Changes in cybersecurity by Forced Teleworking.

A practice-based approach to the changes in cybersecurity practices under coronavirus restrictions.

Student name:	Rens Buursen
Student number:	456466
Supervisor:	Dr. J. H. Pridmore

Master Media Studies – Media & Business
Erasmus School of History, Culture and Communication.
Erasmus University Rotterdam

Masters' Thesis
June 2020.

Abstract

Governmental response to the worldwide coronavirus pandemic is causing large and potentially lasting changes to society. One of these changes set in the Netherlands policy of forced teleworking. In order to mitigate the spread of the virus, all non-essential workers are to work from home, where possible. This policy has an effect on a large amount of subjects, one of which is cybersecurity. For this thesis research was performed into how this forced teleworking changed cybersecurity.

Data for this research was attained by performing interviews with eight different people working from home due to these regulations. Criteria for the selection of these respondents were that they (1) were available to interview under current regulations, (2) needed to have worked the same function before being forced to telework, (3) were forced to work from home due to these regulations, (4) have co-workers, (5) have a basic understanding of the computer systems they operate and (6) need to have work functions that provide access to sensitive data. This research was performed by way of looking through the lens that is practice theory and the transcript of the interviews were analysed by means of constructivist grounded approach.

The results of this research suggest that companies were relatively well prepared in the field of both hardware and software. Both these elements provided little to no problems when the forced teleworking started, and regulations that were in place, could largely be transposed to a teleworking situation. There were some issues however with the willingness of employees to combat IT-related issues, when an IT-department proved unresponsive or incapable of providing adequate technical support. Problems arose in the absence of co-worker closeness, and the absence of a physical security boundary in employee's homes, leading to possible data-breaches. In addition, external factors such as fear of catching the coronavirus proved to be possible stress factors, which could lead to unsafe digital practices.

Keywords: Cybersecurity, Teleworking, Practice Theory, Data Security, Privacy

Table of contents

1. Introduction

1.1. Cybersecurity during a pandemic

Measures to contain the rapid spread of the novel Coronavirus, the cause behind respiratory disease Covid-19, are in effect in some way shape or form in nearly all countries around the world. A pandemic with the same scale and impact to society as Covid-19 has not been seen since the Spanish flu of 1918 (Terry, 2020). The most commonly used frame to justify these measures is the call to 'flatten the curve' meaning to slow down the spread of the disease. This decreases the concentration of cases and patients needing to be treated by hospitals thereby providing some relief to strained healthcare systems (Terry, 2020). One of the most important and well-known measures taken to achieve this is the so called 'social distancing'. This social distancing has been instituted in different forms and with different specific regulation around the world, but in the core the concept remains the same. Refrain from physical contact and stay at home as much as possible (Terry, 2020). Following these social distancing regulations employees opt to have employees, if possible and often involuntarily, work from home. This has led to what is described by TIME magazine as the world's largest work-from-home experiment (Banjo et. al., 2020). Following this, it is important to realize that working from home usually lacks the data protection and IT supported cybersecurity an office setting offers (James & Griffith, 2013; Peacey, 2006), Therefore, this 'experiment' also crosses into the domain of cybersecurity. The convergence of the aforementioned factors aid in creating a necessity to research the implications large amounts of employees working from home and could, after the end of the corona crisis, aid in creating a safer and more cybersecure workplace when working from home.

When examining definitions of cybersecurity, the phenomenon has generally speaking been divided into two sides. There is a technical or machine side, and a human side (Craigen et. al., 2014). According to Conteh and Schmick (2016) the human side is seen as more vulnerable than the traditional technical side: "It is often easy to get computer users to infect their corporate network or mobiles by luring them onto spoof websites and or tricking them into clicking on harmful links and or downloading and installing malicious applications and or backdoors." (Conteh & Schmick, 2016, p.31). Even though these views provide an image that separates the technical side from the human side of cybersecurity, Malatji et. al. (2019) argue otherwise. In their view, to be able to deal with threats stemming from cybersecurity, organizations should create a framework that includes not only the technical aspect of security, but also the social aspect. The misalignment of these social and technical aspects forms, as they put it, a socio-technical gap (Malatji, et. al., 2019).

Acknowledging the misalignment between the social dimension of cybersecurity and technical dimension of cybersecurity leads to an improved understanding of cybersecurity threats. A possible way to explain and investigate this misalignment in cybersecurity dimensions is what can be named theory of practice. This practice theory suggests that there are three main elements to practices performed by humans. These are materials, competence and meaning (Shove, et. al, 2012). Understanding how materials or objects in cybersecurity interact with competences of those using these materials in combination with meaning or motivation is therefore key in explaining misalignment between the social and technical dimensions. Following this orientation highlights a need to research these factors regarding the practices within the field of cybersecurity when teleworking.

1.2. Relevance of cybersecurity practice research

Performing research into how these three factors affect the misalignment between social and technical dimensions in cybersecurity to create threats is relevant in both academic and social fields. The scientific value of this research lies in the understanding of interactions among humans and between humans and (new) technology. Looking from the point of human practice at the integration of technology and cybersecurity is relatively new. This means that the continuation of research into this field can add to currently known phenomena but can also create a new view on cybersecurity actions. In addition, looking at the communication and interaction between employees and organizational entities charged with tasks in the digital field highlight possible managerial and organizational implications.

From a social stance, performing research into practice theory in cybersecurity in teleworking could benefit all parties actively engaged in cybersecurity practices. Social distancing measures, as described above, may be in effect until as late as 2022 (Kissler et. al, 2020). Therefore, it is safe to say that it will be a long time until employees can return to work and working as usual will be restarted. Research that aids data protection and cybersecurity in these coming years is therefore very welcome. In addition, this so-called large experiment can act as a catalyst for the increase teleworking has undergone since the 1970's. Therefore, even after social distancing measures have been lifted, there is a strong possibility large amounts of workers will keep working from home. In the rapidly changing and expanding field of digital media, research into cybersecurity practices is therefore of great aid.

1.3. Research question

Given these pressing issues, a research question was created in order to guide this research. In order to create this research question all domains discussed above, namely involuntary teleworking, cybersecurity and practice theory, were incorporated. This produced the following research question:

> RQ: How has the transition to teleworking due to social distancing measures surrounding the coronavirus changed cybersecurity practices?

In order to answer this research question two sub questions have been devised. These are:

- How were cybersecurity practices at work perceived prior to the outbreak of the Coronavirus?
- How are cybersecurity practices in teleworking experienced during social distancing regulations due to the Coronavirus?

1.4. Summary

The objective of the thesis is to provide the reader with research-based findings that clearly show the differences or problems associated with cybersecurity practices caused by teleworking. As described above, this involuntarily working from home is caused by the social distancing measures imposed to combat the spread of the novel Coronavirus. This is done by not only looking at practices as they are during the times these measures are in effect, but also analysing the practices from before social distancing regulation. This provides the reader with an oversight in both differences and problems associated with cybersecurity practices during these times.

1.5. General outline

As described above, the aim of this thesis is to provide the reader with findings that show the differences or problems associated with cybersecurity practices caused by having to work from home. This thesis will be comprised of five chapters, the first of which is the introduction. After the introduction, a theoretical framework, methodology, results section and conclusion will follow. The theoretical framework will provide insights into current academic literature surrounding (involuntary) teleworking, teleworking and cybersecurity, practice theory and the link practice theory has with cybersecurity including human factors and the socio-technical approach. The methodology chapter will provide an explanation and rationale for the usage of semi-structured interviews and the sampling method used to set up these interviews. In addition, the constructivist grounded approach used to interpret the results will be explained here. The results section will provide the results of these interviews and their interpretations using constructivist grounded approach. The conclusion will provide an answer to the posed research question as well as provide a reflection on methods used and interviews performed. In addition, this conclusion will form the base for recommendations of further research into the field.

2. Theoretical Framework

2.1. Teleworking

The first step in understanding the cybersecurity implications working from home has versus working at work is understanding how working from home actually works. The idea of working from home is by far a new one. In times before the industrial revolution, most if not all work was done from home (Lupton & Haynes, 2000). Following large historical events, working from home has become popular and expanded. The beginnings of working from home in its current form was first implemented on a relatively large scale during the oil crisis of the early 1970's. The driver behind this timing, and the fact that teleworking has been ever increasing can be found in an increase and expansion Communication and Information technology (Lupton & Haynes, 2000; Toffler, 1980).

The Communication and Information technology Lupton and Haynes (2000) speak about however, was a reality experienced two decades ago, so it has to be understood in the context of a work environment of two decades ago. A lot has changed in the world of digital technology in these past twenty years. Van der Meulen (2017) sees the increase of digital technology as an important factor in working from home. Prior to the Corona crisis, approximately 23% of workers in the United States and 15% of workers in the European Union worked from home at least 'some of the time' (Van der Meulen, 2017). According to Van der Meulen (2017), "the practice of teleworking (ie, temporal and spatial flexibility) has been popular with employees" (Van der Meulen, 2017, p. 20). However, large companies like HP, Best Buy and Yahoo! have been decreasing the number of employees working from home, from the viewpoint that having all employees centralized is better for company performance. In addition, research by Groen et. al (2018) shows that when employees are working from home, management tends to focus more on controllable output such as proposed company targets and employee performance indicators. This could indicate a certain lack of trust on the company side towards the employee in performance from working at home.

This distrust gives way to the question as to how employees perform working from home. In answering to this question, Van der Meulen (2017) is clear. According to him employees perform better when working from home than working in the office, but only if the home they work from has less distractions than the office. Bloom et. al (2015) performed research into a Chinese travel agency with over 16.000 employees in order to analyse the benefits of working from home. According to this research, employees working from home perform 13% better than employees working at their regular workplace. In contrast to this however is research performed by Lippe and Lippényi (2019). They state that even though working from home may have benefits for the individual employee, the co-worker effect as they call it, leads to a decrease in productivity overall. Team performance is decreased when one of the team members is working from home since it becomes more difficult for employees to quickly share critical information. “Because co-workers are not immediately available, it will take more effort on the part of the individual employee to make use of their skills and knowledge” (Lippe & Lippényi, 2019, p. 73). This research does not necessarily contradict previous research that showed increased productivity from employees working from home, but it does show that for working from home to be beneficial to the company, certain requirements have to be met.

This previously discussed academic literature on working from home is primarily written from a company’s perspective. Data is acquired based on what is of interest to a company looking to improve its performance, however no clear views are presented on the effect working from home has on employees themselves. According to Dockery and Bawa (2018), there are both positive and negative implications in working from home for employees, yet the overall consensus is that working from home is a positive job attribute. However, as was the case with previously mentioned literature, there are certain conditions that have to be met before both the positive and negative implications can take effect. One of these conditions is the accessibility of technology for employees. As Ter Hoeven et. al. (2016) put it: “Technology use and employee well-being are positively associated through enhanced accessibility and communication efficiency but are negatively related through increased interruptions and unpredictability” (Ter Hoeven et. al., 2016, p. 255). This means that when working from home, having access to technology that assists communications aids the wellbeing of employees, but only when this access does not lead to more work interruptions or a higher unpredictability of the performed work. In addition, in a situation where there are children in the family, working from home does not seem to be as beneficial for the employee. In addition, there seems to be a negative effect on family functioning when the working from home happens on an involuntary basis (Dockery & Bawa, 2018).

Lapierre et. al. (2016) also showed this negative effect. Their research into the effects involuntarily working from home has on the family life of over 250 financial sales professionals showed an increase in work-to-family conflicts. This kind of conflict is found even more often with financial sales professionals who are weak at balancing work and family. The implication here is that when the balance of work and family is voluntary, employees are able to find an equilibrium that works best for themselves. When the balance of work and family is imposed by outside factors, this equilibrium becomes disrupted (Lapierre et. al., (2016).

The absence of this equilibrium is also one of the key reasons behind the research performed by Johnson et. al. (2007) that is focussed more specifically on women working from home. "In many jurisdictions, telework is promoted as a means of giving women more flexibility to balance their paid work with their household responsibilities" (Johnson et. al., 2007, p. 141). Aside from the quest for this equilibrium is also the notion that both work and personal life tend to penetrate each other when working from home. This is seen as a spatial reorganization that goes beyond only the location of the work performed. This reorganization also means the relocation of work into a setting that is mainly focused on things other than work, leading to leakage from both sides to each other (Johnson et. al., 2007). Hilbrecht et. al. (2013) connects with this in stating that the respondents in their research had a need to contain work while at home, since work seemed to seep into non-work home activities. In addition, working from home also seemed to devalue leisure especially for women with children, since working from home not only meant working, but at the same time also meant looking after children. This increased stress and decreased a sense of leisure experienced by other respondents working from home (Hilbrecht et. al., (2013).

2.2. Teleworking and cybersecurity

Working from home versus working at work does not only change the performance of employees and the way work interacts with family life, it also brings forth changes in the field of cybersecurity and privacy. As Peacey (2006) states, the ever-increasing numbers of employees working from home and connecting with their corporate networks, poses a large threat to IT infrastructure and business critical information. Even though this literature becomes outdated fast due to the rapid development of new technology, a lot of the points it discusses are relevant today. Teleworking provides risks to companies not experienced when employees are working in the company's internal environment. Employees working remotely for instance use public infrastructure that is not governed by the company's IT department. This means that a large part of the distance information travels between the company's internal system and the employees' computer are potentially not secure (Peacey, 2006). In addition to this, often when working from home, the computer used for this work is not a device provided for by the company. This means that not only is there a possibility that this device does not have the company mandated security settings, but there is also a strong possibility the device is used for other actions than just work. This means that on top of the security threats associated with working from home there are also threats from regular leisure time usage on the device at the same time (Peacey, 2006).

Newer work, by for instance James and Griffith (2013) support this view. "Teleworking is an established work practice yet often the information security controls in the teleworking location are weaker than those in a corporate office" (James & Griffith, 2013, p. 309). The researchers summarized three main problems in the field of teleworking information security from a report from the consultancy firm Deloitte. The first is in line with Peacey (2006) when they note the danger of data confidentiality breach when data is transported over the internet. Second is again in line with Peacey (2006), when they point to possible compromises to system and data integrity, specifically in the teleworking environment. Third is the breach of data confidentiality in the home-workspace (Deloitte, 2011; James & Griffith, 2013). The risks posed by these three problem definitions can all be relatively mitigated by security settings, end-to-end encryption and for instance securely storing data carrying devices, however firms seem to have problems enforcing these security policies on its employees (James & Griffith, 2013).

The dangers these problems pose become painfully evident in surveys performed by the British government under businesses and employees in the United Kingdom. According to these surveys, as of 2019, approximately 61% of large businesses in the United Kingdom had experienced some form of data breach or cyberattack (Gordon, 2020). According to Gordon (2020), there is no definitive research performed into whether these breaches and cybersecurity threats were predominantly caused by teleworking, however there is a strong connection that can be drawn. This is due to the notion that in sectors where more employees work from home, more data breaches are present. In addition, a lot of these security issues are caused by bad security practices and the absence of attention to detail (Gordon, 2020). Gordon (2020) even goes as far as to suggest that the best way to combat these security issues is to adopt a zero-trust IT security model. This model requires all users to perform identification steps before accessing a company's private network. "… once implemented, IT departments will have much clearer visibility of the exceptions and a way of allowing these less common access requirements through policy-based controls rather than ad hoc workarounds" (Gordon, 2020, p. 16).

There seems to be a common ground within these articles regarding teleworking and cybersecurity in teleworking that speak to the preparedness of the company's infrastructure. It seems that even though teleworking is more prone to security threats than regular work in a company location, safe teleworking is possible when a company has the proper preparation in place for employees to work from home (Gordon, 2020; James & Griffith, 2013; Peacey, 2006). A situation where the number of employees working from home drastically increases due to unforeseen circumstances makes this process difficult. Donnelly and Proctor-Thomson (2015) performed research into home-based teleworking in New Zealand after a series of earthquakes hit Christchurch in 2011. This natural disaster forced large amounts of workers to work from home for longer periods of time until the reconstruction of infrastructure allowed for workers to return to work (Donnelly & Proctor-Thomson, 2015). The implications their findings have for the data security of companies underline the importance of company preparedness for teleworking. According to them, "The often shared and cramped nature of working from home after an earthquake raises significant employee issues around data security, work distractions, health and safety needs, and family relationships" (Donnelly & Proctor-Thomson, 2015, p. 55). It is noteworthy to mention this also links up with findings by Dockery and Bawa (2018) and Lapierre et. al. (2016) in the negative implications involuntarily working from home has on family life.

This research gives insight into teleworking and some of the cybersecurity implications specifically associated with working at home. In addition, some insights are provided on involuntarily working at home as well as teleworking during natural disasters. All of these relate to the current situation of the masses of employees working from home due to restrictions imposed by governments in order to contain the spread of the Corona virus. In order to dive deeper into the implications the change of work location from an office setting to home have on cybersecurity, a step in between is needed. Even though the literature discussed up to this point is diverse, what it shares is the diversity in practices that affect cybersecurity in any way. So in order to conceptualize an answer to the posed research question it is important to create a lens through which to integrate all aspects of work that affect cybersecurity. This lens is practice theory.

2.3. Practice Theory

Practice theory has been used to analyse many different fields of research but is primarily used by organizational scholars. A specific singular definition of practice theory does unfortunately not exist (Nicolini, 2012). However, Nicolini describes the theory of practice as follows: "The appeal of what has been variably described as practice idiom, practice standpoint, practice lens, and a practice or practice-based approach lies in its capacity to describe important features of the world we inhabit as something that is routinely made and re-made in practice using tools, discourse and our body." (Nicolini, 2012, p.2). The key factors integrated within practice theory therefore seem to be tools, discourse and the body. In addition to this, Schatzki argues that practices are created out of a slightly different trinity, namely practical understanding, explicit rules and teleoaffectivity. Teleoaffectivity in this sense can be translated as the wanting of a human to complete a task. According to Galvin and Sunnikka-Blank (2016), these wants include desire, expectations and beliefs.

Following this, Lloyd (2010) argues that practice theory aids in understanding how for instance context affects social practice, which then in turn enables researchers to understand how skills and competences of employees may differ. Furthermore, Ford (2006), states that even though the application of practice theory does not provide the researcher with definitive social statistics, it does provide researchers with new views if judged and interpreted based on relevance to the situation at hand. "Put simply, the logic behind building practical theory is that it helps the practitioner to grasp patters of forces operative in the situation at hand, what Lewin (1951) calls the 'social field as a whole', and not primarily add to academic-theoretic knowledge." (Ford, 2006, p.501). Unfortunately, the absence of these social statistics, and the need to interpret data based on specific relevance to a situation, leads to the inability of the theory to prove hypotheses or a-priori assumptions. (Ford, 2006).

Returning to the proposed lens of practice theory, research into how households in Scandinavia deal with the loss of electricity describes its attributes in a clear and decisive way. “Trentmann (2009) argues that there is a built-in elasticity of everyday life that absorbs these disruptions, and that by looking at this elasticity of how practices change or stay the same, it is possible to identify vulnerabilities or robustness of households.” (Heidenstrøm & Kvarnlöf, 2018, p. 273). In this research however, the disruption is not the loss of power like Heidenstrøm and Kvarnlöf look into, but the Coronavirus pandemic, and the focus does not lie on households but cybersecurity, however it clearly describes the application of practice theory in order to combine everyday practices to be able to better understand the actors behind specific phenomena.

2.4. Practice theory and cybersecurity

There is relatively little academic literature where practice theory is used to view cybersecurity. Kabanda et. al. (2018) performed research into small and medium sized enterprises’ cybersecurity practices in developing countries. Results from this research show that these businesses specifically benefit from the lack of complex systems, but at the same time cybersecurity practices are inhibited by lack of funds and corporate support (Kabanda et. al., 2018). Practices were classed both external and internal environments, with practices like security hygiene and IT security expertise included respectively.

Pastore (2016) states that cybersecurity practitioners in intergovernmental arbitration are important but only aid in mitigating the risk of security breaches if all parties adhere to the same protocols. These can be surmised into three main categories (Pastore, 2016). Firstly the establishment of protocols for the secure transfer and storage of information. Secondly the disclosure of sensitive information has to be limited. Third and finally when the situation arises that a breach is detected, there has to be a process in place to notify those affected by the breach and efforts have to be made to mend the breach (Pastore, 2016). It is important to note here that the first and second of these proposed protocols lines up with the three cybersecurity threats posed due to teleworking by James and Griffith (2013) and Peacey (2006).

In addition to these linkages there is another important connection that needs to be touched upon, which is the human factor in cybersecurity. This is certainly a given when using a practice theory approach to cybersecurity, but it opens up a broader section of cybersecurity research to be applied to this thesis. When looking further into the human factor in cybersecurity, other research emerges that can be linked to the topic of practice theory and communication in cybersecurity. The first step taken in mapping previous research into this topic is defining its key concepts. The first definition needed for this research is the concept of cybersecurity. According to Craigen, et. al. (2014) cybersecurity is a term used broadly and in an unconcise manner throughout literature. They argue that the absence of a clear and decisive demarcation of the concept impedes advances in the scientific and technological field, due to the fact that cybersecurity is viewed predominantly as a technical matter. They state that when cybersecurity is no longer separated as a technical dimension separate from other factors, this could aid in resolving complex challenges posed in the field (Craigen, et. al., 2014). Therefore, the three researchers pose the following definition of cybersecurity: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights." (Craigen, et. al., 2014, p. 17). When connecting this definition with practice theory, it immediately becomes clear that practice theory, with its main concepts of materials, competence and meaning (Shove, et. al., 2012) and tools, discourse and body (Nicolini, 2012) is deeply woven into this definition. This is also backed up by Pridmore and Oomen (2020) who use materials, meaning and competences as building blocks of practice in their research into cybersecurity trainers in healthcare.

2.5. Human factors

Practice theory singles out the humanity in cybersecurity. This is a good thing, since computer systems are programmed, and therefore theoretically predictable. As previously described in the introduction, according to Conteh and Schmick (2016) the human element in cybersecurity is more vulnerable and susceptive to threats than the actual digital systems that are in place. Evans, et. al. (2016) argue that this might be based in the fact that human behavior is not consistent and influenced by the belief that bad things only happen to others. They therefore even propose the creation of a framework that uses Human Error Probability in combination with Error Producing Conditions to be used in the field of cybersecurity, in order to mitigate the potential threat human interaction causes. In addition, the researchers argue that fear appeals, a method of persuasive communication based on an element of fear, aid the effectiveness of cybersecurity practices (Evans, et. al., 2016).

Adding to this are the proceedings of the Human Factors and Ergonomics Society's meeting on addressing human factor gaps in cyber defence (Vieane, 2016). In these proceedings, the human factor in cybersecurity, and more explicitly the absence of training of humans in cybersecurity becomes apparent. "To date, most research in cyber security has been focused on technology applications, thus ignoring consideration of the critical roles humans play in cyber operations." (Vieane, 2016, p.770). Furthermore, Gutzwiler et. al. (2015) state fundamental human capacities are the limiting factor in cyber protection processes, yet cyber environments that are well-defended will almost certainly always rely on human interaction. This means that even though the human is the weakest link in cybersecurity, there is no possibility of creating a secure cyber environment without a social element in the mix.

2.6. Socio-Technical approach

This social element can also be found in literature by Muegge and Craigen (2015). They state that when designing critical infrastructure and communicating cyber security risks, a strong culture of cybersecurity has to be created. This means that meanings, shared beliefs and values, which form the backdrop for action (Smircich, 1983), need to be embedded within the organization of cybersecurity (Muegge & Craigen, 2015). As stated previously in work by Malatji et. al. (2019), aligning the social dimension of cybersecurity with the technical dimension is important for functioning frameworks. However, even though this socio-technical approach combines both the human factor and technological factor in cybersecurity and sees these systems as two side by side instead of separate (Whitworth, 2009), socio-technical approach does not include the 'meaning' dimension. Socio-technical approach does account for the interaction between humans and technology, and even states that to benefit to benefit one, the other must improve, aiming at technological advances as well as training for cybersecurity professionals (Malatji et. al., 2019). However, the motivational and meaning giving aspect of the interaction between humans and technology is left out. The inclusion of this motivation and meaning is what constitutes the practice-based approach (Shove, et. al., 2012; Nicolini, 2012; Pridmore & Oomen, 2020).

Accepting that cybersecurity, from a socio-technical standpoint is an interaction between technology and a human element, practice theory dissolves this dualism and aids in better understanding the interactions or practices that make up cybersecurity (Nicolini, 2012). Practice theory aids in understanding processes as routinized and recurrent. It views interactions between the technical and social part of cybersecurity as two-way traffic and lays an emphasis on things such as conflict, power and elements that make up the "social reality we experience." (Nicolini, 2012, p.6). Therefore, approaching organizational phenomena from a base of practices instead of objects and practitioners, provides a new way of understanding social interactions (Nicolini, 2012). When combining these views and the aforementioned tools, discourse and body from Nicolini (2012) that make up practices, it is also possible to link to Shove, et. al. (2012) and Pridmore and Oomen (2020). Their reduction of practice to three main practices of human interaction, being materials, competence and meaning, starts to provide a lens to view cybersecurity practices and cybersecurity communication through.

In conclusion, practice theory seems to provide a more holistic view on the performance of practices by humans. This is especially important given the performed research that views cybersecurity as a dualistic phenomenon with a social dimension and a technical dimension. Even though this research provides rich insights into the human element of cybersecurity, practice theory sees more than just two dimensions. Practice theory sees the connectivity and interconnectivity of all elements, factors and dimensions, providing a broader and new view on cybersecurity and how the communication of cybersecurity in critical transport infrastructure works.

3. Methodology

3.1. Approach

The aim of performing research by way of a practice-based approach to better understand cybersecurity in teleworking requires an in-depth understanding of multiple phenomena. In order to perform this kind of research, the choice has been made to utilize a qualitative research method. This choice was made due to the nature of qualitative research, which is inductive and interpretive (Bryman, 2008). In addition, Bryman (2008) states that two of the five main focus areas for qualitative researchers are ‘description and context’ and ‘process’, which are by definition deeply woven into a practice-based approach (Bryman, 2008, p.366). Therefore, the choice of a qualitative research method is most suitable for this specific research.

In order to perform adequate qualitative research, six major steps have to be taken (Bryman, 2008). Firstly, general research questions have to be prepared. This specific step has already been performed and has been discussed in the introduction. Secondly, a selection has to be made of relevant subjects and theory. Thirdly, the collection of relevant data has to be performed. The fourth process of this qualitative research is the interpretation of the gathered relevant data. Fifth is the conceptualization and creation of a theoretical framework out of this interpretation. Since however the creation of a theoretical framework requires repeated research and results, for this specific research, efforts will be made to provide preliminary insights into the combination of practice theory and cybersecurity. Qualitative research ends with the writing up of conclusions and findings (Bryman, 2008).

The first two steps of this research have already been performed. As described in the introduction of this thesis, a general research question has been provided. In addition, a theoretical framework has been created in order to provide relevant information surrounding the research topic and more specifically, the research question. These two steps form the basis that the performed research rests on and create the boundaries wherein the research is to be performed.

3.2. Data collection

The third step to be performed is the collection of relevant data. This step has been performed through semi-structured, in-depth interviews. The interviews were partially guided by prepared questions, but the order of these questions was varied depending on the conversation and follow-up questions were possible depending on the responses of the interviewee (Bryman, 2008). The choice to gather data via interviews rests on the ability of interviews to provide researchers with relevant data, especially from a practice-approach viewpoint. “The qualitative research interview attempts to understand the world from the subjects’ point of view, to unfold the meaning of their experiences, to uncover their lived world prior to scientific explanations.” (Kvale, 1994, p. 1).

It is important to note that the qualitative basis in which in-depth interviews lie does not necessarily need one definitive truth to answer the research question. This form of research accepts the fact that since the focus lies on the perception of people, there is no absolute truth, since this truth is based on the understanding of people (Brennen, 2017). In addition, as Hermanowicz (2002) states, interviews “yield data that can be used in understanding the organization and processes of social-behavioral life.” (Hermanowicz, 2002, p.481). Since the aim of this research is to apply practice theory on cybersecurity and cybersecurity communication in critical transport infrastructure, the possibility to understand organization and processes is key to this application. Furthermore, the choice for semi-structured in-depth interviews is made out of two major concerns.

First of all, the use of a standardized or fully structured interview would practically nullify the advantages of qualitative research. Creating a closed interview with only a specific number of prepared questions yields strong information regarding those specific questions but fails to provide data regarding different topics. Issues that are closely related to the questions asked during the interview are not eligible for adoption in the research, since the interview does not allow for them to be discussed. This would therefore decrease the possibility to understand description, process and context, which are in the end the reasons for choosing a qualitative research approach.

Secondly, the choice for semi-structured interviews was made because of the broadness and modernity of cybersecurity and teleworking or working from home. The reality is that due to this modernity and broadness, there is a strong possibility that not all concepts or dimensions that are considered relevant or important according to the interviewees, are included in the theoretical framework discussed previously. With the usage of closed interviews, these topics would be left out of the conversation and would therefore be missing during the analytical part of this research. By choosing a more open style of interviewing, even if topics that are not prepared or researched previously are discussed, these topics will be taken into consideration and included in the final analysis.

3.3. Sampling

These interviews, however structured and prepared, must be performed with respondents relevant to this research. To this end a combination of purposive and convenience sampling was used. The original intention was for this research to be performed by means of a combination of purposive and snowball sampling. This meant that the selected respondents were not only highly relevant to the posed research question, but they would also be the gateway to further respondents. Purposive sampling is viewed by most writers in interview-based qualitative research to be the recommended sampling method. “Such sampling is essentially strategic and entails an attempt to establish a good correspondence between research questions and sampling” (Bryman, 2008, p. 458). In addition, using a snowball method to arrive at new respondents from the originally purposively sampled respondents would yield a better overview of specific practices in a demarcated section of society. Unfortunately, the event responsible for the relevancy of this research, the outbreak of the novel Coronavirus, also meant it became more difficult to find respondents to interview.

To amend this difficulty and still acquire viable information the choice was made to use a combination of purposive and convenience sampling. This meant that instead of focusing on one specific niche in society, a broader perspective was used in order to ascertain respondents. This led to a situation where the respondents and performed interviews still fulfilled the set requirements for this research, however the ascertained data is more of a general, broad nature. This data can therefore be generalized in a better way than when snowball sampling was used, however, the data is less specific and clear-cut than it would have been.

3.4. Sampling criteria

In order to ascertain respondents for this research, the following selection criteria were used:

- Respondents needed to be accessible to interview.
- Respondents had to have worked in an office and from home in the same function.
- Respondents needed to work in sectors that required employees to work from home during the Coronavirus outbreak in the Netherlands.
- Respondents needed to have co-workers prior to the outbreak of the Coronavirus.
- Respondents needed to have at least a basic understanding of the systems they use for their work.
- Respondents needed to have work functions that provided access to sensitive data.

The selection of respondents on accessibility to interview has already been shortly touched upon above. This is the reason the used selection method is partly classed as convenience sampling. Key here is the fact that due to the outbreak of the novel Coronavirus certain regulations have been instated by the Dutch government hampering the acquirement of interview respondents. These regulations have influenced the economical positions of many companies in a negative way leading to a less than desirable willingness to participate in interviews for this research. In order to perform research in the current timeframe however, the choice was made to not only look at which interviews would yield best results, but also acknowledge the fact that it needed to be possible to actually perform interviews in these times. Therefore, the first selection criterium is the accessibility to respondents for interviews.

The second selection criterium is the past and present workspace of respondents. Since this research focusses on the perceived effect the transition of working from home versus working in an office environment has on employees, it is of great importance that respondents have actually worked at both the office and at home. Employees or people who primarily already worked from home are therefore not eligible for this research. The respondent must have undergone a change in workspace from an office setting to teleworking in order to provide the required information.

The third criterium respondents are selected on relates to the second, in the sense that it is derived from the work a respondent does on a daily basis. Regulations put in place by the Dutch government in order to contain the spread of the novel Coronavirus, forced a large part of the Dutch labour force to work from home. However, certain professions were excepted from these regulations. Since this research focuses on the perceived effects these measures have, it is important that respondents are actually in the respective group of the labour force that is actually affected by these regulations. Therefor this third criterium was added to the selection process.

The fourth selection criterium is the existence of co-workers in the job the respondent performs. As described above, the absence of co-workers, or better the issue of needing to share critical information with co-workers whilst working from home leads to a decrease in productivity (Lippe & Lippényi, 2019). In addition, the more co-workers a person has, the more unprotected networks that are used to access company data (Peacey, 2006). Furthermore, it is reasonable to assume that the presence of co-workers in an office setting, aids the secure sharing of data, since co-workers are physically closer to each other. Therefore, it is also reasonable to expect that the absence of this physical closeness can amplify potential privacy problems.

The fifth criterium used to select respondents for this research is a basic level of information technology know-how. This seems like a redundant selection criterium, since the expectancy is that employees are only in their work positions if they know how to operate the systems they need for the performance of their job. However, it is important that respondents understand the consequences of their actions and are able to point to directions of issues that relate to this research, instead of only 'knowing which button to push to make things happen'.

The sixth and final criterium focusses on the access to sensitive data by the respondent based on their occupation. This criterium was added for two specific reasons. Firstly, because of the fact that workers who do not have jobs with access to sensitive data, will not have the awareness of handling this data on a regular basis. Therefore, it is important to select respondents on this criterium. Secondly, this criterium is important since it implies that the employer of the respondent has also acknowledged this sensitivity. Therefore, certain security checks and systems will have been implemented, with which the respondent must work daily. Therefore, this final selection criterium is included in the selection process.

3.5. Respondents

These selection criteria have yielded the following eight respondents. The respondents and data stemming from the interviews were anonymised, for the benefit of readability pseudonyms were added for all respondents.

Sex	Age	Occupation	Pseudonym
Female	26	Client Due Diligence Analyst at a large bank.	Anna
Female	62	Care coordinator in primary education	Britta
Male	27	IT Service Employee at a bank	Charles
Male	28	Senior Application developer at a large independent administrative body	Derek
Female	25	Management trainee at a large management company focused on travel	Elizabeth
Male	25	Project and policy officer at a University of Applied Sciences	Frank
Female	38	Functional Controller of Digital Education Systems at a University of Applied Sciences	Gerda
Female	28	Detecting Financial Crime – Anti Money Laundering analyst at a large bank	Heidi

3.6. Structure and performance of the interviews

The interviews with the aforementioned respondents were held in two specific ways. Most of the interviews were performed via telephone or teleconference. Two of the interviews were held face to face. These face to face interviews, however, were conducted whilst abiding with current regulations surrounding the coronavirus. This means that there was at least 1.5 meters distance between interviewer and interviewee, and there were no other people in the same immediate vicinity. Since the choice was made to use semi-structured interviews, he performance of these interviews was guided by a set of thought out questions and follow-up questions. This does not mean that all questions were premeditated, however it assured a certain structure and coherence in respondents answers (Bryman, 2008). The interview guide used for these interviews can be found in appendix A. Even though this interview guide is written in English for the sake of this thesis, the interviews were held in Dutch, since this is the mother tongue of both researcher and all respondents. All respondents were sent a consent form, which is enclosed in Appendix B, however no respondent returned a filled-out response form, acknowledging that verbal consent was enough. In addition, three respondents made small changes to the interview transcripts, in order for their identity to be concealed as best as possible.

To create valuable information from the interviews, and at the same time have the interviews follow a logical path, the interview questions were set and asked in a specific manner. Since the aim of this research is to find perceived differences in cybersecurity practices between working at the office or working from home, the interviews were split in two major parts. Firstly, questions were asked regarding the situation a respondent was in, before the measures surrounding the Coronavirus took effect. This could then serve as a baseline to which developments could be held. The second part of the interview was centred around the current teleworking setting. Performing the interviews in this way would therefore not only yield qualitative information directly from the questions' answers but would also provide the possibility to compare both situations afterwards. Both of these sides of the interview were started by asking a guiding question, in order to change the focus of the respondent to the specific work location. This also aided in creating an image of the place of work of the respondent, leading to better follow-up questions and a better overall insight into the respondent's workplace setting.

In order to better structure the interviews in a way that fully utilizes a practice-based approach to cybersecurity, the concepts posed above by Shove et. al. (2012) and Nicolini (2012) have been used. According to their research, practice theory can be operationalized into the interworking of materials, competences and meaning (Shove et. al., 2012; Nicolini, 2012). Therefore, the decision was made to subdivide the two parts of the interview into these three categories. Each category was opened with a starting question, after which follow-up questions were used to either broaden or deepen the provided answers from respondents. It was important to operationalize these concepts in ways that spoke to the interview respondents. Asking what 'materials' somebody uses in their office with regards to cybersecurity will not yield desirable results. Therefore, the three concepts as proposed above were operationalized and worked into the opening questions and following sub-questions.

The first concept, materials was firstly operationalized by asking the respondents about what kind of computer, system and digital devices they use at their place of work. This specifically relates to the office they would usually work in. In the second part of the interview, regarding working from home, the focus lies specifically on the differences is devices and systems used whilst working at home. The second concept, concepts, opens by asking respondents about the training and guidance they received when they first started working in the position they have in their company. In the second part of the interview this question pivots to guidance and training received for working from home. The third concept, meaning, was operationalized for the first part of the interview as the responsibility experienced by respondents to work in a cybersecure manner when at the office. This question is asked again in the second part of the interview, however now with a focus on teleworking. Operationalizing these concepts and subdividing the interviews in this way, aids in both creating a better condition wherein respondents answer questions yet at the same time creates a 'baseline' and 'new' situation that can be compared.

3.7. Data analysis

When these interviews were performed the fourth, interpretive or analytical step in qualitative research was performed by way of constructivist grounded theory approach. Since there are multiple interpretations of what a constructivist grounded theory approach entails, the decision was made to utilize the method as described by Strauss and Corbin

(1990). After writing out the performed interviews verbatim, constructivist grounded theory approach relies on deconstructing the produced text and reassembling it in a way that provides an insight into underlying or recurring themes within the data. This is done by first open coding the deconstructed sentences from the dataset by labelling the sentences based on their content. A label in this form is a word or short sentence that is made to comprehend the interpreted meaning of the sentence (Strauss & Corbin, 1990). When open coding is performed for all text fragments, constructivist grounded theory approach continues with axial coding. During axial coding, descriptive labels are created that can house multiple open codes. This leads to a preliminary grouping of text fragments, based on interpreted meaning Strauss & Corbin, 1990). The third and final step, selective coding, combines these created axial codes under new all-encompassing labels that are aimed at explaining observed phenomena (Strauss & Corbin, 1990).

These created codes, and especially the final selective codes, provide great insight into underlying or recurring themes that are present within the interviews, but not necessarily immediately visible. In addition, these created codes, when connected with literature provide the fifth step in qualitative research. That is to say, when the connection between findings and literature creates a conceptual and preliminary set of results that aid in answering the original research question (Bryman, 2008).

4. Results

4.1 Findings

The sixth and final step of qualitative research, before a conclusion can be provided is the writing up of all results and findings. (Bryman, 2008). As described above, the transcripts of the interview were processed by way of constructivist grounded theory approach. Therefore, the text fragments stemming from the interviews were coded in order to reveal underlying themes. The eight performed interviews revealed four main underlying themes, which could be subdivided into twenty-seven subthemes or axial codes, the most interesting of which, will be discussed further on. These axial codes were comprised of approximately 160 open codes. All of these codes can be found in the coding trees provided in appendix C. Before diving deeper into the results of this coding and shedding a light on cybersecurity working from home or from the office from a practice point of view, it is important to discuss the four overarching themes that flow from the performed interviews. These four themes are organizational preparedness, individual work practices, practices that mitigate cyberthreats and practices that act as a catalyst for cyberthreats. It is important to understand these overarching themes, in order to give a preparatory overview of the interview results.

The first overarching theme, organizational preparedness is comprised of the key findings digital diversity, spreading of technical knowledge, the existence of technical knowledge, regular company operations and finally digital communication of practices. This specific overarching theme focusses, as the name suggests, on the preparedness and therefore ruggedness of a company in the field of cybersecurity. In this sense digital diversity for instance is explained as the broadness of types of devices in use by employees of a company. These differences show themselves in things like the fact that for some companies, IT departments hand out specific digital devices, bought in bulk to reduce cost, all with standardized hardware and software. Other companies however, let the employee decide what kind of digital device they want to use, and let the employees purchase this device. As Elizabeth explains: “For my laptop, all I had to do was provide an invoice and that would take care of it.” There was no criterium set for this other than a maximum price. This specific example, backed up by the fact that regardless of device and even operating system the IT department of Elizabeth’s employer is able to provide technical support, reflects as a prepared and knowledgeable IT department. Findings like the spreading of technical knowledge under employees and the existence or pre-existence of technical knowledge aid in this experience. From this overarching theme, there is not necessarily a transition that can be distilled in cybersecurity practices. It is more of an overview that shows how organisational preparedness, both in the field of teleworking and working from home plays a factor in the practices that employees have. Not needing to radically change practices when forced to work from home, means that practices by employees and cybersecurity stay relatively the same.

The second, overarching theme is framed as practices that mitigate cyberthreats. For this specific overarching theme, the findings are not clustered around the preparation but more on the active practices employees have to engage in, in order to protect themselves and their company from cyberthreats. This does not limit itself to practices that are requested or, regulated for that matter, by the companies the respondents work for. These regulations, such as gatekeeping of sensitive data which can restrict access to certain documents, or include access auditing for certain parts of company's systems are also merged with things like personal motivations and legal implications of security breaches. This means that this second overarching theme is more focused on the actual individual day-to-day practices that mitigate the risk of cyberthreats, rather than an overall preparedness.

A good example of this risk mitigation is for instance the position bound authorization that falls under gatekeeping of sensitive data. As Derek puts it:

> "In my case I have a lot of freedom since I am an application developer. This means that I for instance need to share large dumps of processes and technical logging data or technical snapshots of or applications with large suppliers. For instance, with the Microsoft's of this world, so in that sense I have a lot of freedom. I am one of the approximately 150 people who has USB rights."

These USB rights Derek refers to are the rights to actually use USB sticks at the independent administrative body he works at. The thousands of other employees that also work for the same administrative body, aside from about 150 other people, do not have this right and cannot use USB sticks on their work computers. This clearly indicates the effect a specific position bound authorization has on the day-to-day operations at that company.

This second theme shows special practices that are in action in order to mitigate cyberthreats. Remarkably only a small portion of these mitigating practices are primarily derived from teleworking. This could mean that there is no need for these practices to be changed in order to be able to be performed when working from home, or working from home is not seen as a setting that needs additional or special security practices by employees and employers.

The third overarching theme is classified as individual work practices. Under these practices fall working within a specific environment, relations surrounding the workforce and physical workplace features. The difference however between these practices and the practices that mitigate cyberthreats, is the fact that for this specific overarching theme the focus shifts away from the digital environment and cyberthreats. The focus here lies more on physical work environment and the physical workplace. A good example of this are the references to working within a specific environment. This subcategory contains things like internal tension caused by disagreements between employees and workplace flexibility. On the other side it also contains the subcategory of IT structure, which relates to the actual organizational structure of the IT department within the company the respondent works for. This has an effect on the physical workplace since by this subcategory, on-location IT helpdesks and physical IT help are classified.

This third theme shows that there are clear differences between the physical workplace at work and the physical workplace when teleworking. These differences not only mean that different practices are in action, but also clearly highlight how extra practices are necessary in order to cope with the different threats this locational change entails. In order to be mutually exclusive however, this theme is restricted to the physical workplace and its facets, including the relations employees have with one another.

The fourth and final overarching theme is framed as practices that act as a catalyst for cyberthreats. This category seems to yield the most interesting results as it uncovers practices performed by respondents that can have a definite negative impact on their employer’s protection against cyberthreats. A good example of this is for instance the subcategory of IT related workflow issues. These workflow issues show intentional security breaches performed by respondents in situations where the respondent needs to work around a security regulation or system to effectively perform their job. In addition, these workflow issues also include pushback by employees against forced IT regulations, pushback against ineffective work systems and employees working around IT problems.

A good example of this can be found in the interview with Elizabeth:

> “The IT recommends using a certain environment to work in. Citrix. However, I must say that I find that very slow to work in and therefore I just work in Office 365. That has most of the same functionality.”

This clearly shows that since Elizabeth finds Citrix to be a rather slow working program, against the advice of the IT department, she decides to work outside of the protected environment. This intentional working around IT problems therefore shows as a clear practice that can act as a catalyst for cyberthreats.

As described above, this fourth and final overarching theme is a concentration of practices that act as a catalyst for cyberthreats. These threats are found both in practices at the regular workplace, but also when working from home. What seems to be interesting here is that all practices that can be classed as catalysts for cyberthreats at work are also carried over to a situation of teleworking. However, a teleworking situation also adds more ‘dangerous’ practices to those original practices.

4.2. Organisational Preparedness

4.2.1.Office settings and regulations

As described above, the overarching theme of organisational preparedness does not necessarily show the changes in cybersecurity practices that can be attributed to forced teleworking in times of corona. This overarching theme focusses more on, as the name suggests, the preparedness of an organisation in the field of both teleworking and cybersecurity. This does not mean that this theme does not play a large role in teleworking, however it shows that not all practices change depending on whether an employee is working in an office setting or working from home. Therefore these findings can also impact cybersecurity in both an in-office and teleworking setting.

The first of the two sub questions posed in the introduction focusses on the perception of cybersecurity practices in an office setting. This office setting was the original work setting for respondents before the outbreak of the Coronavirus. One of the findings that fall under the aforementioned theme of organisational preparedness is company enforced regulations. These operations encompass enforcing security regulations, and things like fines imposed by a company when an employee is found breaking one of the company's rules. A good example of a company enforcing security regulations can be found in the interview with Elizabeth:

> "Sometimes they send those fake-phishing e-mails. Where you have to click on something. And if you do actually click on something you see a screen with the text 'well, employee, you are not doing well since you clicked this.' To put it like this. So in that way they are also trying to make employees conscious."

This specifically shows that the company has a proactive stance in enforcing security regulation. In addition to communicating regulations and for instance training employees in how to work with specific data, the employer Elizabeth works for actively checks whether its employees actually abide by the set regulations. Another way this enforcing of regulations is done by companies, is to use two sets of eyes for a single project. As Derek points:

> "But I have to check that all technical demands that apply to it, that apply to that specific form of data, whether I have checked that box or not. And on top of that my work is sent to a tester who again checks everything before the acceptation department even looks at it."

For Derek's case it has to be said that the applications Derek creates handle large amounts of sensitive and confidential data. Therefore, even though the principle of two sets of eyes checking for possible issues might seem exorbitant, it serves a good cause. On the other hand however, respondents also showed that even though companies tried to enforce regulations, sometimes they would intentionally and knowingly work around these regulations. Charles for instance uploaded and used specific computer scripts at his workplace, even though he knows this is technically not allowed.

> “I wrote some programs in Python and converted those to EXE files. I can run those on all Citrix environments. I used those to make it easier. I think you’re not supposed to do that actually, but I did anyway.”

With this final quote in mind it is not surprising to state that companies do not always fully trust their employees in their day-to-day practices. This is something that, specifically in teleworking, Groen et. al. (2018) points out in stating that teleworking is not seen as favourable for employers since there is a lack of trust towards the employees from the side of the company. In addition, this also lines up with the notion brought forward by Conteh and Schmick (2016) in stating that the weakest element in cybersecurity is the human element.

4.2.2. The influence of Digital Diversity

Another recurring theme in the interviews seems to be the digital diversity the respondents deal with on a daily basis. Even though this topic is not necessarily connected fully with teleworking, since digital diversity can present itself in a situation at the office too, it is important to acknowledge the potential cyberthreats stemming from it. Digital diversity can be found for instance in the completely free choice Elizabeth had when selecting a new digital device to work on. The IT department and cybersecurity needed to be able to cope with the device she selected. There are large differences between specific devices and the systems they run. In Elizabeth’s situation it is not only the case with the computer but also with the telephone: “For my job you get a phone from work. And they let you choose between an iPhone XR or a Samsung 9.” In this situation, Elizabeth chose the iPhone over the Samsung, however she had never used an iPhone before. “Then they ask you, whether I had had an iPhone before and if there was anything they could help me with. I said I have no idea. And then they started to install everything for me.” In line with this is a remark made by Frank. “Because I actually I prefer to work on my own laptop, so I work with USB sticks to transfer files from my work laptop to my personal laptop.” The major difference between Franks work laptop and personal laptop is the fact that the first is a Windows laptop and the second is a MacBook.

In addition to this difference in operating systems is also the notion that a lot of special systems particularly relevant to the job the respondent performed were used. Even though respondents acknowledged to all using the same systems for basic office text processing like Microsoft Word, PowerPoint and Excel, be it in the form of the old-style Microsoft Office package or the newer Office 365, companies used their own special systems. The interviews brought forward multiple examples of this. Gerda for instance, worked with Remindo and Osiris, both systems primarily used in educational settings.

Anna on the other hand, uses many different systems.

> “We actually use a lot of systems. We have one main system and those are actually all webpages. I’m not sure what it’s called since they’re not applications. They really are webpages. For example, we have one where other departments upload our work assignments. And one where the progression of the work assignments is uploaded. Then we have another system that is used by the entire bank. That contains all the data of the clients.”

Heidi, working for a different bank, acknowledges this. “Yeah, we have, we only work with systems from the bank.” This digital diversity again shows the importance of preparation and security Gordon (2020), James and Griffith (2013) and Peacey (2006) talked about. Since the types of devices and the types of systems used by employees is so broad, the security measures in place need to be well prepared and carefully constructed in order to be applicable to such a large digital diversity. The point made here, is that if a company is able to adequately protect such a large pool of different equipment and practices accompanying these tools, it signals a well-rounded and cybersecure defence mechanism.

All these subthemes regarding office settings, regulations and digital diversity create an image that shows the importance of organisational preparedness. Even though this may not focus on the change that can be found in cybersecurity practices, these subthemes do highlight the importance of carrying out specific set and prepared practices. Therefore the overarching theme of organisational preparedness is an important contributor in cybersecurity practices.

4.3. Practices that mitigate cyberthreats

4.3.1. Access to IT services

The second overarching theme is described as practices that mitigate cyberthreats. This theme is created out of the combining of practices that, like the theme states, have a mitigating effect on cybersecurity. As described above, only a small portion of the subthemes grouped under practices that mitigate cyberthreats are specifically in place in teleworking situations. However, this does not mean that there are little to no practices in place that mitigate cyberthreats in a teleworking setting, it means that these practices are not specific to a teleworking situation.

One of the elements that came forward during the interviews as a potential weak point in the field of cybersecurity in a regular office setting was the access to or accessibility of IT services. In addition to this, it became apparent that some IT departments were viewed in a more negative way than others. When asked about his company's IT department, and the support they could provide, Charles responded as follows: "They don't help you in any way. But yeah, there is an IT department. But all they do is create a support ticket, and that is a very difficult process."

This response was in question to larger IT problems. According to Charles, smaller technical issues were dealt with in an easier and more direct manner, however both his responses carry a firm and negative tone regarding the department that should be playing a key role in his company's cybersecurity. Furthermore, the consequence of this negativity is that Charles and his co-workers lose interest in solving IT issues:

> "Yes sure in the beginning I really wanted to work [on that]. You think, I'm going to send in a thousand tickets. But after a while you really don't care anymore. And then, when you encounter something that doesn't work, you try to fix it yourself and if that doesn't work you ask the IT. Actually everybody thinks about it like that. There were a lot of things that I would come up with, and the response would be, 'Yes we've known about this for a long time but the IT doesn't do anything about it.'"

This demonstrates that even though Charles wanted to initially work together with the IT-department and work in accordance to what the company wants him to do when he encounters an IT-related problem, he quickly realizes that working this way does not provide the results he wants.

Other companies, like Elizabeth’s, are on a totally different side of the spectrum when it comes to trusting and accessing technical help from an IT department. When she was asked if the IT department of the company she works for performed well, she responded in the following manner:

> “Yes I think so. You can just call them and you immediately get to talk to someone. And almost all IT personnel knows everything. Sometimes your call is redirected, but that usually happens straight away. It’s not like… I think you’re call is on hold for a maximum of five minutes. I have never experienced a problem that meant I couldn’t work for half a day.”

The response by Elizabeth shows the effect adequate response to technical issues can have on the mindset of employees. Of course, these two responses showed the very ends of the experienced spectrum of access to IT services. Following from what Galvin and Sunnikka-Blank (2016) stated, that practices are driven by the wanting of a human to do something, described as teleoaffectivity, an interesting suggestion can be made. Since it becomes clear that at the company Charles works for the IT support is not able to adequately deal with more complex digital problems, it seems as if the teleoaffectivity that should drive the request for help from the IT department becomes absent. Since there is some sort of acceptance that the IT department is not going to help in solving issues, issues are left without report or solution. This would at the same time suggest that due to the ease of access and high technical knowledge and skill of Elizabeth’s IT department, employees at that company could have a stronger teleoaffectivity towards IT related issues. This is an interesting point that begs further research.

It is important to note that both Charles and Elizabeth work for relatively large companies. Britta, working for a few elementary schools in the Netherlands does not have the same form of professional IT support both Charles and Elizabeth can experience. When asked about her access to technical support she answered: “I have the mobile phone number of Peter, the IT guy”. This ‘IT guy’ Britta is referring to is actually one of the elementary schools teaching assistants, who happens to have an above average level of knowledge in the field of IT.

This is of course a potential issue. The lack of professional support is in line with Kabanda et. al. (2019), suggesting that this is inhibiting cybersecurity practices. On the other hand however, the smaller scale of the elementary schools Britta works with is a protection to possible cyberthreats. This is due to the fact that smaller companies usually have less complex IT systems and therefore there is less that can go wrong (Kabanda et. al., 2019). What this research does not include is the interactivity between smaller businesses. Even though the systems at Britta's elementary schools may be relatively simple and thereby relatively safe, a huge problem occurs when she works together with other special care institutions. Since these institutions are also small in nature, they also do not have access to high level IT support. This creates a situation where both parties work with different systems and neither has adequate technical support to bridge the systems. In Britta's case this leads to the use of a personal cryptography amongst employees. Britta and the people she works with in different institutions make up their own code words in order to describe certain sensitive issues. This way information regarding students can be exchanged over open channels, since secured channels cannot communicate with each other:

> "It is sometimes very difficult that the systems are not connected to each other. Everybody has a different system. This means that between us and a couple of other care institutions we've developed some form of cryptography."

By creating their own secret code, Britta and her colleagues from other institutions can communicate relatively openly about sensitive information, without having the need to use the systems they feel are not working. This adaptation clearly shows the need to adapt in order to overcome technical problems in smaller companies since the access to IT support is less than desired.

4.3.2. Gatekeeping of sensitive data

Another subtheme that can be classed under the theme of practices that mitigate cyberthreats is the gatekeeping of sensitive data. Gatekeeping in this sense is defined as trying to control access to sensitive data, generally performed by limiting this access based on employee needs. To some this may sound as an odd concept however, gatekeeping in different levels can be found in all respondents' practices. For instance, Heidi, when she wants to work on her work issued laptop, has to log on using her company issued employee card and her personal access codes. In addition, she has to be connected to a special network in order for this to be possible:

> "so you put the card in the side of the laptop and you enter your personal code. And now at home we have a VPN connection. First at the office we also had a VPN connection, however they eventually just installed a company network, so once you were logged on at work you were connected to the banking network. (…) and at home we now have the VPN. That's a kind of pop-up where you have to fill in your personal code before being connected."

Interestingly Charles has to log on to a special system too before he is able to start performing his work. He has to log on into one system before he can log on into the next system: "But we, well I have to log in to the Citrix environment of company (…), and after that I have to log on to the Citrix environment, my own Citrix environment. So actually a Citrix within a Citrix, to make it a little complicated." Even though logging on to a system or on a work computer sounds like a regular practice that does not need a lot of attention, it is the process that keeps unwanted or accidental intrusions out of the company's system. There are also other gatekeeping systems in place, dependent on the company a respondent worked for or the data the respondent handled. Derek's employer for instance uses a special system to audit all logins and mutations performed by employees in their systems:

> "In all our systems we have audit-login. That means that the minute you log in to a system, from the user-end, (…), for all functional actions, they are recorded. They are just audited. So you can see that John Doe logged in at 12:31 and exported this specific data at 12:37."

Now it could be suggested that this is a very extreme form of gatekeeping that almost borders on the infringement of the employee's privacy, however this system is in place with good reason. In the system Derek works with, a lot of sensitive data is stored, regarding not only regular people, but also what they call VIP's. If an employee accesses the data belonging to one of these VIP's, the login auditing system immediately sends a message to the overseeing security officer of the employee who accessed the data:

> "Yes then the security officer of that person receives an e-mail with the message that this person accessed data of a VIP. Please put a digital explanation in our archive why this happened. If that explanation isn't given, the employee is immediately fired."

According to Derek, accessing this data without good reason could even lead to the company starting legal actions against the employee.

All of these forms of gatekeeping do serve a good purpose. However, they limit the amount of people that can access certain types of data, and if types of data are highly sensitive and of such a nature that they demand to remain secret, there is a clear log of who accessed this data and why. This all seems relatively in line with the recommendations made by Gordon (2020) with regards to adopting a zero-trust software defined perimeter approach. The four steps of this zero-trust approach, verifying the user, verifying the device the user is connected with, protecting the data and controlling access to the data can be, at least to some extent found in the practices performed by all of the respondents.

4.3.3. The productivity of teleworking

Shifting away from recurring topics that primarily concerned working in an office setting and moving towards experiences from teleworking, first an important result has to be brought up. When looking at previously discussed subthemes, it becomes apparent that the practices that make up the subthemes, outside of the ones pertaining to physical contact, can all be transferred to a situation of teleworking. In line with Van der Meulen (2017) and partially also Ter Hoeven et. al. (2016) the performed interviews showed that with the current technology, most of the practices that make up respondents' work could be performed at home instead of at the office.

When asked how working from home changed Heidi's work she answered: "Well, you see our work can be performed relatively easy from home, so that did not change a lot actually." Gerda also sees it like this, since she says she is more productive in shorter timeframes. “Well, I notice that I get more work done in a shorter timeframe. That is one of the largest differences with working from home that is actually noticeable.” When asked why she thinks she is more productive, the reasoning seems very logical and practical:

> “Well I smoke, and I had colleagues… I’ve worked at this school for a long time so I know a lot of people. So what happened was that a lot of the times I was asked to join people for a cigarette or to drink some coffee. And that doesn’t happen now. So that saves me a lot of time.”

Charles’ response is in line with Gerda’s reasoning, although in his case, smoking is not the cause. When asked whether he performs better working from home or working at the office he responded that he is more productive at home:

> “See, if you are working well at home, you’re working better than in the office. Because, when you are really focused at work, you will have someone asking you questions or interrupting you. And that really bothers my workflow. So at home you do not have that kind of distraction.”

Interestingly, even though Heidi’s remarks are a clear indication that working from home can be a task that is comparable in ease to working from the office, the latter two quotes do show different results than expected. The quote by Charles, regarding being bothered at the office by his co-workers and therefore being less productive at work seems to be in line with Bloom et. al. (2015) in arguing that working from home people can work more during the time in their shift, yet in contradiction to literature by Lippe and Lippényi (2019). They stated that the absence of co-workers would lead to less productivity. This is not to say that the literature is incorrect. Ter Hoeven et. al. (2016) for instance deals with the possibility of employees being interrupted at work by co-workers due to access to modern technology. Even though here the focus is on modern technology making this interruption possible and the interruption having effect on employee positivity in a telework setting, the core remains the same. Being bothered by co-workers when working is detrimental to work performance. The absence of this interruption leads to increased work performance.

The same is the case for Gerda. Even though the absence of smoke and coffee breaks with co-workers is not something regularly found in literature surrounding teleworking, the core reasoning stays the same. Working from home can be more productive than working from the office, however only if there are less distractions in the teleworking setting than there are in the office (Bloom et. al., 2015; Van der Meulen, 2017). Given that these distractions have such an effect on work productivity, the question can be raised what these distractions do for cybersecurity. If the absence of mutual surveillance can potentially increase cybersecurity risks, distractions from a social perspective when teleworking could potentially add to this. Therefore practices that affect the productivity of teleworking, may also have an effect on cybersecurity.

4.3.4. Company regulations regarding teleworking

As previously discussed, there seems to be an absence in security controls specific to teleworking situations versus working in a corporate office setting. This is also something that is supported by literature provided by James and Griffith (2013). In addition to this, research also shows that teleworking is safer when the company of which the employees are working from home has proper preparation in place (Gordon, 2020; James & Griffith, 2013; Peacey, 2006). Therefore, one of the questions posed in the interviews was whether the company, be that management, Human Resources or the IT department had specific teleworking regulations in place. Most of the responses to this question were classified under the axial code of company forced regulations, however now from a teleworking perspective.

One of the most interesting results stemming from the interviews was the fact that at Derek's company, people initially were not allowed to work from home at all. "Before the corona crisis our teleworking policy was, well you don't work from home unless you had a reason… And that had to be for a very good reason." The reasoning behind this was that social pressure from co-workers would entice people to work harder. Or, as Derek puts it: "For a large part of our population, and that is to say in the field of ICT as well, the intrinsic motivation is relatively low. That means that those people do nothing but look at Reddit all day." This seems to at least partially validate Groen et. al. (2018) in reasoning that companies do not trust their employees enough to work from home. However, when it is mandated by the government, the employer no longer has a choice in the matter.

Other respondents provided information that indicated that there were little to no specific regulations provided by the employer to cope with teleworking. One of these regulations has already been discussed. Elizabeth’s case where the IT department requested employees to work within the Citrix environment when working from home is a good example of these regulations, even though Elizabeth decided not to adhere to those regulations.

When asked whether Gerda had received any regulations focused on teleworking she replied that “At first we did not receive any tips or instructions” however, further on some information and regulations began to be provided for: “In the second week they told us that, dependent on your situation at home, you are completely free to furnish your work environment in the way that you want. That is actually the first thing they said to us.” Eventually, after another week, the company she works for started to adapt to the new teleworking situation. “Then in the third week, they also told us that in order to make work as comfortable as possible, you are allowed to take any devices from your office location to your new teleworking location. Whether that be at home or some other place.”

This seems to imply that there are no extra regulations with regards to cybersecurity imposed for working from home and telework specific regulations that are created are more focused on the physical differences between working from home and at the office. This is also something that becomes apparent in the interview with Charles. One of the changes that was made in order for him to work from home was starting to use an app for his private phone that allows him to call and be called from the company landline on his mobile phone: “There is some sort of an app on my phone that connects to the calling-app. So I call with my own phone, with my private phone. But with a different number of course.”

Going even further than that, or less regulatory than that, was the experience of Frank. When the outbreak of the Coronavirus forced everyone at his office to work from home, he worked another week at his regular office. Since if there are no other people it should be allowed to work there. When he finally was forced to work from home by his management, he stated that the only thing specifically requested when working from home was with regards to digital communications. “Now and then people ask you, when your Teams is not on available, but you are working, to set it to available. And the Outlook agenda is kept up to date a bit better than before.” This then seems to be relatable to the notion of mutual surveillance, where co-workers check on each other in order to make sure everyone follows the rules set by the employer.

All these subthemes show that specific practices, when working in an office setting or when teleworking can have a mitigating effect on cyberthreats. However, these practices may not necessarily be solely focussed on working from home but can be practices carried over from the office. There are some practices, for instance in Charles' case, where the practice of using an app on his private phone in order to use that phone for work, is a practice that is specifically created since the 'normal' practice at work is not available. However, it seems as if practices that are created in order to mitigate cyberthreats are mostly carried over from working in an office setting to teleworking.

4.4. Individual Work Practices

4.4.1. Working environment

The third overarching theme that could be derived from the interviews is classified as individual work practices. The subthemes that are combined under this topic primarily focus on the physical workplace at work and the physical workplace when teleworking. In addition, these practices focus both on the individual and on the employee working together with co-workers. The subthemes in this overarching theme show that dependent on the location the employee works at, specific practices change.

Previously presented results show the importance of both the skill and competence of IT support and the accessibility to IT support via digital communications. Even though modern technologies mean that for most IT-related problems physical human interaction is no longer necessary, some tasks and problem solving still need an employee to go by an IT desk in person. This specific problem is classified under the findings of working in a specific environment, since it relates to the physical organizational structure of IT within a company. Therefore, it falls under the theme of individual work practices.

For Britta for instance, this physical location was centralized in one of the elementary schools she works for. If she had other IT related problems, she was to contact the teaching assistant that was tasked with IT problems at that specific location. Remarkably however, for Heidi, who works for one of the largest banks in the Netherlands, this physical IT location was also centralized. When asked whether she was able to pick up her digital devices at the building she works in, and this building is one of the head offices of this bank, not a regional office, she replied in the following manner:

> “No we indeed had to go to a different office. The head office where the IT is housed. That’s where the laptop was registered to your name and where it was handed out to you. That was also the place where your access pass was activated with the code within the laptop. So if there is anything wrong with your computer, then you have to go there.”

This means that Heidi needs to go to a different location than where she regularly works in order to have physical IT support. Instead of having some support located at her workplace, she needs to actively travel to one location in order to receive support.

Contrary to this however is the bank Anna works for. This bank has, specifically now that due to the regulations surrounding the Coronavirus employees are forced to work from home, tried to bring these physical IT points closer to its employees. “The situation now is that separate service points have been created throughout the country, so people do not have to travel too far if there is something wrong with their laptop in times of Corona.” These service points, specially created in larger regional offices in multiple cities throughout the Netherlands, clearly show a company’s effort to decentralize and provide accessible services for its employees. This means that, when it comes to the materials part of practice, as described by Shove et. al. (2012) and Pridmore and Oomen (2020), Anna receives better and more accessible support, helping her perform.

This seems as if it is in clear contrast with literature by Van der Meulen (2017), since that stated that even though the rapid increase of technology aids the possibility of teleworking, companies prefer a centralized form of working. Even though this might be the case, literature by Lippe and Lippényi (2019) could also provide insight here. Their research showed that the absence of co-workers leads to a decreased productivity when teleworking. This decreased productivity is due to the fact that employees use each other’s skills and knowledge “…because these considerations have consequences for individual-level performance.” (Lippe & Lippényi, 2019, p. 73). This could be interpreted as relevant only for the collaboration of regular employees, however it could also be expanded to the aforementioned decentralization of IT services. Since IT helpdesks can be seen as places that provide employees with skills and knowledge, whether it is in the way of technical support surrounding problems or training and guidance for software, these helpdesks can impact individual level performance. Therefore, this centralizing and decentralizing of IT structure could potentially influence individual employees' performance, not only when teleworking but also when working in a centralized building. This then, is not necessarily something that is definitely different for the forced teleworking situation due to the coronavirus, however it is also something that can be generalized to regular work practices from the office.

4.4.2. Workforce relations

During the interviews, many respondents made remarks with regards to what could be classed as workforce relations. This finding clusters multiple different topics that all relate in some way shape or form to the relationships employees have with one another and are classed under the theme of individual work practices. As discussed above, the presence and interactions of co-workers with one another is important in the performance of the individual employee. In addition, according to Lippe and Lippényi (2019) manager-reported team performance also suffers from the absence of physical access to co-workers. Therefore, it is important to understand how relations between employees are experienced. In addition, two of the three proposed steps for creating cybersecurity in practice by Pastore (2016) are focused on the sharing and communicating of data. Since Lippe and Lippényi (2019) has already shown that the sharing of data and knowledge is an important factor in both individual and team success, this process needs to be safe but very efficient.

Given this sharing dependent performance and the importance of securing it, it is interesting to see how Gerda, working for a university of applied sciences sees mutual trust as an important factor. As a functional controller, one of her tasks is that she has to grant access to teachers that want to view exam questions prior to the exam being offered to students. When asked about how this process works, she answered the following:

> "If somebody says he or she doesn't see the course and reports it, then I trust that person and believe that he or she actually has the right to access the course. That is all in good faith. I do not have a list of examiners and their corresponding courses. That is all in good faith."

The expression of this seems to show that Gerda works in an environment where workforce relations are shaped in such a way that these decisions can be built on mutual trust. Another good example of this is in how Gerda's co-workers enforce company policy. When Gerda was asked how her co-workers responded when she forgot to take her laptop home with her at the end of the day, one of her employers' regulations, she said that her co-workers confronted her about that. "I have been addressed by my co-workers regarding that the first time I did that. And since then I have always taken it with me." These two quotes not only show that Gerda works in an environment where mutual trust is an important pillar, however it also shows that there seems to be mutual surveillance of co-workers in relation to cybersecurity. The absence of this mutual surveillance in a teleworking situation can also mean the absence of necessary precautions in the field of cybersecurity.

Another example of co-workers holding each other to standards set by their employer can be found at Elizabeth's workplace. At her workplace it is required by all employees that when you leave your workplace, you lock your computer. This is because of the fact that people from outside of the company can have access to the same rooms as the employees work in. To keep external eyes away from this data, all employees are required to lock their computer screen when leaving their desk. When this does not happen, some departments have made their own rules amongst co-workers: "Some departments have, if you spot somebody who forgets it, that you have to buy treats for the entire department. So in that way they try to, well, they try to put it more into people's consciousness instead of setting harsh penalties for it." All of these fragments and academic literature clearly show that workforce relations can be important in mitigating potential cyberthreats but can also create dangerous settings. Understanding these practices in light of teleworking shows that there are two dangers brought forth by working from home that do not, or to a lesser extent, occur when working at the office. Firstly the increased communications needed when working from home create to adequately protect these communications. Secondly, the absence of co-workers also means the absence of mutual surveillance. Therefore practices that aided in making the workplace a more cybersecure place, are lost when working from home.

4.4.3. Workplace security

Elizabeth’s previous quote does not only give information regarding the relations the workforce at her company has with one another, it is also a subtle reference to workplace security. The reason why the rule of having to buy an entire department treats because you left your computer unlocked is instated between employees is due to the fact that data breach is a valid threat at that office. This threat is primarily caused by the presence of people from outside of the organization inside of the building. This threat is a good example of the returning theme of workplace security in the interviews with the respondents.

Derek for instance talked about how at his office, he needs a security card with RFID chip to be able to access his workplace: “Behind the elevator shaft there is a door that you open with your card. Just a regular RFID chip.” Gerda’s workplace was the same, however more intricately secured. When asked to describe how she enters her office in the morning she said that talked about entering the building she works in at street level:

> “And you can only enter there with an employee card. That gives you access to the location. In addition to that you also have different authorizations for different floors. So you need to have access per floor as well. And we requested that access. So at the moment I go to my workplace, I first have to validate my employee card, after that I could enter the building. And the moment I want to go to a secured floor, I had to open each door with my employee card. In addition to that, my office was also locked with the card.”

These two examples show the lengths companies go to in order to protect their workplaces from intrusion. Elizabeth’s workplace will have had some similar way of protecting against this, but due to the nature of the operations of the company, a possibility of external presence was normal.

Since the current situation dictates that where possible employees should work from home, this locational security aspect is impaired and a different situation becomes apparent. Even though working from home for may feel as safe as working at the office, the interviews provided evidence to support the contrary. Charles for instance, works at the same table as his girlfriend does, however she does not work for the same company he does. “No, we have a separate table in the apartment, and we both sit at this table. That’s pretty cramped, but luckily we both have two monitors.” Elizabeth experiences a similar situation where her housemates have access to restricted documents: “Well I must say that when my housemates walk in, I don’t immediately have the urge to minimalize my PowerPoint window. Whilst of course they are not authorized to see the data in that presentation.” In addition to that, Frank, who like Gerda works for a university of applied sciences, touches on this subject as well when answering how his workplace at home looks. “… But I do change it up with the living room where my housemates are also working or studying. It is better that way.” These practices, or maybe the lack thereof for Elizabeth’s case, show that working from home can clearly increase risks to cybersecurity, depending on whoever lives with the employee.

The data Frank handles on a day-to-day basis is not as delicate as Gerda’s, Elizabeth’s or Charles’, however it does show that even though a company may go to great lengths to minimize the dangers of external people viewing sensitive data, the individual employee working from home does not. This is something that is also discussed by James and Griffith (2013) and is also mentioned in the report by Deloitte (2011). These sources speak of two specific dangers when it comes to teleworking and security. The first of which is that security controls in teleworking situations are weaker than at the corporate office (James & Griffith, 2013). This clearly shows in the fact that even though Frank’s, Elizabeth’s and Charles’ people they are living with would not be allowed in the same building or office they work in, they are able to view sensitive data on their computer screens when at home. This means that these findings indicate that the danger of confidentiality breach is higher in teleworking situations than it is in a corporate setting, as proposed by Deloitte (2011) and James and Griffith (2013).

4.4.4. Niche practices and technical differences

The experiences described above seem to be relatively generalizable across the different employers the respondents have. This is to say that even though the individual experience may differ from respondent to respondent, most of the practices can be found in some shape or form in each company. Inside these overarching themes however, there were also some experiences that related only to the specific niche the respondent works in or relating to the personal situation of the respondent. For instance, in Derek’s case, there was a special safe practice in place that made him use dummy data to test the applications he builds:

> “I just have my, err, but those aren’t systems that contain data, that is fake data we make ourselves. … We are there to build the technique and the flow, so in my specific case for the API Gateway, I have to send a message that fulfils the specification but with 1234567 as social security number and random gibberish as name.”

In this case, there is special regulations in place in order to prevent possible data breaches when Derek tests the application he built. This is a phenomenon not seen in any of the other respondents’ interviews. Another interesting finding that was only found in one of the interviews is a Coronavirus related personal circumstance that is linked with Gerda. Due to fears of being infected with the Coronavirus, she decided to do her grocery shopping in the middle of the day, during work hours. She made this decision so she can do her shopping when the grocery stores are less crowded, however this means she is not working for some time during the afternoon. This specific behaviour was classified as fear induced work breaks and presented in the following manner:

> “So when I was logged in, I would leave for about an hour to do grocery shopping. But that was more because I was so scared, and I was hoarding a little bit, so I wanted to avoid the busy hours of the grocery stores. So in the beginning I did that, but I don’t do that anymore.”

This does not necessarily have specific overlap into the field of cybersecurity when teleworking, but it does illustrate one of the points Donnelly and Proctor-Thomson (2015) make. They stated that based on their research into forced teleworking after an earthquake, the fact that the earthquake happened seems to raise pressures on people and family life. This raised pressure can then in turn lead to less safe practices in the field of cybersecurity. The current situation with forced teleworking due to the outbreak of the Coronavirus is not exactly the same as the aftermath of a devastating earthquake, however the point could be argued that the situation is frightening and adds pressure on personal and family life. This in turn could then, like Donnelly and Proctor-Thomson (2015) suggest, lead to less safe practices.

The final point that needs to be made is the fact that dependent on the job performed by the respondents, there were different digital skills taught and expected. All respondents worked with some form of Microsoft Office on a daily or at least weakly basis. There seemed to be an expectation that all employers have of their employees, which is that employees know, understand and are able to effectively work with programs such as Word, Excel and PowerPoint. In addition, it appears that there is a difference in the knowledgeability of these programs that changes per employee. Elizabeth noted this as well in answering a question regarding the level of technical training provided by her employer: "Well, the average age of our company is somewhere in the mid-forties. And I feel there is a lot of difference in how people use PowerPoint and those kinds of programs, versus my generation."

This quote highlights the fact that even though many employers expect a certain level of literacy when it comes to these programs, there can be big differences between the skills individual employees possess. The notion can therefore be made that training in the field of software is not necessarily provided for in a balanced way for all respondents. When Heidi was asked about how she was taught to use the systems she needs for her job she replied: "All systems were explained. The first two weeks were a real onboarding, where we received knowledge sessions." This means that for the use of the systems specific to the bank Heidi works for, there is special training provided. However, when it comes to the usage of other systems, there is no mention of training. Anna, working for a different bank, explains that her employer expects her to be able to work with the basic software on a computer without training: "… Just the basic handling of computers, that is expected of you." When it comes to the e-mail client she uses, she makes the following interesting remark: "I do send a lot of e-mails. And that has not really been explained to me. Well, maybe a little because we work via e-mail a lot. And everybody can, at least a lot of people can just send an e-mail."

This final quote provides the best overview of this situation. The training of employees to work with systems specific to the job the employee has seems to be in order. The danger however becomes apparent in the usage of software that the employee is expected to be able to work with. The possibility here is that cybersecurity is affected by the incorrect usage of systems the employer expects the employee to be able to work with, without any training.

All the subthemes discussed under the overarching topic of individual work practices therefore show that practices are dependent on the location where the employer works, being in an office setting of in a teleworking setting. In addition, the subthemes show that where there are many practices shared between all respondents, some respondents have practices that are specific and unique to them or their work.

4.5. Practices that act as a catalyst for cyberthreats

4.5.1. External interference

The final overarching theme that was found in the interviews is classified as practices that act as a catalyst for cyberthreats. These practices, found in both a teleworking setting and in an office setting, can create danger or dangerous situations for both the company and client privacy. The focus here lies on the dangers that are created from teleworking, such as internal interference and the interference leisure usage of devices can have on cybersecurity.

Even though it is not possible to definitively state that teleworking is the reason behind increased data breaches, it is clear there is a connection. As Gordon (2020) puts it: "industries with low levels of remote working such as manufacturing and public sector organisations do not show a major increase in breaches in comparison with sectors that have higher levels of remote working such as professional services." (Gordon, 2020, p. 14). Gordon (2020) provides some reasons why this could be the case and gives an overview of potentially dangerous practices that can lead to these data breaches in a teleworking setting. One of these reasons is external interference.

This topic of external interference is also experienced by many of the respondents of the interview. One of these external interferences has already been discussed regarding the housemates of Elizabeth and Frank, who both have potential unauthorized access to restricted documents, primarily due to the location both of the respondents use to work from. Derek also gives a clear example of how a work location that is not in an office setting could lead to a data breach due to restricted information being picked up by people other than co-workers. This is not so much a cybersecurity issue as it is a privacy issue however, it does clearly show the point that employees should be mindful when handling private information in a public setting.

> “In fact, a short time ago I had to, this was before the Corona crisis, I needed to access my e-mail. Only at that time the external login was down. That took a couple of days so it bothered a lot of people. So I went to a waiting room of a local office in the city near me. Next to me a co-worker from operations sat down who had exactly the same problem. She had to reschedule an appointment because her son had fallen ill. But she was just talking about a client with full name and credentials in the waiting room.”

So the sharing of information over the phone, even when the other person on the call is allowed to hear the information discussed, can lead to a breach of data and privacy, due to unauthorized people overhearing the conversation. Heidi’s bank actually has some information regarding this. She explained that even though there are no definitive rules set for working from home, she is supposed to consider specific privacy and data security issues: “Well, it’s more of you know, don’t put your 80 inch television in front of the window so your entire neighbourhood can read who’s account you are viewing.” This is also something that Anna recounts in the interview:

> “If during work, so to speak, somebody breaks in or looks through the window, now I do not live in an apartment that has direct sight from the street, but then it’s no longer about me, its more for other people. For instance, if you live in a large family or a dorm. You know, this is maybe less applicable to me, but those are things that you need to be conscious about. Be extra aware that if you go out for a walk you really lock your laptop so nobody can walk in and view your screen.”

This means that at least some of the respondents, and some of the employers of the respondents are aware of the dangers of external interference during teleworking. This is in line with the suggestion made by James and Griffith (2013) and the Deloitte rapport (2011) that suggest that a large danger of teleworking is the breach of confidentiality caused by outsiders having unwanted or unexpected access to the remote workplace.

4.5.2. Leisure interference

Another of these dangers that was found to be a recurring theme in the interviews is the interference leisure has on teleworking. Hilbrecht et. al. (2013) suggests that when teleworking, the actual performance of work activities has to be demarcated from the rest of the day, and rest of the home environment. This is in line with Johnson et. al. (2007) in suggesting that when teleworking both social life and work life can penetrate each other leading to negative results in both fields. This means that work seeping into leisure time can be experienced as a negative consequence of working from home but at the same time, leisure seeping into work can lead to negative work output. For both these proposed phenomena evidence was found in the interviews. Heidi for instance explained that she would go do grocery shopping or doing the laundry when she was supposed to be working. Britta also notices the entanglement of private and professional life, and also sees that as something negative:

> "Well what I notice is that work and private life are starting to intertwine too much with each other. Despite having a separate working space. What I notice now is that the time, your commute is usually the time that you switch off from work and return to your home situation."

Charles gave a rather remarkable reference to this entanglement when asked. He stated that he should actually be working at the time the interview was performed, but he was working on a bike whilst participating in the interview via a headset plugged into his phone. "Err, well yes, so I'm technically working right now haha. But I'm also working on a bike. So I'm not sure whether I have a clear separation or not." All these references clearly show that the border between work and private life seems to blur during teleworking.

In addition to this entanglement of professional and private life, there is one other activity that has to be discussed in order to give a better understanding of the effect of leisure practices on cybersecurity. This activity is classed as uncontrolled device usage and presented itself in the interviews primarily in two ways. Using a work device for leisure and using a private device for work operations. The latter has already shortly been touched upon, when discussing the fact that Frank preferred to work on his own MacBook instead of his work-issued Windows laptop. Another example of this is Gerda having multiple WhatsApp groups with her co-workers connected to her personal phone and private number.

Furthermore, these issues can actually also be caused by regulations specifically in place to protect data. Britta for instance, talks about how her not being allowed to install her own printer on her work laptop means she has to work via her private computer: “Well, what is difficult is that on my, on the laptop that I have from work, I cannot install my home printer. So if I want to print something, than I have to first send it to my private laptop before I can print it. That is really difficult.” Now this may seem like innocent behaviour however the implication here is that possible restricted information is stored on unrestricted devices. Personal devices are by nature outside of the scrutiny and supervision of the employers’ security measures.

The other side is using a work device for leisure activities. Elizabeth for instance, uses the same computer for her work operations as well as her leisure activities. When talking about how her work spills over into her leisure time she makes the following remark about her laptop: “I really have to force myself that I, when I want to watch Netflix at night, that I close all my work tabs in my browser. Sometimes I have up to twenty tabs open if I have to do some research. So I don’t think, oh I still have to do this tomorrow.” Another example is provided by Charles, who is trying to find a different job. With the regulations regarding the Coronavirus, his job interviews are no longer face to face, but via Zoom meetings, and his work-issued laptop has a better camera than his personal laptop: “Err, well, for instance I for the Zoom meeting of last week, for the job interview, I just did it on that laptop. It just has a better camera.”

These quotes show that employees definitely are using the company issued hardware for non-work-related activities. Therefore, the results seem to strengthen the findings by Peacey (2006) in stating that leisure time usage of a work device is a dangerous practice. Furthermore, the notion that compromises to system and data integrity are higher in teleworking (Deloitte, 2011; James & Griffith, 2013) also seem to be supported by these results.

Both the subtheme leisure interference and external interference show practices that can be detrimental to cybersecurity. Interestingly, these subthemes are constructed of practices that are found more often in teleworking than in working from an office setting.

This seems to suggest that teleworking does add some relatively more dangerous practices to employees practices surrounding work, whilst at the same time dangerous practices that were already present at the office, are carried over.

5. Conclusions

This thesis started by posing the question of how the transition to teleworking due to social distancing measures surrounding the coronavirus has changed cybersecurity. This question is divided into both a 'normal' situation of working in an office setting and a 'new' situation, where there is forced teleworking due to the coronavirus. The results show that there are specific factors at play which can be divided into the themes of organisational preparedness, practices that mitigate cyberthreats, individual work practices and practices that act as a catalyst for cyberthreats.

First, organisational preparedness. The two most important findings that were discussed under this overarching theme were the influence of digital diversity and office settings and regulations. Both these subthemes give an overview of the level of preparedness in a more static setting. That is to say that these themes are made up out of practices that do not change depending on whether an employee is teleworking or working in an office setting.

Organisational preparedness can be found in the proactivity of a company in enforcing security regulations and using two sets of eyes for potentially dangerous adaptations. In this a company safeguards itself against human element, which is seen as the weakest element in cybersecurity (Conteh & Schmick, 2016; Groen, et. al., 2018). In addition, organisational preparedness can also be found in the ability of IT departments to support and secure various different forms of hardware and software. Possessing this ability shows that the company has a well-rounded defence against cyberthreats and enough and diverse in-house knowledge to deal with a plethora of technical issues on the spot. This gives off a signal that shows the company is serious about the preparation it needs against cyberthreats (Gordon, 2020; James & Griffith, 2013; Peacey, 2006). Therefore this overarching theme does not focus on the actual transition from working in an office setting to teleworking but it shows the environment in which this transition takes place.

The second overarching theme combines the special practices in action in order to mitigate cyberthreats. Interestingly only a small portion of these specific practices are created for teleworking situations. Most of these practices originally stem from a setting of working in the office and are currently carried over to a teleworking setting. This suggests that either there is no strong pressure on employees to change the practices they have developed in an office setting, or the practices they have developed in an office setting are adequate for the tasks performed when teleworking. Subthemes like the gatekeeping of sensitive data and the existence of company regulations both of which are in line with Gordon (2020), are clear examples of this.

The access to IT services and the productivity of teleworking are also classified under the overarching theme of practices that mitigate cyberthreats because of the practices that constitute these subthemes. When looking at access to IT services, it becomes clear that the accessibility of IT services seems to be a factor in how employees respond to technical problems. As shown by Galvin and Sunnnikka-Blank (2016), practices are driven by the wanting of a human to perform a certain task. From the interviews it appears that in situations where IT support is inadequate, employees do not want to use and need this support. Therefore, employees start working around technical problems instead of solving them, creating possible new cyberthreats. With regards to the transition to teleworking this means that when the distance between IT support and the employee is increased employees will have a tendency to start working around technical issues instead of solving them.

An interesting point of further research has to be added under the overarching theme of practices that mitigate cyberthreats as well. From the performed interviews it appears as if literature on employees being interrupted in their work, like Bloom et. al. (2015) and Van der Meulen (2017) are correct in stating that working from home is more productive, but only if employees are less interrupted. Since these interruptions can have such a significant effect on employee performance, it seems an interesting point to research whether these interruptions also have an effect on cybersecurity practices. It could be suggested that the increased possibilities of digital communications lead to more distractions and interruptions at work, and therefore create potential cyberthreats. On the other hand however, increased communication can give way to mutual surveillance between employees, potentially mitigating this risk.

The third overarching theme, individual work practices, focusses more on the physical features of both the regular workplace and telework place as well as the relations surrounding the workforce. The subthemes and practices that they are created out of show that there are clear differences between the physical workplace at work and the physical workplace when teleworking. These differences mean that firstly there are different practices in action, and secondly there is a need to change practices in order to cope with these locational differences.

The working environment is the first subtheme discussed in relation to these individual work practices. What becomes clear here is that practices can be shaped by both the physical working environment employees work in as well as the organisational shape of the company the employees work for. The second subtheme making up individual work practices is workforce relations. As described above, two of the three steps proposed by Pastore (2016) to create a secure cyberenvironment are focused on the sharing and communicating of data. Therefore, these workforce relations are an important factor in creating a cybersecure environment. With regards to the transition of working from an office setting to teleworking, this implies importance implies two things. Firstly, since the means of communication changes to solely digital when teleworking, this poses a threat to cybersecurity. Secondly, the absence of co-workers in the telework place also means an absence of mutual surveillance, which can be detrimental to cybersecurity.

The third subtheme, workplace security, seems so obvious it could easily be forgotten. Transiting from working in an office setting to working from home means that all the physical workplace security was in place, now remains unused. This is fully in line with James and Griffith (2013) in stating that security controls in teleworking situations are weaker, and therefore the risk of data breach is increased. In addition, it is important to note that even the composition of households where employees work from can be of influence here.

The fourth and final subtheme under individual work practices is classed as niche practices and technical differences. This subtheme zooms in on specific practices that are special or unique to specific respondents. The most interesting finding here is a respondent mentioning fear as driving force behind specific actions. This fear could add pressure to the personal and family life of employees. In turn, like Donnelly and Proctor-Thomson (2015) suggest, this could then lead to less safe practices when working. Therefore, it is important to understand the reason why a transition is made to teleworking, since this driving force can influence not only the location employees work from, but also the emotional state of the employees.

The final overarching theme, practices that act as a catalyst for cyberthreats clearly shows the threats to cybersecurity teleworking practices can create. These threats are created by external and leisure interferences. Both these interferences come from outside of the working milieu. That is to say, neither of these findings are primarily created by co-workers or the employer, both are created by either the employees themselves, or their immediate surroundings in a teleworking setting.

As Hilbrecht et. al. (2013) suggests, it is important to make a clear distinction between performing activities that can actually be classified as work, versus the what an employee does the rest of the day. In addition, there also has to be a distinction between a telework setting, and the home environment. This since the penetration of social life in working life can have negative effects in both fields (Johnson et. al., 2007). The practices found under the two aforementioned subthemes show that this is correct, at least from the social life towards working life. The transition to teleworking can definitely negatively affect work performance and therefore cybersecurity.

6. Bibliography

6.1. Academic

Bloom, N., Liang, J., Roberts, J. and Ying, Z., J. (2015) Does working from home work? Evidence from a Chinese experiment. *The Quarterly Journal of Economics*, 165-218.

Brennen, B. (2017). *Qualitative research methods for media studies* (2nd ed.). New York: Routledge.

Bryman, A. (2008). *Social Research Methods.* Oxford University Press.

Conteh, N., Y. and Schmick, P., J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31-38.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21.

Deibert, R., J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32*(4), 411-424.

Deloitte (2011, July). *Next Generation Telework: a literature review*. https://melbourneinstitute.unimelb.edu.au/assets/documents/hilda-bibliography/other-publications/2011/Next_Generation_Telework-A_Literature_Review-July_2011.pdf

Dockery, A. M. and Bawa, S. (2018). When two worlds collude, working from home and family functioning in Australia. *International Labour Review(3)*, 157. 609-630.

Donnelly, N. and Proctor-Thomson, S., B. (2015). Disrupted work: home-based teleworking (HbTW) in the aftermath of a natural disaster. *New Technology, work and employment*(30), 1, 47-61.

Evans, M., Maglaras, L., A., He, Y. and Janicke, H. (2016). Human behavior as an aspect of cybersecurity assurance. *Security Comm. Networks, 9*, 4667-4679.

Ford, R, (2006). Organizational learning, change and power: toward a practice-theory framework. *The Learning Organization, 13*(5), 495-524.

Galvin, R. and Sunnikka-Blank, M. (2016). Schatzkian Practice Theory and energy consumption research: Time for some philosophical spring cleaning? *Energy Research and Social Science, 22*, 63-68.

Gordon, S. (2020). Securing workers beyond the perimeter. *Network Security*(1), 14-16.

Groen, B., A., C., Triest, S., P. van, Coers, M. and Wtenweerde, N. (2018). Managing flexible work arrangements: Teleworking and output controls. *European Management Journal 36*, 727-735.

Gutzwiller, R., S., Fugate, S., Sawyer, B., D. and Hancock, P., A. (2015). Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting: *The Human Factors of Cyber Network Defense*, 322-326.

Heidenstrøm, N. and Kvarnlöf, L. (2018). Coping with blackouts: a practice theory approach to household preparedness. *Journal of Contingencies and Crisis Management, 26*, 272-282.

Hermanowicz, J., C. (2002). The Great Interview: 25 Strategies for Studying People in Bed. *Qualitative Sociology, 25*(4), 479-499.

Hilbrecht, M., Shaw, S., M., Johnson, L., C. and Andrey, J. (2013). Remixing work, family and leisure: teleworkers' experiences of everyday life. *New Technology, Work and Employment*(2), 28, 130-144.

James, P. and Griffith, D. (2013). A secure portable execution environment to support teleworking. *Information Management & Computer Security*(3), 22, 309-330.

Johnson, L., C., Andrey, J. and Shaw, S., M. (2007). Mr. Dithers Comes to Dinner: Telework and the merging of women's work and home domains in Canada. *Gender, Place & Culture*(2), 14, 141-161.

Kabanda, S., Tanner, M. and Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of organizational computing and electronic commerce*(28), 3, 269-282.

Kissler, S., Tedijanto, C., Lipsitch, M. and Grad, Y., H. (2020). Social Distancing strategies for curbing the COVID-19 epidemic. *MedRxiv Preprint,* 1-21. doi: 10.1101/2020.03.22.20041079

Kvale, S. (1994). *InterViews: An introduction to qualitative research interviewing*. Thousand Oaks, CA, US: Sage Publications, Inc.

Lapierre, L., M., Steenbergen, E., F. van, Peeters, M., C., W. and Kluwer, E. (2016). Juggling work and family responsibilities when involuntarily working more from home: a multiwave study of financial sales professionals. *Journal of Organizational Behavior,* 37, 804-822.

Lewin, K. (1951). *Field Theory in Social Science.* Harper & Row.

Lippe, T. van der and Lippényi, Z. (2019). Co-workers working from home and individual team performance. *New Technology, Work and Employmet(1)*, 35, 60-79.

Lloyd, A. (2010). Framing Information Literacy as Information Practice: Site ontology and Practice Theory. *Journal of Documentation, 66*(2), 245-258.

Lupton, P. and Haynes, B. (2000). Teleworking – the perception-reality gap. *MCB University Press 18*(7), 323-327.

Malatji, M., Von Solms, S. and Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security, 27*(2), 233-272.

Meulen, N. van der. (2017) Does remote working really work? *RSM Discovery 29*, 20-22.

Muegge, S. and Craigen, D. (2015). A Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks. *Technology Innovation Management Review, 5*(6), 6-16.

Nicolini, D. (2012). *Practice Theory, Work, and Organization.* Oxford University Press.

Pastore, J. (2016). Practical Approaches to Cybersecurity in Arbitration. *Fordham international Law Journal*(1), 1023-1032.

Peacey, A. (2006). Teleworkers – extending security beyond the office. *Network Security*(11), 14-16.

Pridmore, J., H. and Oomen, T., A., P. (2020). A Practice Based Approach to Security Management: Materials, Meanings and Competence for Trainers of Healthcare Cybersecurity. *Manuscript submitted for publication.*

Shove, E., Pantzar, M. and Whatson, M. (2012). *The dynamics of social practice: Everyday life and how it changes.* Thousand Oaks CA: SAGE.

Smircich, L. (1983). Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly, 28*(3), 339-358.

Strauss, A. & Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park: Sage Publications.

Ter Hoeven, C. L., Zoonen, W. van, and Fonner, K., L. (2016). The Practical Paradox of Technology: The influence of communication technology use on employee burnout and engagement. *Communication Monographs, 83*(2), 239-263.

Toffler, A. (1980) *The Third Wave.* New York: Collins.

Vieane, A. (2016). Proceedings of the Human Factors and Ergonomics Society 2016 Annual Meeting: *Adressing Human Factors Gaps in Cyber Defense*, 770-773.

Whitworth, B. (2009). A brief introduction to sociotechnical systems. In Khosrow-Pour M. (Ed.). *Encyclopedia of Information Science and Technology,* 2nd edition, 394-400. Hershey, PA: IGI Global.

6.2. Digital media

Banjo, S., Yap, L., Murphy, C. and Chan, V. (2020, February 3). *The Coronavirus Outbreak has become the World's Largest Work-from-home experiment*. TIME Business. Retrieved from: https://time.com/5776660/coronavirus-work-from-home/

Terry, M. (2020, April 2). *Compare: 1918 Spanish influenza Pandemic versus COVID 19.* Biospace. Retrieved from: https://www.biospace.com/article/compare-1918-spanish-influenza-pandemic-versus-covid-19/

Wakefield, J. (2020, April 2). *Zoom boss apologises for security issues and promises fixes.* BBC News. Retrieved from: https://www.bbc.com/news/technology-52133349

7. Appendix

Appendix A: Interview Guide

Focus Area	Questions
Internal (Working in the office) - Materials - Competences - Meaning	Could you tell me about the office you work in? What's the setting like and what kind of environment is there? - What does your team look like? - How does your office look like? - What kinds of digital devices do you use? - In what ways are you taught new skills?
	Could you tell me about the computer and systems you use at work? - How are IT devices regulated and given out? - What kind of digital environment do you work in? - How do you share data with co-workers or different companies? - How is your security set up? - How do you use communications software? - Have you ever had problems with the computers and systems you work with?
	Could you tell me about the training or guidance you received when you first started working with the systems you use? - Are there basic expectations of you and your co-workers when it comes to certain digital programs? - What kinds of training do you receive for new or different software? - What kinds of guidelines for IT do you have and how are these enforced? - In what way do you deal with IT problems? Do you google search, is there an IT department?
	How responsible do you feel for acting in a (Privacy/Data) secure way? Why is that? - How much of this responsibility is actually yours? - Do you have certain fears that drive you to perform tasks in a more secure way? - What do you think is the purpose of doing things in this way? - Do you feel that there are certain vulnerabilities in your work that are secured this way? - Are there certain rules or regulations you would like to push back on? Do you feel resistance in some way when you perform tasks a specific way in order for them to be more secure?

	- Do you feel any emotions when actively performing tasks focused on cybersecurity?
Working External (Teleworking) - Materials - Competences - Meaning	Could you tell me about the place you work at now? - What does your home look like? - Do you have a separate room to work in? - Are you living alone or with other people? - What kind of digital devices do you have?
	Could you tell me what the differences are in the devices and systems you use now that you are working from home? - Are you working on your own computer or did the company provide one? - Are you clearly splitting work/leisure? - Do you use systems in a different way now that you work from home? - What kind of programs do you use now, that you did not use when working at the office? - Have you ever had problems with the systems you work with?
	Could you tell me about the training or guidance you received when you first started working from home? - Is there extra information specifically made for this situation? If so, what are the main points discussed? - What kinds of training did you receive for working from home? - Are there clear differences in guidelines while working from home? If so, how are these enforced? - How do you deal with IT problems now that it is more difficult to contact support or IT? - What systems or devices do you miss at home?

	What kinds of differences do you experience while working from home versus working at your office? What kinds of implications does this have for the field of cybersecurity? - Do you feel more or less responsible for cybersecurity now that you are on your own at home? - Do you have certain fears or problems you encountered specifically from home that drive you to perform tasks in a more cybersecure way? - Do you think there are certain vulnerabilities in cybersecurity practices of your work that are increased because you are working from home? - Do you feel that there are certain rules or regulations connected to working from home that you do not agree with or want to push back on? - Do you feel different (emotions) when actively performing tasks focused on cybersecurity when working from home?

Appendix B: Consent Form

CONSENT REQUEST FOR PARTICIPATING IN RESEARCH

For questions about the study, contact:

Rens Buursen
(Deleted Contact Info)

DESCRIPTION

You are invited to participate in research about cybersecurity practices during involuntary teleworking. The purpose of the study is to understand possible vulnerabilities to cybersecurity and data privacy by looking at the differences in practices working from home has during the outbreak of the novel Coronavirus, versus working in the office.

You acceptance to participate in this study means that you accept to be interviewed.
In general terms this means that the questions of the interview will be related to your workflow and security practices both in and out of the office.

Unless you prefer that no recordings are made, I will use a recording device to record the interview.

You are always free not to answer any particular question and stop participating at any point.

CONTACTS AND QUESTIONS
If you have questions about your rights as a study participant, or are dissatisfied at any time with any aspect of this study you may contact, anonymously, if you wish:

Dr. Jason Pridmore
(Deleted Contact Info)

SIGNING THE CONSENT FORM
If you sign this consent form your signature will be the only documentation of your identity. Thus, you DO NOT NEED to sign this form. In order to minimize risks and protect your identity you may prefer to consent orally. Your oral consent is sufficient.

I give consent to be audiotaped during this study:

Name Signature Date

Appendix C: Coding trees

Selective to Axial codes

Selective code	**Organisational preparedness**
Axial Codes	Digital Diversity
	Spreading of Technical Knowledge
	Existence of Technical Knowledge
	Regular Company Operations
	Digital Communication of Practices
	Company Enforced Regulations

Selective code	**Practices that mitigate Cyberthreats**
Axial codes	Indicating Potential Cyber problems
	Special Safe Practice
	IT-guided Security
	Efforts to Improve IT Service
	Mitigating Cyber Responsibility
	Legal implications of security breach
	Assessment of security risks
	Gatekeeping of Sensitive Data
	Personal motivations
	Access to IT services

Selective code	**Individual Work Practices**
Axial codes	Working within a specific environment
	Relations surrounding the workforce
	Physical Workplace Features

Selective code	**Practices that act as a catalyst for cyberthreats**
Axial codes	Uncontrolled device usage
	IT Service Shortcomings
	IT Related Workflow Issues
	External Influences
	Limitations to digital possibilities
	Leisure interference
	Dangerous Fallout
	Corona Related Personal Problems

Axial to open codes

Organisational preparedness

Axial code	**Digital Diversity**
Open code	Differences in Digital Devices
	Digital Devices
	Digital environment
	Personal Device Preferences
	Personal IT Adaptations
	System Requirements
	Telework devices

Axial code	**Spreading of Technical Knowledge**
Open code	Access to IT training
	Buying IT Knowledge
	Delegating IT Training
	IT Training Operations
	IT Training
	IT Knowledge Accessibility

Axial code	**Existence of Technical Knowledge**
Open code	Absence of knowledge
	Centralized Work Knowledge
	Digital Skills
	IT Literacy
	Limited IT Knowledge
	Digital Expectations

Axial code	**Regular Company Operations**
Open code	Changing Company Structure
	Internal Human Resource Regulation
	Company Oversight
	Enforcing Security Regulations
	Fines imposed by Company
	Forcing internal security Policy
	Requirement of personal proactiveness
	Work operations
	Work Structure
	Client difficulties
	Telework Operations
	Telework Structure

Axial code	**Digital Communication of Practices**
Open code	Absence of Communications Device
	Digital Communications
	Distribution of Responsibility
	Problem communciations

Axial code	**Company enforced regulations**
Open code	Company Policy
	Constriction of IT measures
	IT Regulations
	Workplace Security

Practices that mitigate cyberthreats

Axial code	**Indicating potential Cyber problems**
Open code	Difficulties caused by IT security restrictions
	Difficulties caused by privacy restrictions
	Digital Environment Shortcomings
	Time Pressures Cuasing Cyberthreats
	Cyberthreats caused by expectations
	Teleworking IT Threats

Axial code	**Special Safe Practice**
Open code	Usage of Dummy Data for Testing Purposes

Axial code	**IT-guided Security**
Open code	Differences in Internal and External Login
	External Login Security
	Internal Login Security
	Internal System Structure
	Office VPN
	Security Considerations
	Security Regulations
	Teleworking VPN

Axial code	**Efforts to Improve IT service**
Open code	Feedback on IT help
	Financing IT
	IT Maintenance
	IT Corona Adaptations
	IT Flexibility
	Updating Digital Environment

Axial code	**Mitigating Cyber Responsibility**
Open code	Assigned Responsibility
	Distribution of Responsibility
	On the Job IT Training
	Outsourcing
	Taking responsibility for cyberthreats
	Delegating IT Responsibility

Axial code	**Legal implications of security breaches**
Open code	Confidentiality
	Copyright Issues
	Data Sensitivity
	Governmental Regulation
	Legal consequences
	Restricting Personal information
	Client Privacy

Axial code	**Assessment of security risks**
Open code	Determining Security Risks
	Frustrating Processes
	Known Cybersecurity Issues
	Risk Assessment

Axial code	**Gatekeeping of sensitive data**
Open code	Access Auditing
	Absence of digital restrictions
	Absence of outflow checks
	Data Accessibility
	Digital Restrictions
	Position bound authorization

Axial code	**Personal motivations**
Open code	Lack of motivation to perform
	Personal Problem Solving
	Personal Security Motivations
	Professional Security Motivations
	Reluctance to perform
	System Doubts
	Teleworking Discipline
	Telework benefits
	Telework Drawbacks

Axial code	**Access to IT services**
Open code	IT Problem Solving
	IT Confidence
	IT accessibility

Individual work practices

Axial code	**Working within a specific environment**
Open code	Workplace Flexibility
	Workplace
	Internal Tension
	IT Structure

Axial code	**Relations surrounding the workforce**
Open code	Co-Workers
	Co-workers enforcing company policy
	Inflexible Employees
	Absence of Social Pressure
	Mutual Trust
	Telework Co-worker IT Threats
	Work Demography
	Balanced results

Axial code	**Physical Workplace features**
Open code	Physical Data Transfer
	Physical teleworking Issues

Practices that act as a catalyst for cyberthreats

Axial code	**Uncontrolled device usage**
Open code	Personal Device Work Usage
	Work Device Leisure Operations
	Work Device Leisure Usage
	Unauthorized digital device usage

Axial code	**IT Service Shortcomings**
Open code	Imbalance in IT capacity
	Indifference regarding IT issues
	IT Training Absence
	IT Training Shortcomings
	IT Problems Specific to Teleworking

Axial code	**IT Related Workflow Issues**
Open code	Intentional Security Breach
	Breaking Digital Restrictions
	Pushback against ineffective systems
	Pushback on IT regulation
	Working around IT problems
	Work Operations impared by IT Problems
	Work operations interfering with privacy
	Convenience Security Threats

Axial code	**External Influences**
Open code	Concern versus Influence
	External Pressures
	Family Interference
	Partner Considerations
	Teleworking with Roommates
	Trusting Roommates

Axial code	**Limitations to digital possibilities**
Open code	decoupling of IT systems
	Dependency on Software companies
	Interconnected Security Risks
	Connection Issues
	Overloaded network
	Outdated Digital Systems
	Outdated Practices
	Shortcomings of Digital Environment
	Telework Device Absence
	Telework Device Vulnerabilities

Axial code	**Leisure interference**
Open code	Digital Leisure Separation
	Leisure
	Telework leisure separation

Axial code	**Dangerous Fallout**
Open code	Consequences of failure to adhere to regulations
	Dangers of unauthorized data access
	Possible exploitation dangers
	Security Threats caused by IT Problems specific to Teleworking

Axial code	**Corona Related Personal Problems**
Open code	Fear induced work breaks