challenges

MDPI

Article

Challenges of Managing Information Security during the Pandemic

Emelie Mannebäck and Ali Padyab *

School of Informatics, University of Skövde, 54128 Skövde, Sweden; emelie.manneback@gmail.com
* Correspondence: ali.padyab@his.se

Abstract: The COVID-19 pandemic of 2019 surprised information security practitioners in the organizations due to the change imposed on employees' work routines. Employees were asked to work from home, and therefore changes were necessary to reduce information security risks actively. The abrupt change of work environments brought many challenges to the practitioners, which caused them to make decisions regarding organizational information security. This article aims to uncover those challenges through an ethnography study within an organization during the fourteen months of teleworking. On an overarching level, we found four challenges to be of concern: technical security, regulations and policies, employee awareness of security issues, and, finally, preparedness for the new work environment of teleworking. We believe that the challenges brought by the analysis will inspire discussions about the future of research and practice regarding information security management in case of disasters.

Keywords: information security; COVID-19; teleworking

Citation: Mannebäck, E.; Padyab, A. Challenges of Managing Information Security during the Pandemic. *Challenges* **2021**, *12*, 30. https://doi.org/10.3390/challe12020030

Academic Editors: Palmiro Poltronieri and Susan L. Prescott

Received: 25 October 2021
Accepted: 12 November 2021
Published: 16 November 2021

1. Introduction

In mid-January 2020, the public health agency of Sweden [1] reported on their official website for the first time that there was a new virus spreading through China. Because of the problematic situation, a recommendation from the Sweden's public health agency was presented on March 16 [2], which encouraged everyone to work from home to prevent any further spread of the coronavirus. This recommendation would affect information security in many organizations because the pandemic presented new challenges and reshuffled priorities of issues concerning information security [3]. A reason for the potential effect on information security could be that more employees started working from home, and the way employees handled information was new to them [4].

The unprecedented number of employees who started to work from home put immense pressure on the organizations' infrastructure, equipment, and information security [5,6]. For example, the insecure nature of private home networks puts high demands on securing access to the organization's network, and one way of addressing this could be to use encrypted communication such as a virtual private network (VPN) connection. Private networks are estimated to have over 20 connected devices, and an alarming number of these are neither secure nor regularly updated [5]. Ultimately, these devices could compromise the network and make it more accessible for vulnerable points to be exploited during a cyberattack. Beyond the IT-security-related issues with employees working from home, there are also risks regarding information security and how to manage the possibility of employees accessing sensitive information safely from home [7].

Many organizations have implemented various security countermeasures to respond to the teleworking challenges [8,9]. For example, Furnell and Shah (2020) emphasize educating all employees with the necessary knowledge applicable in different situations rather than having a handful of well-educated employees [10]. It is essential to mention that the organization should strive to achieve a comprehensive information security awareness, which starts at the workplace and must be transferred into employees' homes. When

educating employees on information security awareness, one must also examine what is taught, when it is taught, and how employees will likely learn [11]. On the other hand, focusing on the employees is only part of the solution, and the security is only adequate when all countermeasures, including IT security, work in harmony [7,12].

The COVID-19 pandemic significantly impacted employees' working habits, and those changes are likely to last long. The increased popularity of teleworking correlates with the alarming surge of cyberattacks, making it challenging for organizations to ensure information assets are well protected [9,10,13,14]. However, research in this area lacks empirical studies on how such challenges surfaced during the practice of managing information security during the teleworking shift of the COVID-19 pandemic. Thus, this study examines the effects of changes to the work environment on information security during COVID-19 within a group of IT professionals in the healthcare sector. The study is carried out in collaboration with a special unit within one of the biggest counties in Sweden that specializes in IT and supports many departments with, e.g., their information systems, risk analysis, system development, and procurement of technical-medical equipment. Therefore, this study poses the following research question to fulfil the study's aims: How has the abrupt change in the work environment and processes affected information security during COVID-19? This research takes us on a journey of the challenges experienced by an organization in practicing information security for over a year of teleworking. The research contributes by providing knowledge on handling abrupt changes in the work environment and processes while safeguarding information security.

2. Background

2.1. Information and IT Security

Information security is meant to ensure business continuity and minimize potential business damage by limiting the impact of security incidents [15]. Organizations of all sizes handle large amounts of information, which means that they need to apply various technical and administrative measures to uphold an optimal level of confidentiality, integrity, and availability of information [16,17]. Confidentiality itself is defined as the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Moreover, the definition of integrity is coupled with the property of accuracy and completeness. Lastly, availability is defined as being accessible and usable on demand by an authorized entity. Ultimately, information security is the protection of information and its critical elements, such as any system or hardware that uses, stores, or transmits information [16–18].

Often associated with information security is IT security, which is a term that encompasses the technology which is meant to support the process of electronically safeguarding the information. If information security is more focused on creating policies and guidelines to protect the assets, IT security is focused on protecting the confidentiality, integrity, availability, and traceability in the information systems [16]. In the digital age, vast amounts of information are processed, stored, communicated, and multiplied across the businesses, authorities, and organizations, small or large, in our society. Information security as a practice also involves the necessary applications and management of appropriate controls to identify and analyze a wide range of threats. Ultimately, information security aims to limit the effect and consequences of information security incidents [17].

Organizations have subsequently implemented information security solutions. However, their effectiveness depends on various technical and administrative countermeasures [19]. Moreover, the users can become a threat to any information security solution, and therefore, they are the weakest link in information security [20].

2.2. Teleworking

The International Organization for Standardization [21] specifies that all types of work done outside the office, including from home, are collectively referred to as teleworking. The importance of ensuring security requirements for teleworking to guard the sensitive

information accessed and passed over the communication links has been discussed by many studies [11,22–24]. One of the most outstanding issues with teleworking is ensuring information security is regarding employees not using a VPN. Another reason for this issue, which is often overlooked, is that many employees share their home space with other people, such as roommates, family, friends, or partners. The potential of these individuals gaining access to an unattended or open computer is a significant security risk. To address this, organizations invest in advanced technology and provide awareness and training programs to teach their employees the proper protocol for teleworking [24].

Because of the COVID-19 pandemic, there was an unforeseen increase of employees transitioning from working in-office to teleworking. In the US prepandemic, around 10% of employees worked from home full-time, and another 20% would work from home from time to time. In comparison, during COVID-19, almost all employees who could work from home began to do so [24]. In the EU, before the pandemic, less than 10% of the employees worked from home daily, compared to 38% by April 2020 [25].

Since the outbreak of COVID-19, the Swedish civil contingencies agency (MSB) has provided guidance and recommendations on teleworking, both for the people within organizations who coordinate the information security work and employees who are teleworking. MSB is a governmental agency responsible for issues concerning civil protection, public safety, emergency management and civil defense before, during and after an emergency or crisis in Sweden. Organizations are recommended to take action and assess their information security practices related to teleworking by asking questions such as [26,27]:

- What rules apply to teleworking and the use of IT systems outside the organization?
- What capacity does the organization have for how many people can work remotely?
- Has the organization adopted continuity plans?

Furthermore, MSB has also provided further information on the proper safety and infrastructure when working from home on their website www.cert.se (accessed on 28 August 2021). On this website, more direct information is provided on the consequences of working from home and what to consider from both the organization's and employee's perspectives. Examples of measures to consider are [5]:

- Only allow users to run approved applications by blocking unauthorized software.
- Ensure the equipment employees use for work at home is up to date (hardware, operating systems, third-party applications, and antivirus signatures).
- All communication with the organization's network and services should be secured by, for example, using VPN.

2.3. Increase of Incidents during the COVID-19 Pandemic

During the COVID-19 pandemic, there has been an increase in incidents regarding information security throughout the Swedish network [28]. Furthermore, in the annual review by the National Cyber Security Centre (NCSC), it is revealed that there has been a record number of cybersecurity incidents that occurred between September 2019 and August 2020 [29]. In addition, researchers at IT security companies report that there has been a 45% increase of cyberattacks directed at health care worldwide, and the healthcare sector tops the list for cybercriminals compared to other industries [7,30]. Concerning Sweden, during COVID-19, the number of cyberattacks has increased by 32% [30].

One reason for the increase in incidents is the transition from working in an office environment to working from home [29,31,32]. Moreover, it has been found that the vulnerabilities of organizations' systems have not increased, but the change in the work environment and work processes have affected the opportunity to exploit the vulnerabilities. The fact that employees work more from home has shifted the attack surface and made it possible for threat actors to succeed more easily with the existing vulnerabilities. In addition, the risk of human error is higher, and many organizations have been forced to come up with solutions quickly to allow their employees to complete their tasks. This ultimately means that the solutions for working from home have not been set up securely [6,31,32].

Specific organizations have been targeted primarily during COVID-19, including hospitals, medical centers, and public institutions. Cybercriminals have used ransomware attacks on these organizations. An example of such an attack is the incident in the Czech Republic on 12 March 2020, which led to the Brno University Hospital being forced to shut down its entire IT network, which also impacted the Children's Hospital and the Maternity Hospital [33]. Furthermore, from the beginning of the pandemic, cybercriminals have carried out social engineering attacks by using themes around the pandemic to distribute various malware packages. An example of this was presented in early 2020 when cybercriminals had started using fake versions of decease spread maps to gain access to personal data stored in users´ web browsers. With this attack, criminals got access to users´ credentials and credit card data [33].

2.4. Research Gap and Motivation

Several researchers have recognized that the crisis of COVID-19 sped up the deployment of new working methods and the adoption of teleworking. Different countries have adapted to the new situation on varying levels, depending on their readiness [34,35]. Organizations that invested effort, time, and sufficient budget into their digitalization avoided greater abruptions to their operations [33]. Research shows that a remarkable number of organizations, due to the crisis of COVID-19, adopted a higher level of teleworking than what they were prepared for [34,35].

Some studies have warned that organizations did not sufficiently equip employees from working in-office to teleworking. A survey study by Georgiadou, Mouzakitis and Askounis [33] aimed to evaluate the cybersecurity culture exhibited by organizations from different countries and business domains when teleworking became a necessity due to the COVID-19 crisis. One of the most stunning results of that study was that 53% of the participants had not received any security guidelines from their employers in preparation for working from home during the pandemic. Perhaps this result reflects that organizations mainly think of information security from technological security solutions, such as firewalls, antivirus software, intrusion detection systems, and security operation centers (SOCs). At the same time, the human factor is overlooked in the context of information security, even though humans and their behavior can make up the biggest threats to information security [33]. Another finding shows that in three-quarters (75%) of businesses, there are no explicit cyber security-framed, written rules that employees are expected to follow when working at home [10]. These findings are compounded by the fact that only 6% of businesses say they are 'open' to investing in cyber security training [36].

The sudden transition from office-based working to working from home dramatically changed the cyber threat landscape, leading to new cyber risks. With employees accessing the organizational resources from private units and networks, governmental agencies, cybersecurity firms, and in-house cybersecurity specialists must outline proper guidelines for the employees working from home [37]. Attempts to set up such guidelines and achieve cybersecurity throughout the organization might fail due to various reasons; among others, the solutions do not consider organizations´ cybersecurity requirements and the expectations of the employees working from home [38,39], or lack of employee support [10].

Previous studies concerning teleworking and information security have researched the topic from different angles. One stream of research has focused on organizational readiness to protect the data from cybercriminals while teleworking [33,40]. In those studies, the focus was on the most common cyberattacks during the pandemic. Among the cyberattacks that have technical origins, ransomware and DDoS were prevalent [7]. On the other hand, the most common techniques for social engineering used are phishing, scamming, spamming, smishing, and vishing [41]. Drawing on the trends of common security vulnerabilities and cyber threats towards teleworking, another stream of research has proposed various security controls that can reduce the risk of cyberattacks while teleworking [39]. To name a few of these controls, user education, VPN, multifactor authentication, firmware updates,

software updates, antimalware software, strong security policies, and the physical security of the home office have been suggested by previous studies [7,10,38].

However, there are several gaps in the literature concerning the cybersecurity challenges of teleworking. Most of the research on teleworking has been focused on the prepandemic era when organizations had the choice, budget, and time required to prepare and facilitate an environment where employees could work from home. Thus, organizations had the opportunity to investigate how teleworking could be secured gradually. However, the COVID-19 crisis imposed the need for the mass transition to teleworking, even organizations unprepared for such a sudden transition. In this regard, the first gap involves the abrupt changes to the organization's information security practices to such changes. Moreover, extant research has paid less attention to the perspectives of employees and those who play an essential role in the rapid adaptability of teleworking. While scholars emphasize recognizing the necessity of investing in human capital to tackle information security threats [35,42,43], previous research in this area is often disconnected from employees' perspectives and how the organizational practices of teleworking take shape. Moreover, there is a discrepancy between formal processes and those used in practice, i.e., the actual processes are shaped within the enactment of day-to-day activities and their respective challenges [44–46]. Therefore, the second gap pinpoints the lack of empirical investigation into unraveling the complexities of information security in everyday teleworking practices during the pandemic.

3. Theoretical Framework

Practice theory is a prominent analytical tool for analyzing contemporary organizations, as it is generally understood to be complex, dynamic, distributed, and transient [47]. The premise of practice theory is the human agency in organizational life that performs activities that share meanings and understanding [48]. The perspective also entails exploring what people in an organization actually do instead of what they are supposed to do [49]. As opposed to the technology determinant views, which "posits technology as an external, largely independent, and irrevocable force for change" [47], the practice perspective explores the implications of information technologies for practices. It offers a distinct conception of when people actually engage with the technology in practice [50].

Various studies show that introducing best practices to an organization does not guarantee the expected results from before (e.g., [51,52]). What matters is knowing in practice; it implies that knowledge(ability) and practices are mutually constitutive "so it does not make sense to talk about either knowledge or practice without each other" [53]. The practice perspective has been employed in various areas within information security, such as risk management [54], policy development [44], and information security training [55]. The results from these studies imply that people in the organizations do not slavishly follow the imposed practices, but information security practices matter when they are enacted in practice (cf. [56]). When information security policy and business requirements conflict, individuals must find innovative ways to address the business requirements while not undermining information security [57].

4. Methodology

4.1. Ethnography

Ethnography is the study of "a group in its natural setting for a lengthy time period, often several months or several years" [58]. Central to the ethnographic approach is the context of practice in which a researcher attempts to investigate. "Understanding actions and beliefs in their proper context provides the key to unravelling the unwritten rules and taken-for-granted assumptions in an organization" [59]. The ethnographic approach in this study allowed us to gain a deep understanding of the people who were somewhat affected by the abrupt change of working from the office to teleworking and how employees perceived information security decisions. Our investigation started in March 2020, when the Swedish health authority gave recommendations to all organizations to switch to

teleworking due to the spread of the Coronavirus. The study continued till May 2021 in which the government waived such restrictions. During this period, one of the authors followed the transition to teleworking and interacted with employees, attended meetings, had conversations with them, and closely followed the information security decisions.

4.2. Research Setting

Our research study setting has been Alpha (a pseudonym), which consists of IT professionals working within one of the biggest counties in Sweden. Alpha provides support for several different healthcare departments, i.e., information systems and IT-dependent medicine technical products. As part of Alpha´s responsibility, it assists other departments with risk management, implementation projects, and procurements of IT-dependable products. Furthermore, employees at Alpha have backgrounds in areas differing from computer engineer to systems science.

The majority of Alpha' staff had been working from home since the spring of 2020 in adherence to the recommendations of Sweden's public health agency. Teleworking impacted these employees' work environments and work processes.

The unit that works with information security within the county, primarily for one of the larger hospitals, states in their guidelines that ensuring the information generated and used within the healthcare must be an integral part of the departments' processes. The guidelines ultimately mean that all people who in some way manage this information have a responsibility to safeguard it. However, when browsing the county´s intranet, most of the information regarding working safely from home is copied from the MSB's website. In some instances, the employees are simply directed to use a provided link that redirects them to MSB´s website. There is, however, some guidance given by the county´s IT department countermeasures to consider before teleworking to safeguard the information. The guidance is given more from the perspective of IT security and not information security.

Because of the laws and regulations to consider with healthcare, while upholding a complex information flow between the municipalities, primary caregivers, private clinics, and patients and staff, it is not easy to maintain acceptable information security. Furthermore, some of the issues with information security in healthcare are that the different parties do not have access to the same information systems and that they might not have the proper knowledge on information security in general, but also on what their technology needs are and what they must do with that technology to preserve, e.g., the confidentiality of their assets. Another issue could be that the departments hold onto old routines, perhaps without a reasonable cause, and then incorporate new technology, leading to unforeseen problems because of mismatch in need and solution [16].

One of the most demanding challenges for public actors is maintaining adequate resources to secure their IT environments, which has led them to deal with different and sometimes contradictory requirements and recommendations from both national and regional levels. The effect of this is that both the work with and the level of attained information security differs significantly among different public actors. Moreover, the challenges build on all operations undergoing a rushed digitalization due to the pandemic [60].

4.3. Data Collection

Below we present the sources and procedure of the data collection. The data were gathered qualitatively using different techniques explained in the following sections. By applying different data collection methods, the study benefited from methodological triangulation, which gives the credibility of the results [61–63].

4.3.1. Internal Documents

Document analysis is a type of qualitative research that applies a systematic procedure to analyze documentary data to answer specific research questions [63], a method used for several years in qualitative research [62]. As with other methods in qualitative research,

document analysis is an iterative process that involves repeated review and interpretation of the data to enable empirical knowledge to be gained [63].

This method is effective because it can provide the researcher with insight and understanding of the roots of the phenomena of the study [62]. The researcher can also apply this data collection method to track change and development by comparing available documents related to the research topic [62]. Moreover, by reviewing periodic and final reports, the researcher can picture how an organization has performed over time [62].

Document analysis can result in citations, quotations, or even complete passages drawn from, i.e., records, correspondence, and official reports [64,65]. Moreover, using data analysis collectively with another data collection method, the researcher can contextualize data collected during interviews by drawing data from documents [62].

Therefore, as part of the data collection, internal documents available to Alpha were analyzed. Internal newsletters were analyzed to understand when the employees started teleworking and which information was given in the process of moving from working in-office to from home. The first newsletter mentioning COVID-19 was published at the end of February 2020, and from 13 March, Alpha started teleworking as much as possible to avoid spreading the virus in the workplace.

Moreover, different websites of the county´s intranet have been reviewed to gain insight into the information available to employees regarding information security and news related to information security during COVID. For example, one webpage (last updated 31 March 2020) provides information on information security during the pandemic. However, this webpage is mainly made up of links to other sites to get advice, information on malicious emails, or incidents linked to information security and COVID-19. An example of one of the external sites that are linked is informationssakerhet.se. This gives off the impression that the county itself has no information of its own to provide but relies heavily on external sources and primarily directs its employees to these external sources.

Available policies regarding teleworking have also been included. One of which deals with teleworking with mobile equipment, and another explains the routine for teleworking within the county. The one about mobile equipment predated the pandemic and was last updated 5 July 2019. This policy only mentions information security once, which is linked to the general policy on information security within the county, which does not even include teleworking. The second routine on teleworking was last updated on 14 January 2019, and in this one, information security is mentioned twice. The main message is that the same degree of information security must be upheld when teleworking as when working in the office, but the focus is on the technical aspect of teleworking. The routines that were in place before the pandemic provided the employees with simple conditions to handle computer and information appropriately when teleworking, which included:

- Not to use insecure networks;
- To use a VPN for communication on the county network;
- Not to lend out any county devices;
- Not to connect any private devices to the county´s equipment;
- Always to lock or shut off the computer when it is not in use;
- Not to use other printers than the ones in the office;
- To be mindful of where in the home to telework (i.e., not angled towards a window).

In addition, tips provided by the county´s IT department were analyzed. These tips are limited to IT security and what the employee should think of when starting to work from home, i.e., they need a computer provided by the employer and access to a stable ethernet connection.

Lastly, guidelines were analyzed to better understand the prerequisites of the employees transitioning from working in the office to teleworking. For example, in March 2020, the county published guidelines concerning how some departments, including Alpha, would work during the COVID-19 crisis. This showed us that the focus was on how the employees would have to analyze their health to help stop the spread of the virus, but the information about teleworking was limited. The county primarily referred to the older

routine mentioned above and the technical requirement such as a VPN connection to access the intranet. Some information was also provided about statutory and contractual rules and insurance, with no mention of information security.

4.3.2. Diaries

The analyzed diaries entail minutes of meetings and thoughts written down in retrospect. The meeting minutes provided insight into the different types of meetings being held and the different parties participating. The thoughts written down in retrospect provided insight into when the pandemic started to affect Alpha, both concerning their work environment and processes. Furthermore, these thoughts included observations of other employees' behavior and actions regarding information security. For example, in some instances, family members of participants in digital meetings could be heard in the background, which would question the environment the employee worked in where sensitive information might be discussed or handled. A complimentary interview was done with another expert within the county, who reviewed and confirmed the findings to minimize the researchers' bias.

4.3.3. Focus Groups

During our data-gathering period, the employees at Alpha were teleworking. Therefore, it was not possible to have conversations with them while working in the office. We sought a technique to involve them more actively. In this regard, a focus group technique is a feasible approach to interview several participants simultaneously [58]. A focus group method is a qualitative data-gathering technique that involves participants in a planned discussion to explore a specific topic [66]. Moreover, the method is an interactive discussion between participants, led by a moderator, focusing on a specific set of issues [67].

The focus group sessions were conducted by a moderator responsible for running the session and guiding the participants through the questions and discussions. This approach requires the moderator to be highly involved to make sure that all participants get a chance to voice their thoughts. Moreover, it is up to the moderator to interject in the discussion and probe for deeper discussions based on the answers when it is appropriate [68]. The level of involvement by the moderator depends on the openness of the research questions [69].

This research method highlights the interaction between participants and what they may reveal about shared ideas, reactions, or opinions on the topic discussed. Furthermore, this allows for the participants to follow up on each other's answers [66]. Typically, for documentation, the focus group sessions are recorded in some way, either with just audio or also with video, which can be done with several types of equipment or tools. This allows for the material to be analyzed once the sessions are concluded. The approach is similar to how other qualitative data collection approaches document their sessions, for example, interviews and observations [70]. In addition, the collected data from these sessions are not limited to the transcripts of the session but may also include notes taken by the moderator, body language, results from debriefing sessions, or any presession questionnaires [66]. Furthermore, the analysis process of the material starts while conducting the sessions, which is done by listening for inconsistent, vague, or cryptic comments [71]. Some additional tips for developing focus group questions are avoiding vague wording, phrasing the questions as open-ended, and designing the questions from general to more specific [72].

The procedure of each session was as follows. First, the facilitator gave a brief introduction to the practicalities of the session. Second, we started the discussion by asking the participants about their experience of working with different platforms during the pandemic and what they think of information security in general. Third, we deepened the discussion on information security practices during teleworking, and the work situation and the work environment have affected information security. Next, we asked the participants how they perceived the guidelines and regulations regarding a secure teleworking environment. The rest of the session was dedicated to understanding information security awareness among the participants. In this regard, we presented them with three scenarios

in which the use of IT systems was deemed risky. After each scenario, we asked them about their reaction to a presented situation and what security risks they see relevant to the case. We closed the session by having a general discussion focused on reflecting upon their attitude toward information security after the pandemic and what improvements they could suggest.

4.4. Data Analysis

Qualitative data from the documents, diaries, and transcripts from the focus group sessions allowed us to create a "thick" description of events concerning the practice of information security for safeguarding teleworking during the data-gathering phase [73]. We sought to question what information security challenges surfaced and how the employees at Alpha reacted to them. Next, we adhered to the guidelines of thematic analysis for coding and reporting the results [74]. The process involves assigning codes to the transcribed data and then grouping the codes into themes for analysis. First, the authors read through the documents and transcripts to understand the events and key activities. Second, the materials were analyzed by applying codes to every passage of the transcript. Next, after coding all contents, the codes were compared to each other, and in case there was an association with each other, higher-order categories were created.

5. Results

Alpha encountered different challenges regarding the secure management of work routines when transferred to a home environment. Those challenges relate to how the organization prepared itself regarding teleworking on a general level. Examples of this are the perceived levels of how good and stable the IT tools and security were at the pandemic's beginning, dealing with rules and regulations, awareness of secure teleworking practices, and, lastly, preparedness after the pandemic. Below we present these challenges in great detail.

5.1. Challenges with the Technical Security

Various IT-related challenges surfaced throughout the teleworking period. The county had many IT tools in place but lacked the means to create a secure teleworking environment. Alpha expressed concerns regarding which tools are deemed secure to use in which situations while the county had not yet had resources to assess all the risks associated with the IT environment. For example, Alpha was using all or some of the same meeting platforms available within the whole county; Skype for Business, Teams, Cisco VMR (Virtual Meeting Room), Zoom, and Cisco Video Conferencing. The work routines dictated them to choose from a pool of various communication tools since various authorities and organizations within the county use different tools. The challenge for Alpha was to answer users' (i.e., other employees within the county) questions regarding the security of different tools and platforms since the tools´ assessments have either not been widely known within the county or simply have not been completed.

> *We get many questions about platforms and whether they are secure or not and what types of information classes they can be used for. And not least considering that we currently have a Skype to Teams transition, which is admittedly paused, and that is one of the reasons why we used Cisco VMR sometimes because we at least got it verbally that it is more secure because the IT environment is here [administered and located within the county and not outsourced].*

On the other hand, participants from Alpha have brought up the issue of employees being confused about which platform to choose since Teams is the standard meeting platform in the county. Therefore, employees had little to no time pondering about the characteristics of meetings and which platform to use since they can only arrange meetings with Teams. The other platforms most often hinge on employees being invited from other parties such as foreign companies, other counties, or authorities.

Another challenge was related to maintaining the same level of protection, because the IT used to telework should be handled in the same way as it would have been in the office; kept out of reach of unauthorized people, locked, and kept separate to the smart card which, i.e., allows connecting to the VPN service. However, Alpha could not manage all aspects of employees´ home offices, as two experts brought up the issue at Alpha:

> *If there is a print queue and paper come out even if the computer is locked.*
>
> *There may be a document waiting in the printer queue that is patient-sensitive and that could be printed with the other documents that the family member wanted to print out.*

5.2. Challenges with the Policies and Regulations

This challenge relates to the rules and regulations in place regarding information security when teleworking within the county. In general, it was observed that the employees had not spent any time before the focus group session to reflect on the rules for teleworking. This finding came as a surprise because cyberattacks have been a hot topic within the county during the pandemic. The situation could be related to the fact that no rules or regulations regarding information security when teleworking could be found on the county´s intranet or that the information was not accessible to all. Instead, employees are expected to act with common sense and adapt their security behavior from in-office to teleworking. This might be a reasonable expectation of employees at Alpha owing to their technical competencies. However, in the broader perspective, this is not sufficient for employees that do not work with information security or questions related to information security. Participants from the focus groups believed that this situation needs to be improved and demanded:

> *Develop a more structured and organized work with information and education in information security for the employees. And how we should act when we work from home.*

However, top-down policies and regulations are deemed part of the solution, and it should be complemented a knowledge-sharing platform where employees and experts can exchange information as a unit. Alpha revealed that they have identified that they too should aim to get better at educating themselves on information security:

> *We belong to a group that has better knowledge of information security than others, but it is important to continue to keep the dialogue open and remind each other of what applies.*

Therefore, other challenges surface when there is no face-to-face contact as opposed to the office-presence which requires good communication between the team members and the team with other employees:

> *Perhaps we should also be better at transferring knowledge, especially to new employees. Then we also need to think about how we can help each other in work on information security when we are not sitting in the same corridor.*

5.3. Challenges with the Information Security Awareness

As part of their tasks prior to the pandemic, Alpha had previously worked continuously to raise employees' awareness regarding information and IT security practices to safeguard the information. However, broadening that awareness to be applied while teleworking has not been a focus. Internally, Alpha has discussed issues related to teleworking from various perspectives, such as IT security and information security. However, they have not identified similar discussions being held in a significant number of Alpha's departments within the county. The responsibility of ensuring that employees follow regulations and policies regarding information security lies with the individual department managers, and they are tasked with following up that their employees follow the established regulations. However, no follow-ups have been made in connecting to the increase of teleworking.

When Alpha transferred into teleworking, its first activity was to re-educate its employees, and the second was to ensure that the organizational awareness would remain effective. However, there were various bumps in the road regarding keeping up with the information security work when working with their users. The previous awareness (i.e., before the pandemic) regarding working securely with confidential information should be transferred to the new way of working. Nevertheless, Alpha had a hard time changing the mindset of the employees so that they were compliant with the best practices. For example, a challenge was to get a message across when working with the patient's data from home:

> *These are the kind of things that you sit at work and have paperwork on patients that you've been given paper, so you can't take them home. The papers are going to stay at work and be locked up. Similarly, it should be with a laptop. You are not allowed to download patient information on a laptop and bring them home to work with them. Then you've taken them out of the workplace. I don't think people are aware that this is the case. There is no awareness of it.*

The most significant challenge for the county regarding rules, regulations, and policies regarding teleworking was to provide clear and easy-to-read rules for the employees to follow while also ensuring that each individual has the opportunity to follow the rules and make a choice to follow them. The process of following up is an integral part of allowing employees to telework, and therefore, the challenge was to involve the managers in this as well.

Moreover, there were some challenges to measuring the effectiveness of information security awareness due to various reasons. One reason was related to the fact that monitoring employees is more difficult in the home environment. Security in the office environment is much more restrictive due to the physical and administrative countermeasures that Alpha could check were in place:

> *I have reflected about how I know who is in the meeting and that no one else is listening. The rooms [meetings] do not have four walls in the same way as physical meetings.*

However, there were uncertainties concerning monitoring if employees apply their security training and education at home. For example, security experts at Alpha could not observe if employees would write their username/password for any tools, platforms, or systems on sticky notes. An expert at Alphas brought up the pre-existing issue with computer locking during lunchtime and how that could escalate when teleworking:

> *Considering how difficult it is for healthcare departments to secure information when people are at work, for example, to lock the computer when you go to lunch, it will not be easier when people work from home.*

5.4. Challenges with the Preparedness

This theme deals with the level of preparedness on information security and teleworking before the pandemic and the continued preparedness for potential issues after the pandemic.

An example of the issues Alpha experienced was that the VPN was not dimensioned for the increased number of users and forced the IT department to quickly upgrade and divide the users into different connections. If the county did not have the tools and culture for teleworking, issues like the VPN might not have been surprising. However, considering the efforts towards digitalization and the many collaborations within Sweden and internationally, this was unexpected.

> *I do not think that instructions or recommendations on how to work at home have kept pace with the change in the work environment. I think there is a lack of information material.*

Furthermore, the focus group sessions revealed a gap in information security knowledge between the participants. When asked, most participants could not define information security, nor what activities they perform in their roles as part of Alpha related to informa-

tion security. The following is an example of one of the answers given when asked how they work with information security:

> *Like a little all the time depending on how you define information security. It is infrequent during a day that it is stated that 'this is about information security'.*

However, a few more experienced employees could give a fair definition of information security and answer what activities relate to information security they perform internally at Alpha, with users, and for customers. In combination with answers given when asked about scenarios regarding teleworking, it was inferred that the participants firstly think about IT security and secondly information security. Consequently, Alpha was more prepared for handling IT security issues than information security-related issues.

Moreover, a subtheme emerged: the new normal. This subtheme was identified through the discussions on teleworking on a broader scale and the fact that many organizations within the county have found ways of continuing working without employees' in-office presence. This new normal state for some departments may not change once the pandemic is over. For example, both from an environmental and economic perspective, allowing employees that spend many hours in meetings to work from home and using digital meeting platforms (i.e., Teams) is quite appealing. It would not come as a surprise if the county makes it a rule to use digital meetings as a first choice and meet face-to-face as a second choice if participants must travel to participate. Furthermore, as can be seen below, the participants in the focus group agreed that this new normal is not something that will go away once the pandemic is over:

> *I have been thinking that it will never be the same after the pandemic because many will not come back [to work in the office].*

Relating to the central theme of preparedness, with the new normal of increased use of teleworking on a broader scale, Alpha anticipated a need for the county to review its policies, guidelines, tools, and education to prevent any incidents regarding information security from occurring. When experts from Alpha were asked if they believed that there would be any incidents in need of handling once the pandemic has passed, one replied:

> *On the other hand, I think it is something that you have to work with and put in place rules about this because I am convinced that sitting at home and working has come to stay. I think there will be a lot of this in the future. And we notice that using these tools for meetings in the region has made it much easier. You don't have to go to meet and such, but then you actually need to reason about the prerequisites to be able to do it.*

In Table 1, we summarize the challenges experienced by Alpha:

Table 1. Summary of the challenges experienced by Alpha during the teleworking period of the COVID-19 pandemic.

Theme	Challenge	Type of Challenge
Preparedness	An unstable and undimensioned VPN	IT security
Information security awareness	Employees have different levels of knowledge regarding a suitable home-office set-up	Information security
Technical security	Difficult for employees to control the unpredictable nature of updates in the home-office environment, i.e., router firmware	IT security
Technical security	Ways of limiting the expansion of the attack surface	IT security

Table 1. *Cont.*

Theme	Challenge	Type of Challenge
Preparedness	Concerns that employees work with insecure private devices due to lack of company-owned devices for employees needing to telework	IT security
Information security awareness	The digital space does not have four walls	Information security
Policies and regulations	Lack of instructions on the proper way of teleworking	Information security
Information security awareness	Too much focus on IT and not enough on behavior	Information security
Technical security	Access email and some internal websites with insecure devices	IT security
Technical security	Monitoring unauthorized communication channels	IT security
Information security awareness	Control the surrounding environment of the teleworker	Information security
Policies and regulations	Lack of defined rules related to information security when teleworking	Information security

6. Discussion and Conclusions

Understanding abrupt changes in the work environment imposed by the COVID-19 pandemic on IT and information security management is crucial, given the consequences of increased cyberattacks globally during this period. Analyzing the challenges of such abrupt changes in security management paves the way towards better preparedness for future crises and a secure transition to teleworking. Our investigation of Alpha during 14 months of teleworking resulted in four broad categories of security management challenges: technical security, rules and regulations, information security awareness, and preparedness. Our study contributed to security research in two ways. First, most studies done in the context of teleworking during the COVID-19 pandemic are disconnected from the organization's context and how practices take form [47]. While prior studies on cybersecurity challenges of teleworking before, this study is among the first that has empirically investigated this topic. Our results give a detailed view of the security challenges that have emerged through the abrupt changes in the working environment. Second, our study complements previous studies by reinforcing the involuntary aspect of teleworking. Previous studies have focused on home-user and telework groups who willingly change the work environment, who might not be necessarily the same, for example, in a pandemic situation in which in-office employees were forced to work from home. Below, we discuss each challenge in the light of literature and the analytical lens of practice theory.

Concerning the technical challenges experienced by Alpha, two aspects seemed prominent. First, Alpha dealt with technical difficulties of teleworking (e.g., accessing and using a stable VPN) that affected all employees teleworking within the county. Second, Alpha had challenges regarding technical security outside its control zones, such as employees' working devices and external organizations. The abrupt changes to teleworking made it challenging to immediately respond to such considerations' various technicalities for technical security controls. Various research has pinpointed the technical controls as a requirement of teleworking [7,13]. However, our research showed that in practice, technical security does not always stem from the organizational premises, but the chain of stakeholders' IT devices and infrastructure should be focused on too. One example is that, despite providing a secure VPN to employees, a simple DNS poisoning attack on the home router will simply circumvent all the confidentiality and integrity security provided by the VPN tunnel. From a practice perspective, our result strengthened the need for more empirical research on practical challenges instead of focusing only on the prescriptions of best practices or what actors aspire to do [75].

Concerning policies and regulations of teleworking, our result shows that policies regarding secure teleworking were perceived differently among the top management

and the employees. On the one hand, managers believed that prepandemic policies and regulations regarding secure teleworking were deemed sufficient, contrary to what employees brought up during the focus group sessions. Moreover, another challenge that could be the reason behind this discrepancy of viewpoints was the lack of follow-up routines to monitor if the teleworking policies were followed. It is crucial to mention that lack of communication from top-down and bottom-up contributed significantly to dislodging the role of the policies and regulations [44,76,77]. Previous studies suggest having policies in place to ensure physically protect home office devices [7,10]. However, the inherent practice challenge we found in a teleworking situation is the difficulty of follow-up if physical home space and working environment comply with the policies.

The major challenge regarding raising employees' awareness of secure teleworking was the county´s overreliance on employees' knowledge of teleworking before the pandemic since the culture of working from home existed at many departments within the county, albeit not all employees had this experience. Such a mindset underestimated the need for new and updated security awareness, mainly ignoring that many employees were working from home for the first time. The result agrees with the low security awareness and training programs during the pandemic [36,37]. Our analysis shows that the challenge lies within a strategic approach towards security management decoupled from organizational practices [78]. While strategic enforcement on protecting high-impact areas (e.g., the confidentiality of patient data) existed at Alpha, devising controls (e.g., security awareness) was not in line with the new means of change in the work environment, i.e., teleworking. Therefore, our result points to the situated challenges and practical resolutions introducing conflicting priorities which is in agreement with the practice theory: shifting of structures must take place in everyday crises of routines and the inadequacy of knowledge with which the agent, carrying out a practice, is confronted in the face of a situation [79]. The contribution, herein, is the challenge of misalignment of security practices with the changing of routines when shifting towards teleworking.

Concerning the preparedness theme found for our empirical investigation, it seemed that Alpha's prior culture of teleworking helped with the forced transition at the beginning of the pandemic. As many scholars agree that teleworking will become a new norm in many organizations [9,10], there is still a lack of knowledge if the management of securing has kept up with the speed of transition. Particular attention should be given to the lessons learned during the pandemic period regarding the effects of IT and information security decisions on the organizations' overall security posture. Our study contributes to this debate by theorizing the interaction between changes to work routines and InfoSec management. The implication of this research is to fill the gap between the challenges that emerge from the practice compared to the prescription of best practices. While the traditional view on security management indicates best practices resemble situated practices [76,80], the combination of findings supports the conceptual premise that it is crucial to account for the challenges that emerge from work practices.

We acknowledge some of the limitations of this study which will hopefully lead to a natural progression of this work. This study was limited to one unit; thus, the findings cannot be generalized. A more extensive sampling would provide statistical generalizations into how organizations have experienced the changes due to the pandemic. One example could be to test whether there is a statistically meaningful relationship between preparedness and security incidents. Future research could look further into how other organizations have experienced changes in information security during the pandemic, how challenges were addressed, and present recommendations for organizations to mitigate the challenges brought by this study. Moreover, our studied organization did not experience any apparent cyberattack during the pandemic. While some cyberattacks are passive and go undetected, it could be interesting to study organizations that experienced cyberattacks during the teleworking period and study the relationship between teleworking practices and cyberattack success.

Author Contributions: Conceptualization, methodology, formal analysis, writing—original draft preparation, E.M. and A.P.; data collection and curation, E.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Folkhälsomyndigheten Nytt Coronavirus Upptäckt i Kina—Folkhälsomyndigheten. Available online: http://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2020/januari/nytt-coronavirus-upptackt-i-kina/ (accessed on 28 August 2021).
2. Folkhälsomyndigheten Personer över 70 bör Begränsa Sociala Kontakter Tills Vidare—Folkhälsomyndigheten. Available online: http://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2020/mars/personer-over-70-bor-begransa-sociala-kontakter-tills-vidare/ (accessed on 28 August 2021).
3. Lanz, J.; Sussman, B. ICYMI | Information Security Program Management in a COVID-19 World. Available online: https://www.cpajournal.com/2020/08/18/icymi-information-security-program-management-in-a-covid-19-world/ (accessed on 28 August 2021).
4. MSB Arbeta Säkert på Distans. Available online: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-sakert-pa-distans/ (accessed on 29 August 2021).
5. Cert Säkerhet Och Infrastruktur Vid Arbete Hemifrån [uppdaterad 26 March 2020]—www.cert.se. Available online: https://www.cert.se/2020/03/sakerhet-och-infrastruktur-vid-arbete-hemifran (accessed on 28 August 2021).
6. Fredriksson, A.; Wolf-Watz, O. *Kartläggning Och Analys av Förutsättningar för Arbete Hemifrån under Coronapandemin*; Myndigheten för Arbetsmiljökunskap: Gävle, Sweden, 2021; p. 52.
7. Pranggono, B.; Arabo, A. COVID-19 Pandemic Cybersecurity Issues. *Internet Technol. Lett.* **2021**, *4*, e247. [CrossRef]
8. Alavi, R. WFH: Think Before You Click. *ITNOW* **2020**, *62*, 40–41. [CrossRef]
9. Botha, R.; Furnell, S. Facing up to Security and Privacy in Online Meetings. *Netw. Secur.* **2021**, *2021*, 7–13. [CrossRef]
10. Furnell, S.; Shah, J.N. Home Working and Cyber Security—An Outbreak of Unpreparedness? *Comput. Fraud Secur.* **2020**, *2020*, 6–12. [CrossRef]
11. Talib, S.; Clarke, N.L.; Furnell, S.M. An Analysis of Information Security Awareness within Home and Work Environments. In Proceedings of the 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010; pp. 196–203.
12. Babbs, A. How to Leverage Data Security in a Post-Covid World. *Comput. Fraud Secur.* **2020**, *2020*, 8–11. [CrossRef]
13. He, Y.; Aliyu, A.; Evans, M.; Luo, C. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J. Med. Internet Res.* **2021**, *23*, e21747. [CrossRef]
14. Weil, T.; Murugesan, S. IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Prof.* **2020**, *22*, 4–10. [CrossRef]
15. Von Solms, R.; van Niekerk, J. From Information Security to Cyber Security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
16. Isaksson, J.; Sanne, T. Smarta Kort En del av en intelligent IT-lösning i hälso-och sjukvården? *Högsk. Jönköp* **2006**, 104. Available online: https://www.semanticscholar.org/paper/Smarta-Kort-%3A-En-del-av-en-intelligent-IT-l%C3%B6sning-i-Isaksson-Sanne/a70129e3c3cc3cd0096ff5dcdeec9aa55d60654e (accessed on 25 October 2021).
17. International Organization for Standardization ISO/IEC 27000: 2018. Available online: https://www-sis-se.libraryproxy.his.se/api/document/get/80001198 (accessed on 28 August 2021).
18. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*, 4th ed.; Cengage Learning: Boston, MA, USA, 2014; ISBN 978-1-111-13821-9.
19. Åhlfeldt, R.-M.; Spagnoletti, P.; Sindre, G. Improving the Information Security Model by using TFI. In *New Approaches for Security, Privacy and Trust in Complex Environments*; Venter, H., Eloff, M., Labuschagne, L., von Solms, R., Eds.; IFIP International Federation for Information Processing; Springer: Boston, MA, USA, 2007; Volume 232, pp. 73–84. ISBN 978-0-387-72366-2.
20. Reid, R.; Van Niekerk, J. From Information Security to Cyber Security Cultures. In Proceedings of the 2014 Information Security for South Africa, Johannesburg, South Africa, 13–14 August 2014; pp. 1–7.
21. International Organization for Standardization ISO/IEC 27002: 2017. Available online: https://www-sis-se.libraryproxy.his.se/api/document/get/8025294 (accessed on 28 August 2021).
22. Mihailović, A.; Cerović Smolović, J.; Radević, I.; Rašović, N.; Martinović, N. COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications. *Sustainability* **2021**, *13*, 6750. [CrossRef]
23. Mahr, A.; Cichon, M.; Mateo, S.; Grajeda, C.; Baggili, I. Zooming into the Pandemic! A Forensic Analysis of the Zoom Application. *Forensic Sci. Int. Digit. Investig.* **2021**, *36*, 301107. [CrossRef]

24. Faulds, D.J.; Raju, P.S. The Work-from-Home Trend: An Interview with Brian Kropp. *Bus. Horiz.* **2021**, *64*, 29–35. [CrossRef] [PubMed]
25. Carrapico, H.; Farrand, B. Discursive Continuity and Change in the Time of COVID-19: The Case of EU Cybersecurity Policy. *J. Eur. Integr.* **2020**, *42*, 1111–1126. [CrossRef]
26. MSB. Informationssäkerhet För Dig Som Arbetar Hemma. 2020. Available online: https://www.informationssakerhet.se/siteassets/nyheter/informationssakerhet-for-dig-som-arbetar-hemma--rad-fran-msb.pdf (accessed on 28 August 2021).
27. MSB. Till Dig Som Samordnar Organisationens Informationssäkerhet När Flera Arbetar På Distans. 2020. Available online: https://www.informationssakerhet.se/siteassets/nyheter/rad-till-dig-som-samordnar-organisationens-informationssakerhet-nar-flera-arbetar-pa-distans.pdf (accessed on 28 August 2021).
28. Humla, P.-O. Cyberattacker når Rekordnivåer under COVID-19. Available online: https://home.kpmg/se/sv/home/nyheterrapporter/2020/04/cyberattacker-okar-i-sparen-av-covid-19.html (accessed on 28 August 2021).
29. Hurst, A. Over a Quarter of Cyber Security Incidents Related to COVID-19—NCSC. *Inf. Age* **2020**. Available online: https://www.information-age.com/over-quarter-cyber-security-incidents-related-covid-19-ncsc-123492522/ (accessed on 25 October 2021).
30. Goldroth, A. Cyberattacker-Mot-Sjukvarden-i-Sverige-Okar-Med-32-Procent. Available online: https://it-halsa.se/cyberattacker-mot-sjukvarden-i-sverige-okar-med-32/ (accessed on 28 August 2021).
31. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
32. Okereafor, K.; Manny, P. Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing in the COVID-19 Pandemic.Pdf. *Int. J. IT Eng. IJITE* **2020**, *8*, 13–23. [CrossRef]
33. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from Home during COVID-19 Crisis: A Cyber Security Culture Assessment Survey. *Secur. J.* **2021**. [CrossRef]
34. Grigorescu, A.; Mocanu Nicolae, A. Teleworking Perspectives for Romanian SMEs after the COVID-19 Pandemic. *Manag. Dyn. Knowl. Econ.* **2020**, *8*, 383–399. [CrossRef]
35. Tokarchuk, O.; Gabriele, R.; Neglia, G. Teleworking during the Covid-19 Crisis in Italy: Evidence and Tentative Interpretations. *Sustainability* **2021**, *13*, 2147. [CrossRef]
36. IBM Cost of Insider Threats. Available online: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/ (accessed on 20 September 2021).
37. Chapman, P. Defending against Insider Threats with Network Security's Eighth Layer. *Comput. Fraud Secur.* **2021**, *2021*, 8–13. [CrossRef]
38. Eiza, M.; Okeke, R.I.; Dempsey, J.; Ta, V.-T. Keep Calm and Carry on with Cybersecurity @Home: A Framework for Securing Homeworking IT Environment. *Int. J. Cyber Situat. Aware.* **2021**, *5*, 1–25. [CrossRef]
39. Ahmad, T. *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*; Social Science Research Network: Rochester, NY, USA, 2020.
40. Naidoo, R. A Multi-Level Influence Model of COVID-19 Themed Cybercrime. *Eur. J. Inf. Syst.* **2020**, *29*, 306–321. [CrossRef]
41. Hijji, M.; Alam, G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access* **2021**, *9*, 7152–7169. [CrossRef]
42. Crossler, R.E.; Johnston, A.C.; Lowry, P.B.; Hu, Q.; Warkentin, M.; Baskerville, R. Future Directions for Behavioral Information Security Research. *Comput. Secur.* **2013**, *32*, 90–101. [CrossRef]
43. Vroom, C.; von Solms, R. Towards Information Security Behavioral Compliance. *Comput. Secur.* **2004**, *23*, 191–198. [CrossRef]
44. Niemimaa, E.; Niemimaa, M. Information Systems Security Policy Implementation in Practice: From Best Practices to Situated Practices. *Eur. J. Inf. Syst.* **2017**, *26*, 1–20. [CrossRef]
45. Njenga, K.; Brown, I. Conceptualising Improvisation in Information Systems Security. *Eur. J. Inf. Syst.* **2012**, *21*, 592–607. [CrossRef]
46. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. Foundations for an Intelligence-Driven Information Security Risk-Management System. *J. Inf. Technol. Theory Appl. JITTA* **2016**, *17*, 25–51.
47. Feldman, M.S.; Orlikowski, W.J. Theorizing Practice and Practicing Theory. *Organ. Sci.* **2011**, *22*, 1240–1253. [CrossRef]
48. Jarzabkowski, P. *Strategy as Practice: An Activity Based Approach*; Sage: London, UK, 2005.
49. Smets, M.; Morris, T.; Greenwood, R. From Practice to Field: A Multilevel Model of Practice-Driven Institutional Change. *Acad. Manag. J.* **2012**, *55*, 877–904. [CrossRef]
50. Leonardi, P.M. Theoretical Foundations for the Study of Sociomateriality. *Inf. Organ.* **2013**, *23*, 59–76. [CrossRef]
51. Carlile, P.R. Transferring, Translating, and Transforming: An Integrative Framework for Managing Knowledge Across Boundaries. *Organ. Sci.* **2004**, *15*, 555–568. [CrossRef]
52. Nelson, R.R. IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices. *MIS Q. Exec.* **2007**, *6*, 67–78.
53. Orlikowski, W.J. Knowing in Practice: Enacting a Collective Capability in Distributed Organizing. *Organ. Sci.* **2002**, *13*, 249–273. [CrossRef]
54. Bergström, E.; Lundgren, M.; Ericson, Å. Revisiting Information Security Risk Management Challenges: A Practice Perspective. *Inf. Comput. Secur.* **2019**, *27*, 358–372. [CrossRef]

55. Pridmore, J.; Oomen, T.A.P. A Practice-Based Approach to Security Management: Materials, Meaning and Competence for Trainers of Healthcare Cybersecurity. In *International Security Management: New Solutions to Complexity*; Jacobs, G., Suojanen, I., Horton, K.E., Bayerl, P.S., Eds.; Advanced Sciences and Technologies for Security Applications; Springer International Publishing: Cham, Switzerland, 2021; pp. 357–369. ISBN 978-3-030-42523-4.
56. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information Security Management Needs More Holistic Approach: A Literature Review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
57. Siponen, M. Six Design Theories for IS Security Policies and Guidelines. *J. Assoc. Inf. Syst.* **2006**, *7*, 19. [CrossRef]
58. Leedy, P.D.; Ormrod, J.E. *Practical Research: Planning and Design*, 11th ed.; Pearson: Boston, MA, USA, 2016; ISBN 978-0-13-374132-2.
59. Myers, M.D. Qualitative Research in Information Systems. *MIS Q.* **1997**, *21*, 241–242. [CrossRef]
60. Oehme, R. *Övergripande Studie av Offentlig It-Drift (Informationssäkerhet) i Västra Götaland*; Knowit: Stockholm, Sweden, 2020; p. 61.
61. Eisner, E.W. *The Enlightened Eye: Qualitative Inquiry and the Enhancement of Educational Practice*; Teachers College Press: New York, NY, USA, 2017; ISBN 978-0-8077-5824-3.
62. Bowen, G. Document Analysis as a Qualitative Research Method. *Qual. Res. J.* **2009**, *9*, 27–40. [CrossRef]
63. Gross, J.M.S. Document Analysis. In *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*; Frey, B.B., Ed.; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2018; ISBN 978-1-5063-2615-3.
64. Labuschagne, A. Qualitative Research—Airy Fairy or Fundamental? *Qual. Rep.* **2003**, *8*, 100–103. [CrossRef]
65. Rapley, T. *Doing Conversation, Discourse and Document Analysis*; SAGE: Thousand Oaks, CA, USA, 2018; ISBN 978-1-5264-2617-8.
66. Belanger, F. Theorizing in Information Systems Research Using Focus Groups. *Australas. J. Inf. Syst.* **2012**, *17*, 109–112. [CrossRef]
67. Hennink, M.M. *Focus Group Discussions: Understanding Qualitative Research*; Oxford University Press: New York, NY, USA, 2014; ISBN 978-0-19-985616-9.
68. Sobreperez, P. Using Plenary Focus Groups in Information Systems Research: More than a Collection of Interviews. *Electron. J. Bus. Res. Methods* **2008**, *6*, 209–216.
69. Tausch, A.P.; Menold, N. Methodological Aspects of Focus Groups in Health Research: Results of Qualitative Interviews With Focus Group Moderators. *Glob. Qual. Nurs. Res.* **2016**, *3*, 9–11. [CrossRef]
70. Strauss, A.L.; Corbin, J.M. *Basics of Qualitative Research: Grounded Theory Procedure and Techniques*, 2nd ed.; SAGE: Thousand Oaks, CA, USA, 1998; ISBN 978-0-585-38332-3.
71. Krueger, R.A. Designing and Conducting Focus Group Interviews. *Soc. Anal. Sel. Tools Tech.* **2001**, *36*, 4–23.
72. Jefferson How to Create Effective Focus Group Questions. Available online: https://online.jefferson.edu/business/create-effective-focus-group-questions/ (accessed on 28 August 2021).
73. Geertz, C. *The Interpretation of Cultures: Selected Essays*; Basic Books: New York, NY, USA, 1973.
74. Braun, V.; Clarke, V. Using Thematic Analysis in Psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [CrossRef]
75. Niemimaa, E. A Practice Lens for Understanding the Organizational and Social Challenges of Information Security Management. In Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, 27 June 2016.
76. Baskerville, R.; Siponen, M. An Information Security Meta—Policy for Emergent Organizations. *Logist. Inf. Manag.* **2002**, *15*, 337–346. [CrossRef]
77. Brown, J.S.; Duguid, P. Organizational Learning and Communities-of-Practice: Toward a Unified View of Working, Learning, and Innovation. *Organ. Sci.* **1991**, *2*, 40–57. [CrossRef]
78. Bromley, P.; Powell, W.W. From Smoke and Mirrors to Walking the Talk: Decoupling in the Contemporary World. *Acad. Manag. Ann.* **2012**, *6*, 483–530. [CrossRef]
79. Reckwitz, A. Toward a Theory of Social Practices: A Development in Culturalist Theorizing. *Eur. J. Soc. Theory* **2002**, *5*, 243–263. [CrossRef]
80. Siponen, M.T. An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *Eur. J. Inf. Syst.* **2005**, *14*, 303–315. [CrossRef]