other identified approaches that have been addressed by the consultants, specifically involving security into the daily role of the complete workforce and nudging instead of forcing has not been mentioned by the consultants. A reason for this can be for example that this is outside of the scope of the consultants' interests. Organizations state that this can take years, consultants might only focus on a more specific and short to medium term approach for organizations.

Despite consultants addressing that priorities is one of the main security challenges, E3 also addresses that a good CEO's number one priority is business continuity. So organizations that were already set up for teleworking, this rapidly increasing use of teleworking went very smooth from a continuity perspective like O2 specifically addressed. After business continuity is out of danger, organizations can focus on adjusting their cybersecurity management to the new situation. However, organizations that had a hard time adjusting to these changes, it could be that business continuity was only ensured after a longer period and just started prioritizing security. Again, O3 mentioned that they started this year with switching to a new device management system, this shows that security is not forgotten, but this current effort made by organizations might not be seen by consultants yet. This might also apply to the approach 'Establishing security culture', this requires a lot of time and resources, but might not pay off immediately and take some time before the results are visible to consultants.

So regarding the conflicting perspectives on cybersecurity being a priority or at least given a high enough priority. Both literature and the interviews show that there cybersecurity is receiving more attention and a higher priority [15]. However, at the same time literature and the consultants indicate that this is still a challenge, with valid arguments [21]. Given the interests of the consultants, they would probably not be very eager to conclude that cybersecurity should not be higher priority. While organizations do not have the ability to allocate all their resources to cybersecurity and make it their number one priority, this simply is not feasible and would not make it a viable organization. Furthermore, consultants might not be able to be aware of the time it takes to adjust to an environment that changed tremendously and took a heavy toll on resources. Also, the efforts made by to organizations to improve their cybersecurity might be there, while this investment takes time to show. Moreover, it is also possible that that despite organizations efforts made, cybersecurity consultants will always address cybersecurity as not being prioritized enough.

5.2. Implications

This study reveals and provides an understanding of the challenges related to high levels of teleworking of organizations and their approaches to manage these challenges. Aforementioned, despite the already existing literature regarding the related risks and even practices to manage these risks [75] [76] [77]. This study took place in a period that significantly differs from the period other literature is published.

The results show a shift to a more conventional teleworking model has only been in progress for a couple of months and organizations now had the time to adjust to the changed environment..

Before conducting the thematic analysis using all the interviews and identifying the current challenges and approaches, the need and implications of this study already became clear. The use of the semi-structured interviewing method allowed discussions which not only resulted in interesting findings for this study, but for the respondents as well. Several respondents stated that the topics addressed in the interviews brought new insights that they will certainly use in the upcoming sessions within the organizations. This was in particular the case for the respondents that were interviewed after a few interviews, since data from these earlier interviews was used. So to a certain extent, at that moment, this study already proved its societal relevance.

During the interviews it has been addressed that the maturity of an organization is an important factor in relation to cybersecurity's importance. Smaller organizations might have other risks that are more endangering to the business than cybersecurity risks, which explains not having cybersecurity as a high priority. Furthermore, the lack of resources has also been identified as an challenge, which would also especially apply to smaller organizations. O5 addressed that more organizations are sharing their security policy with other organizations, which can be considered a win-win situation. Smaller organizations that do not have the priority and resources to properly secure their organization can use this as best practice, while the organizations that share this information benefit from the improved security of these smaller organizations, since these are also part of the supply chain and impose a risk if they do not proper cybersecurity. To be clear, this research shows in no way how organizations should manage these identified challenges. However, the findings of this research can support organizations by helping them understand what the main cybersecurity challenges related to high levels of teleworking are and how organizations are approaching these. As mentioned in the introduction, not only organizations benefit from improved cybersecurity, society as a whole benefits from secure organizations as for example data breaches, financial losses or outage of critical infrastructure is not in the interest of most civilians.

The goal of this research regarding scientific relevance has been discussed in the introduction: creating an overview and understanding of the main security challenges related to high level of teleworking and the approaches taken by organizations to manage these challenges. As mentioned throughout this report, the implications and the security risks and threats identified using the thematic analysis are not an significant addition to the body of literature. Nevertheless, this was not the goal of this research, the security challenges and approaches of organizations are the main focus of this study. The identified challenges show how organizations perceived difficulties in responding to security risks that are related to the increasing use of teleworking and the approaches show how organizations are handling these challenges. This is knowledge that is not yet available in the current body of literature. These challenges also reveal why improving security or managing risks and threats related to the increase use of teleworking is not always possible. For example given the 'security vs. privacy' challenge, which is a security challenge in general. However, the increase use in teleworking resulted in privacy becoming a more important part of the equation since a large share of employees moved to their private homes instead of the more 'public' office. This limits organizations in improving security in various ways, for example not being able to monitor and secure their employees private environments. Each of the four challenge show different kind of difficulties perceived by organizations while improving security and manage the identified risks. The discussed approaches are responses to these challenges. Since the challenges are not found in the literature, the described responses to these challenges are definitely an addition to the body of literature as well. Aforementioned, the literature study does provide knowledge regarding cybersecurity practices specifically for teleworking related security risks and threats. There are definitely similarities between the discussed approaches and these practices like the education of the workforce. However, they are not directly linked to the identified challenges and are more general. Some of the practices outlined in the updated NIST framework standards are: requiring MFA, securing all types of teleworking devices or secure and patch remote access servers. Despite being useful practices to improve cybersecurity, they do not particularly focus on the identified challenges such as 'priorities' or 'control & awareness'. Furthermore, literature provides these practices as measures organizations should take, while this study shows what organizations currently are doing to manage these challenges. So without focusing on what organizations should do, this paper provides an in-dept understanding of organizations' security challenges related to the high levels of teleworking and how organizations respond to these challenges.

5.3. Limitations

Unfortunately, the decision to maintain a broad scope for this study resulted in certain limitations that should be addressed.

Starting with the fact that this study focused on organizations in general. Although the main focus of the research is high levels of teleworking, which excludes organizations that do not use a teleworking model since physical presence is required. However, as already mentioned in this chapter, maturity is an important factor as well as the industry the organization is operating in. For example E2 pointed out that public organizations have more strict requirements. Or E4 stating that the main risks also depends on the organization handling sensitive data and that smaller companies tend to move their workforce back to office. Furthermore, the security challenges of organizations that already had a teleworking model in place before the start of the pandemic are probably less severe or these organizations were able to manage these challenges to a certain extent that are still of great importance for other organizations that are less mature. It seems that mature organizations are in a better position than less mature organizations, given that they probably have more resources and for example already a proper device management system in place. However, O5 disagrees saying that some very mature organizations have a real limited and almost 'stupid' view on security. Additionally, the organizations' location is able to affect the challenges and approaches. Although several respondents work with international clients and were able to provide a general view, E2 mentioned for example that Nordic countries moved their workforce back relatively fast. Or O2 that lives in a certain country in America stated that privacy is not perceived as important as it is in Europe. So regulation and culture of the country the organization is based is able to make a serious difference.

It is clear that characteristics of organizations play a significant role in relation to their cybersecurity challenges and approaches. Although consultants were able to provide a more general view as they have various types of clients in different industries and countries, they are likely to be larger organizations, since small organizations do not have the resources to use these services that they provide. Additionally, three of the five respondents are CISOs, while not all organizations have the role of a CISOs. So all the provided perspectives originate from individuals work in a large organization or have large organizations as clients. Given what is discussed in sub-section 4.1.2, the respondents from organizations can be considered large. Which is also a starting point for future research that will be discussed in the upcoming section. This is important to note, since the perspectives from smaller organizations might significantly differ from the current results. All participants were able to name risks and challenges related associated with the increasing use of teleworking. However, it is more likely that if individuals from smaller organizations were interviewed that they would not always be aware of all these risks, since they not always have a role that is solely responsible for cybersecurity. This could have possibly led to the identification of a separate challenge, organizations not always being aware of the risks and threats related to high levels of teleworking. Awareness is already part of one of the identified challenges. However, this does mainly concern the awareness of employees given the 'control & awareness' challenge, not particularly the awareness of high level managers. So not including small organizations potentially changed the outcome of this research.

This research took place in a period where the increase use of teleworking was prominently visible among organizations. However, there are some flaws in this research that might have resulted in results that are not up to date. Since a few months most organizations are allowed to let their whole workforce return to the office. However, organizations do not seem to move completely back to the office. Given the characteristics of the teleworking models discussed in the literature study and information gathered from the interviews, it can be argued that most organizations are shifting to the use of the conventional teleworking model, the increased risks have been known and they had between 2-3 years to properly adapt and organize, so the shock of the pandemic has worn off. Although the interviews did involve discussions about the current situation, this 'post-pandemic' situation has not been the main focus of this research. As well as the recent change in the environment caused by the restrictions being dropped and enabling organizations to decrease the use of teleworking. Despite the results suggesting that there there currently is a shift the widely used crisis-induced teleworking model to the conventional teleworking model, how this change affected the challenges and approaches has not been researched. So there is a possibility this specific shift does have an impact on these challenges and approaches, but the interviewees were not specifically asked about the challenges since this shift, only the relation to the high levels of teleworking.

Another limitation of this research is the methodology. Although using data from previous interviews

led to interesting findings and discussions that were helpful and add value to the quality of this research, there is also a downside. It is possible that the outcome would be different if the order of the interviews is changed since this would result in different data to start with. As shown in tables 3.1 and 3.2, the first interviewees were consultants, this could have affected the data from the other interviews. Also, as this research has been conducted by only one researcher, so the performed thematic analysis depended on the the judgement and interpretation of one researcher. This could have affected the used quotes and the final identified themes which is a risk to the validity of the analysis.

5.4. Future research

Building on the identified limitations of this study, a similar research could be conducted focusing on less mature organizations or organizations in a specific industry since this could lead to a different challenges and approaches. Furthermore, since organizations are currently shifting from the crisis-induced teleworking models to conventional teleworking models, a similar study can be done after a certain period of time. The last few years with the pandemic shows how much an environment can change, so it would be interesting to see if these cybersecurity challenges and approaches are similar in the future and identify possible developments. It could for example be that, against expectations, after a few years the majority of the workforce moved back to the office or that less mature organizations were able to properly manage the identified challenges.

As mentioned in sub-section 4.3.2, it is possible that the identified implications of high levels of teleworking are related to the incentives of employees to bypass security policies. If it is more difficult to communicate through secure channels, employees might feel the need to bypass these secure channels. Also, higher work pressure is mentioned, combined with too many controls and restrictions that make it harder to complete daily tasks, it can also be an incentive to bypass security policies. Although this has not been studied nor discussed, this might be an interesting idea for future research to study this relationship.

Another possible future research can focus on one specific related challenge. For example the 'security vs privacy' and instead of using the consultants or high level roles in organizations as the main data source, focusing on how employees perceive this challenge. Or the 'control & awareness' challenge, off the record one of the respondents mentioned that there are large organizations using psychologists to help them understand why employees are bypassing controls. So a future study could research the employees motives to comply or not comply to certain security controls.

5.5. Link to the program

The central focus of the Engineering and Policy Analysis program is on analyzing and solving complex problems that involve several parties with conflicting interests. These complex problems require solutions that not only solve the technological aspect, but address the societal and political aspects as well. Cybersecurity is one of the grand challenge identified by the program [92]. This study aimed to inform decision-makers by providing them the understanding of the identified challenges and approaches which can be helpful when managing or identifying their own cybersecurity challenges. As discussed throughout the report, lack of resources can be an serious challenges, mainly for smaller organizations. So this provided knowledge can be very helpful for certain decision makers, since it shows how other large organizations are currently managing their security challenges related to the increase use of teleworking. Furthermore, this research contributes to the body of research and can be used by other researchers as discussed in the previous section.

6

Conclusion

The aim of this thesis is not only to gain a deeper understanding of the current main cybersecurity challenges organizations are facing that are related to the high levels of teleworking, but to understand how organizations are approaching these identified challenges as well. Five different research sub-questions have already been answered in section 4.6. This chapter gives the concluding remarks of this research and the answers of the sub-questions will be used to answer the following main research question:

> *"How did the increasing use of teleworking affect organizations' approaches to managing cybersecurity challenges?"*

Starting with the current levels of teleworking, the measures taken to reduce the spread of COVID-19, resulted in organizations implementing a variation of a crisis-induced teleworking model. The majority of the interviewees currently estimate the teleworking levels to be at 50 % or higher. So the volume and frequency of employees working remote are relatively high and are expected to stay at these levels.

Moving on to the cybersecurity challenges that are associated with these levels. There is already a significant body of literature devoted to the security risks and threats of teleworking, in relation to the pandemic, but also from before the pandemic. The pandemic that pushed these teleworking levels to extreme heights did not introduce any completely new risks and threats. However, these risks rose along with these levels and so these require more attention.

This study used thematic analysis to identify the following four different cybersecurity challenges in the interviews that are related to the high levels of teleworking that organizations are currently facing in this continuously changing environment:

- Security vs. Privacy has always been a challenge for organizations. However, as individuals' private environment is now part of the corporate infrastructure they want to maintain the same level of security as at the organizations' premise. Accomplishing this without invading employees' privacy is still a significant challenge at this point in time.

- Control & Awareness is the second challenge that relates to the risk of employees bypassing security measures. If an organization imposes a lot of controls to manage certain risks, employees can experience these controls as a burden. Once these employees are not aware of the risks the organization is trying to manage, employees will get creative, find new solutions and bypass these controls, which in the end harms the organization's security. So introducing such measures without considering awareness can even be counterproductive.

- Lack of resources is currently a serious concern for especially for small and medium sized organizations. The increase among organizations in security awareness and the acknowledgement of cybersecuritys importance, resulted in a higher demand of skilled individuals which is very challenging given the already significant shortage in the labour market. Furthermore, organizations want their employees to secure their private environment, but do lack the resources as well.

- Priorities are according to the organizations not part of their main security challenges. However, consultants disagree and state that cybersecurity is often still seen as a burden and neglected, regardless of the increase in cybersecurity attention and the increased risks related to high levels of teleworking. Again, organizations' security currently depends more on the workforce due to the increased use of teleworking and they neither have security as their number one priority.

Proceeding with the following identified approaches used by organizations to manage these current challenges:

- Technology & Processes are often chosen first by organizations to approach their cybersecurity risks. More mature organizations currently have a device management system in place and deciding on what software they want to build their infrastructure. Although this enhances overall cybersecurity, given the 'control & awareness' challenge, more technical controls results in employees bypassing these controls which can even decreases security. So there is a balance that should be considered, no technical controls will harm organizations' security, as well as too many without considering other factors like awareness of the employees.

  There are organizations that allow their employees to use their own devices with the condition that they use an enclave that separates the corporate and private environment on the device. Without invading the privacy of their employees and provide managed devices that require more resources, organizations can to some extent secure the private environment. However the private physical environment remains untouched by the organizations. Moreover, more organizations provide their employees endpoint security tools and require employees to use them, which also enables organizations to secure the device, while respecting their privacy.

- Education of the workforce is deemed one of the most successful approaches to manage the identified challenges. Especially since organizations have a limited ability to technically securing the private environment and given the 'control & awareness' challenge, raising awareness can be done by educating. Organizations are currently improving the awareness and knowledge of the workforce by repeating awareness campaigns, security information weeks, e-learnings and simulation exercises. Some of these are specifically focused on the cybersecurity risks of teleworking. Furthermore, there are organizations that have detection systems in place to give additional educational attention to employees that do not comply with the security policies. Furthermore an increase in awareness of the workforce and management can also support the prioritizing of cybersecurity. Given the lack of skilled people in the field, organizations are currently focusing on upskilling a significant amount of individuals.

- Establishing security culture is an approach that concerns the assumption that it is not possible to reach the desired level of security through only technology, processes, knowledge and awareness. Organizations start involving cybersecurity into the daily roles over the whole workforce. Without forcing and too many restrictions, but by giving employees responsibilities and nudging them by discussion. This counter-intuitive approach that takes years to achieve can be an effective approach, as without such culture, education is forgotten and controls become less effective over time. However, it is in conflict with is found in literature that organizations should enforce their security policy, although it is not clear how 'forcing' enforcement is.

- Pandemic as a priority trigger is not as a specific approach to manage the challenges as the other three. However, since one of the challenges is concerning the priorities, it is still considered relevant. The increase in cyberattacks due to the pandemic resulted in cybersecurity receiving a lot of attention among organizations. Organizations want to become more mature, while over the past years it lacked the effort. However, organizations are currently giving cybersecurity a higher priority. Organizations started exchanging threat information with other organizations. A large share of organizations still keep their security policy confidential, while the amount that make it public information is rising. Less mature companies that do not have the resources or the knowledge can use this as best practice, while the organizations that share this information benefit from others developed security as well since they are also often part of the supply chain.

7

Appendices

7.1. Appendix A: Interview protocols

Table 7.1: Interview Protocol Consultants

Introductory questions
- What is your current role and responsibility at your current organizations?
- When did you start your career at this organizations? Did you have any prior relevant experience?
- In which industries are the clients you have been working with?
Teleworking
- To what extent are and were your clients subject to high levels of teleworking?
- How are your clients affected by the high levels of teleworking?
Challenges
- What are the main cybersecurity risks and threats of your clients that are associated with the high levels of teleworking?
- What are a few main cybersecurity challenges your clients are currently facing related to the high levels of teleworking?
- (Possible question to aim for the preferred type of answers) According to literature these main challenges are the result of the high levels of teleworking, do you recognize these at your clients?
Approach
- How are organizations approaching these main challenges?
- Did the high levels of teleworking affect the advice you give clients related to their cybersecurity management approach?
- How do you see these challenges being dealt with in the future?

Table 7.2: Interview Protocol Organizations

Introductory questions
- What is your current role and responsibility at your current organizations? And could you give some characteristics of the company?
- When did you start your career at this organizations? Did you have any prior relevant experience?
Teleworking
- To what extent is and was your company subject to high levels of teleworking?
- How have the high levels of teleworking affected your organization?
Challenges
- What are the main cybersecurity risks and threats of your organization that are associated with the high levels of teleworking?
- What are a few main cybersecurity challenges you are currently facing related to the high levels of teleworking?
- (Possible question to aim for the prefered type of answers) According to certain cybersecurity Consultants these main challenges are the result of the high levels of teleworking, do you recognize these at your organization?
Approach
- How are you approaching these main challenges?
- How do you see these challenges in the future and how will they being dealt with in the future?
- Consultants mention the following main challenges as being the result of the high levels of teleworking, why do you think they different or similar?

Bibliography

[1] Gartner. (2021, April 7). Gartner Forecasts Worldwide IT Spending to Reach 4 Trillion in 2021 [Press release]. https://www.gartner.com/en/newsroom/press-releases/2021-04-07-gartner-forecasts-worldwide-it-spending-to-reach-4-trillion-in-2021

[2] International Monetary Fund. (2021, July). Fault lines widen in the global recovery. IMF. https://www.imf.org/en/Publications/WEO/Issues/2021/07/27/world-economic-outlook-update-july-2021#Overview

[3] Racz, K. (2021, November 11). New Hybrid Work Statistics: The 5th Annual State of Remote Work Report. Owl Labs. Retrieved March 15, 2022, from https://resources.owllabs.com/blog/state-of-remote-work-report-2021

[4] Digital McKinsey and Global Risk Practice. (2020, June). Cybersecurity in a Digital Era. McKinsey and Company. https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/cybersecurity%20in%20a%20digital%20era/cybersecurity%20in%20a%20digital%20era.pdf

[5] PT Security. (2021, July). Cybersecurity Threatscape. https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity_threats_2021-Q1-eng.pdf

[6] IBM. (2021, July). Cost of a data breach report 2021. https://www.ibm.com/downloads/cas/OJDVQGRY

[7] Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2), 146-157. doi:10.3934/ELECTRENG.2021008

[8] Mihailovi, A., Cerovi Smolovi, J., Radevi, I., Raovi, N., & Martinovi, N. (2021). COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications. Sustainability, 13(12), 6750.

[9] Turner, C., Turner, C. B., & Shen, Y. (2020). Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior. Journal of Advanced Research in Social Sciences, 3(2), 22-30.

[10] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 1-20.'

[11] Contreras, F., Baykal, E., & Abid, G. (2020). E-leadership and teleworking in times of COVID-19 and beyond: what we know and where do we go. Frontiers in Psychology, 11, 3484.

[12] Toleikien, R., Rybnikova, I., & Jukneviien, V. (2020). Whether and how does the Crisis-Induced Situation Change e-Leadership in the Public Sector? Evidence from Lithuanian Public Administration. Transylvanian Review of Administrative Sciences, 16(SI), 149-166.

[13] EY. (2021, July). Cybersecurity: How do you rise above the waves of a perfect storm? https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

[14] PwC. (2022, February). 2022 Global Digital Trust Insights with reflections from The Netherlands. https://www.pwc.nl/nl/actueel-en-publicaties/diensten-en-sectoren/technologie/bestuurders-niet-betrokken-cybersecurity/download-global-digital-trust-insights.html

[15] PwC. (2022a, January). Reimagining the outcomes that matter. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html

[16] Gompert, D. C., & Libicki, M. (2021). Towards a Quantum Internet: Post-pandemic Cyber Security in a Post-digital World. Survival, 63(1), 113-124

[17] Eijkelenboom E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law & Security Review, 40, 105513

[18] Tokarchuk, O., Gabriele, R., & Neglia, G. (2021). Teleworking during the Covid-19 crisis in Italy: Evidence and tentative interpretations. Sustainability, 13(4), 2147.

[19] Mannebäck, E., & Padyab, A. (2021). Challenges of Managing Information Security during the Pandemic. Challenges, 12(2), 30.

[20] Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. john wiley & sons.

[21] Maurer, C., Kim, K., Kim, D., & Kappelman, L. A. (2021). Cybersecurity: is it worse than we think?. Communications of the ACM, 64(2), 28-30.

[22] Hennink, M., & Kaiser, B. N. (2021). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. Social Science & Medicine, 114523.

[23] Cambridge Dictionary. (2022, May 11). teleworking definition: 1. the activity of working at home, while communicating with your office by phone or email, or. . .. Learn more. Retrieved May 12, 2022, from https://dictionary.cambridge.org/dictionary/english/teleworking

[24] Gan, V. (2015, December 1). Bloomberg - Are you a robot? Bloomberg. Retrieved May 12, 2022, from https://www.bloomberg.com/tosv2.html?vid=&uuid=f8f5bfb7-d1d3-11ec-be0f-564a51594874 &url=L25ld3MvYXJ0aWNsZXMvMjAxNS0xMi0wMS93aGF0LXRlbGVjb21tdXRpbmctbG9va2VkLWxpa2UtaW4tMTk3Mw==

[25] Global Workplace Analytics. (2022, January 18). Latest Work-at-Home/Telecommuting/Remote Work Statistics. Retrieved May 12, 2022, from https://globalworkplaceanalytics.com/telecommuting-statistics

[26] Kowalski, K. & Swanson, J. (2005). Critical success factors in developing teleworking pro-grams. Benchmarking: An International Journal.

[27] Harris, L. (2003). Homebased teleworking and the employment relationship: Managerial challenges and dilemmas. Personnel Review, Vol. 32 No. 4, pp. 422-437.

[28] European Union. (2020). Telework in the EU before and after the COVID-19: where we were, where we head to. https://joint-research-centre.ec.europa.eu/system/files/2021-06/jrc120945_policy_brief_-_covid_and_telework_final.pdf

[29] Gartner. (2020, March 19). Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus. Retrieved May 13, 2022, from https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88–of-organizations-have-e.

[30] European Commission. (2021, April). Living, working and COVID-19 (Update April 2021): Mental health and trust decline across EU as pandemic enters another year. Eurofound.

[31] Wigert, B. B. (2022, March). The Future of Hybrid Work: 5 Key Questions Answered With Data. Gallup.Com. Geraadpleegd op 13 mei 2022, van https://www.gallup.com/workplace/390632/future-hybrid-work-key-questions-answered-data.aspx#:%7E:text=Fast%20forward%20to%20February%202022,39%25%20worked%20entirely%20from%20home.

[32] Morgan, R. E. (2004). Teleworking: an assessment of the benefits and challenges. European Business Review, 16(4), 344357. https://doi.org/10.1108/09555340410699613

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

[34] Yang, H., Zheng, C., Zhu, L., Chen, F., Zhao, Y., & Valluri, M. (2013). Security risks in teleworking: A review and analysis

[35] Zernand, M 2003, The Risks and Management of Telework, EBS Review, Issue 16, pp.101-104.

[36] Beauford, M. (2022, January 19). The State of Video Conferencing in 2022. Getvoip. Retrieved May 16, 2022, from https://getvoip.com/blog/2020/07/07/video-conferencing-stats/

[37] Blahopoulou, J., Ortiz-Bonnin, S., Montañez-Juan, M., Torrens Espinosa, G., & García-Buades, M. E. (2022). Telework satisfaction, wellbeing and performance in the digital era. Lessons learned during COVID-19 lockdown in Spain. Current Psychology, 1-14.

[38] Ipsen, C., van Veldhoven, M., Kirchner, K., & Hansen, J. P. (2021). Six key advantages and disadvantages of working from home in Europe during COVID-19. International Journal of Environmental Research and Public Health, 18(4), 1826.

[39] Criscuolo, C., Gal, P., Leidecker, T., Losma, F., & Nicoletti, G. (2021). The role of telework for productivity during and post-COVID-19: Results from an OECD survey among managers and workers.

[40] Pearl, R., MD. (2022, May 10). Americans Say Covid-19 Pandemic Is OverEven If Fauci, CDC Disagree. Forbes. Retrieved May 17, 2022, from https://www.forbes.com/sites/robertpearl/2022/05/09/americans-say-covid-19-pandemic-is-over-even-if-fauci-cdc-disagree/?sh=31976b4b530c

[41] WFH. (2022, March). Working From Home Around the World. https://wfhresearch.com/wp-content/uploads/2022/03/Global-Working-from-Home.pdf

[42] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110.

[43] IT Governance. (z.d.). Cyber Security. What is Cyber Security? Definition and Best Practices. Geraadpleegd op 9 mei 2022, van https://www.itgovernance.co.uk/what-is-cybersecurity

[44] Janani, A. K. (2021, 19 juli). Application Security: Definition, Types, Tools, Approaches. DevOps and Software Engineering Glossary Terms | Atatus. Geraadpleegd op 9 mei 2022, van https://www.atatus.com/glossary/application-security/

[45] Forecepoint. (2021, 6 mei). What is Network Security? Geraadpleegd op 9 mei 2022, van https://www.forcepoint.com/cyber-edu/network-security

[46] Kaspersky. (2022, 9 maart). What is Cloud Security? Www.Kaspersky.Com. Geraadpleegd op 9 mei 2022, van https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security

[47] European Commission. (z.d.). Critical infrastructure and cybersecurity. Energy. Geraadpleegd op 9 mei 2022, van https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

[48] Trendmicro. (z.d.). What is IoT security? Definition. Geraadpleegd op 9 mei 2022, van https://www.trendmicro.com/vinfo/us/security/definition/iot-security

[49] CIS. (2021, June 15). Election Security Spotlight CIA Triad. Retrieved May 11, 2022, from https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad

[50] Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-F496.

[51] Shred-IT. (2020, October). Data protection Report 2020. https://www.shredit.com/content/dam/shred-it/global/documents/Shred-it_2020-Data-Protection-Report_US.pdf.coredownload.inline.pdf

[52] Society of Human Resources Management. (2021). Navigating Covid-19 - Impact of the pandemic on mental health. SHRM. Retrieved May 22, 2022, from https://shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/SHRM%20CV19%20Mental%20Health%20Research%20Presentation%20v1.pdf?_ga=2.1019
20404228.1588356218

[53] Green, C., & Jodka, S. (2020, March). COVID-19 POSES INCREASED CYBERSECURITY RISKS TO EMPLOYERS AND BUSINESSES.

[54] Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021, July). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In International Conference on Human-Computer Interaction (pp. 583-590). Springer, Cham.

[55] Rubinstein, C. (2020, April 10). Beware: Remote Work Involves These 3 Cyber Security Risks. Forbes. Retrieved May 23, 2022, from https://www.forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/?sh=267586a661c4

[56] Wagenseil, P. (2022, March 18). Zoom security issues: Whats gone wrong and whats been fixed. Toms Guide. Retrieved May 23, 2022, from https://www.tomsguide.com/news/zoom-security-privacy-woes

[57] Ponemon institute. (2020, October). Cybersecurity in the Remote Work Era: Keeper. https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf

[58] Wang, Z., Zhu, H.,& Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910.

[59] FBI. (2021, March 17). IC3 Releases 2020 Internet Crime Report. Federal Bureau of Investigation. Retrieved May 24, 2022, from https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

[60] Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials, 15(4), 2091-2121.

[61] CIO COUNCIL. (2021). Telework Safe&Secure. Retrieved May 30, 2022, from https://www.cio.gov/assets/resources/telework-infographic.pdf

[62] IBM. (2014, May). IBM Security Services 2014 Cyber Security Intelligence Index. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

[63] Tenable. (2017, 1 augustus). Whitepaper: Survey Report: Trends in Security Framework Adoption. Tenableő. Geraadpleegd op 5 mei 2022, van https://www.tenable.com/whitepapers/trends-in-security-framework-adoption

[64] TanGensys Technologies Pvt Ltd. (2021, 25 januari). NIST Cyber Security Framework. TanGensys Technologies Pvt Ltd - Blockchain | IoT | Machine Learning | Enterprise Applications | Cyber Security. Geraadpleegd op 26 april 2022, van https://tangensystech.com/nist-cyber-security-framework/

[65] IT Governance. (z.d.). ISO 27005 | IT Governance USA. Geraadpleegd op 2 mei 2022, van https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005

[66] Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. Information & Computer Security.

[67] Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1.

[68] Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. Computers & Security, 95, 101846.

[69] Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cyber crime and security. International Journal of Research in Engineering and Applied Sciences, 2(1), 48-51.

[70] Alqatawna, J. F. (2014). The challenge of implementing information security standards in small and medium e-business enterprises. Journal of Software Engineering and Applications, 7(10), 883.

[71] Shiff, L. (2021, 13 mei). Comparing ITILő vs ISO 20000 for Service Management. BMC Blogs. Geraadpleegd op 11 mei 2022, van https://www.bmc.com/blogs/iso-20000-vs-itil-whats-the-difference-and-how-are-they-related/

[72] Susanto12, 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.

[73] Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: a framework for assessing cybersecurity risks. Cluster Computing, 23(3), 1827-1843.

[74] Gro, S. (2021, June). A critical view on CIS controls. In 2021 16th International Conference on Telecommunications (ConTEL) (pp. 122-128). IEEE.

[75] Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), 1401-1407.

[76] CSRC. (2020). Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions. ITL. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

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

[78] Chen, Y., & Sivakumar, V. (2021). Invesitigation of finance industry on risk awareness model and digital economic growth. Annals of Operations Research, 1-22.

[79] Steptoe, A., Wardle, J., Cui, W., Baban, A., Glass, K., Karl Pelzer, ... & Vinck, J. (2002). An international comparison of tobacco smoking, beliefs and risk awareness in university students from 23 countries. Addiction, 97(12), 1561-1571.

[80] Ivevi, A., Mazurek, H., Siame, L., Bertoldo, R., Statzu, V., Agharroud, K., ... & Bellier, O. (2021). The importance of raising risk awareness: Lessons learned about risk awareness sessions from the Mediterranean region (North Morocco and West Sardinia, Italy). Nat. Hazards Earth Syst. Sci. Discuss, 1-25.

[81] Jen, R. (2012). How to increase risk awareness. Paper presented at PMIő Global Congress 2012North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management Institute.

[82] Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, 103614.

[83] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, ., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.

[84] Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill-building approach (Seventh edition). Wiley.

[85] Adams, W. C. (2015). Conducting Semi-Structured Interviews. In Handbook of Practical Program Evaluation (pp. 492505). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119171386.ch19

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

[87] Bailey, J. (2008). First steps in qualitative data analysis: transcribing. Family practice, 25(2), 127-131.

[88] Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. International Management Review, 15(1), 45-55.

[89] Braun, V., & Clarke, V. (2021). One size fits all? what counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18(3), 328352.

[90] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

[91] DeCuir-Gunby, J. T., Marshall, P. L., & McCulloch, A. W. (2011). Developing and using a codebook for the analysis of interview data: An example from a professional development research project. Field methods, 23(2), 136-155.

[92] TU Delft. (2022). MSc Engineering and Policy Analysis. Geraadpleegd op 10 juli 2022, van https://www.tudelft.nl/onderwijs/opleidingen/masters/epa/msc-engineering-and-policy-analysis