Addressing telecommuting in cyber security guidelines

Department of Management and Entrepreneurship

Master's thesis

Author:
Nea Parppei

Supervisor:
Professor Reima Suomi

11.04.2022

Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master's thesis

Subject: Information System Science
Author: Nea Parppei
Title: Addressing telecommuting in cyber security guidelines
Supervisor: Professor Reima Suomi
Number of pages: 67 pages
Date: 11.04.2022

Cyber security threats are becoming more common than before. New phenomena in society include new cyber security threats which organisations and society should prepare for. One of these phenomena is telecommuting. Telecommuting has its roots already in the 1970s, but it has become increasingly popular during the last years. Especially the pandemic caused by Covid-19 has changed the way of working drastically. Pandemic and the social distancing forced many organisations to have their employees working from home. Information technology has abled telecommuting, but it has also brought some problems such as security issues. Cyber security threats have increased and become more diverse during the mass telecommuting caused by Covid-19. Telecommuting has some special features that can increase cyber security threats and risks. In this research the following cyber security threats relating to telecommuting were identified to be most relevant: cyber attacks, social engineering, unauthorized access and physical security.

Previous literature has identified that there exist cyber security threats in telecommuting, but it has remained unclear how organisations manage and mitigate these in practice. Many of the identified threats relate to employees' unwanted behaviour. Employees are unaware of the threats facing the organisation in telecommuting. Some employees have not been provided with proper guidelines and instruction on secure way of working. Information security policies and guidelines are important for maintaining cyber security in organisations. Policies can be even seen as the basis for organisation's cyber security. This research studied which guidelines could be applicable in a telecommuting environment in order to mitigate the common cyber security threats. Most prominent cyber security guidelines for telecommuting identified in this research were guidelines for personal and mobile devices, guidelines for social engineering, guidelines for physical security, network guidelines, password guidelines and guidelines for online meetings.

Case study of multiple cases was used as a method for this study. The cases are seven Finnish universities. The empirical data consists of cyber security and telecommuting guidelines from the universities. These guidelines were analysed by reflecting to the theoretical framework. The analysis showed that especially guidelines for physical security and online meetings were lacking. The presence of outsiders in the telecommuting environment was addressed poorly. Outsiders are a threat both to physical and online meeting security as outsiders may see or hear confidential things. In addition, guidelines were not addressing data labelling and information release. Threats specific to Covid-19 were also addressed poorly even though cyber criminals have exploited the pandemic. Guidelines seemed to be otherwise comprehensive. Threats that were addressed poorly have been especially relevant during the pandemic which suggests that organisations' guidelines are not quite up to date even though otherwise applicable. Organisations should review and update their guidelines periodically and if a major change occurs in the operation environment.

Key words: telecommuting, cyber security, cyber security policy, cyber security guidelines

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätieteet
Tekijä: Nea Parppei
Otsikko: Etätyö tietoturvaohjeistuksissa
Ohjaaja: Professori Reima Suomi
Sivumäärä: 67 sivua
Päivämäärä: 11.04.2022

Kyberturvallisuusuhat ovat yleistymässä. Uudet ilmiöt tuovat mukanaan uusia kyberturvallisuusuhkia, joihin organisaatioiden ja yhteiskunnan tulee varautua. Yksi näistä ilmiöistä on etätyö. Etätyön juuret ovat jo 1970-luvulla, mutta sen suosio on kasvanut viime vuosina. Erityisesti Covid-19 ja sen aiheuttama pandemia ovat muuttaneet työn toimintatapoja radikaalisti, sillä pandemia pakotti monet työntekijät etätyöhön. Tietotekniikka on mahdollistanut etätyön, mutta se on tuonut myös ongelmia liittyen kyberturvaan. Kyberturvallisuusuhat ovat lisääntyneet ja monipuolistuneet pandemian aiheuttaman laajalle levinneen etätyön myötä. Etätyössä on joitain erityispiirteitä, jotka voivat lisätä kyberturvallisuusuhkia ja -riskejä perinteiseen työntekoon verraten. Tässä tutkimuksessa tärkeimmiksi etätyöhön liittyviksi kyberuhiksi tunnistettiin kyberhyökkäykset, sosiaalinen manipulointi, valtuuttamaton pääsy ja huono fyysinen turvallisuus.

Aikaisemmassa kirjallisuudessa on havaittu, että etätyöhön liittyy kyberturvallisuusuhkia, mutta on jäänyt epäselväksi, miten organisaatiot hallitsevat ja vähentävät niitä käytännössä. Monet tunnistetuista uhista liittyvät työntekijöiden ei-toivottuun käyttäytymiseen. Työntekijät eivät välttämättä ole tietoisia etätyön uhista organisaatiolle. Osalle työntekijöistä ei ole myöskään annettu asianmukaisia ohjeita kyberturvallisista työskentelytavoista. Tietoturvapolitiikat ja -ohjeet ovat tärkeitä organisaatioiden kyberturvallisuuden ylläpitämisessä. Politiikkoja voidaan pitää jopa organisaation kyberturvallisuuden perustana. Tässä tutkimuksessa selvitettiin, minkälaisia ohjeita tarvitaan etätyössä yleisten kyberturvallisuusuhkien lieventämiseksi. Tässä tutkimuksessa tunnistetut kyberturvallisuusohjeet etätyöhön liittyivät henkilökohtaisten ja mobiililaitteiden käyttöön, sosiaaliseen manipulointiin, fyysiseen turvallisuuteen, turvattomiin verkkoihin, salasanoihin ja online-kokouksiin.

Tutkimusmetodina tässä tutkimuksessa käytettiin usean tapauksen tapaustutkimusta. Tapauksina toimivat seitsemän suomalaista yliopistoa. Empiirinen data koostuu Suomessa toimivien yliopistojen kyberturvallisuus- ja etätyöohjeista. Nämä ohjeet analysoitiin teoreettiseen viitekehyksen avulla ja siihen viitaten. Analyysi osoitti, että erityisesti fyysistä turvallisuutta ja online-kokouksia koskevat ohjeet ovat puutteellisia. Ulkopuolisten läsnäolo etätyöympäristössä on huomioitu huonosti. Ulkopuoliset ovat uhka sekä fyysiselle että online-kokousten turvallisuudelle, koska ulkopuoliset voivat nähdä tai kuulla luottamuksellisia asioita. Lisäksi datan merkitsemiseen ja tiedon jakamiseen liittyvät ohjeet puuttuivat. Covid-19 oli myös huomioitu huonosti, vaikka pandemian aikana on ollut useita kyberhyökkäyksiä, jotka ovat hyödyntäneet Covid-19 tuomaa epävarmuutta. Yliopistojen ohjeet näyttivät muuten olevan kattavat. Huonosti huomioon otetut ohjeet ovat sellaisia, jotka ovat olleet esillä etenkin pandemian aikana. Vaikuttaa siltä, että organisaatioiden ohjeet eivät ole täysin ajan tasalla, vaikka ne muuten olisivat tarkoituksenmukaiset. Organisaatioiden tuleekin tarkistaa ja päivittää ohjeitaan säännöllisesti ja aina, jos toimintaympäristössä tapahtuu suuria muutoksia.

Avainsanat: etätyö, kyberturva, kyberturvapolitiikka, kyberturvaohjeet

TABLE OF CONTENTS

LIST OF TABLES

1 Introduction

1.1 Background

Telecommuting is listed as one of the main trends in cyber security 2021. This is due the pandemic caused by Covid-19 which has increased the amount of telecommuting substantially. Telecommuting increases cyber security risks. The systems and devices may be less secure, and the working habits are different from a traditional workplace. (Gartner, 2021; Kaspersky, 2021; Northeastern, 2021.) Cyber criminals have exploited the pandemic and the following mass telecommuting. Cyber crimes have become more diverse, and the methods have developed. Cyber crimes exploit different characteristics of human nature, and they try to appeal emotionally as well as use different influence mechanisms. (Naidoo, 2020, 317-318.)

Telecommuting creates variety of different challenges for organisations. Security risks can be seen as most alarming ones for organisation's systems. (Khan et al., 2020, 1.) Telecommuting has also created problems in the capacity of organisations' systems. For example, the virtual private networking software of United States' Air forces could support only half of the in-house workers at once. (CNN, 20.3.2020.) This could lead to cyber security risks if other less secure networking software would be used due to unavailability of the private networking software.

Telecommuting creates new kinds of threats which are hard to monitor. For example, using personal devices in work can expose corporate information to danger. Either naive user can expose the data, or malicious actor can have access to data more easily. (Flores et al. 2016, 1008.) Guidelines and policies for telecommuting are needed to support cyber security. For example, Gordon (2020, 15) suggests that organisations should move to zero-trust approach, which means that every user and device should be verified.

Even though the quick transition to telecommuting is due the pandemic, telecommuting is most likely here to stay. However, the change has been fast, and organisations need to adapt to it. (Curran, 2020, 12.) Some organisations have already decided that they will move into permanent or long-term telecommuting mode. Other organisations have decided that part of their employees will work remotely also in the future. (Obada-Obieh et al., 2021, 675.) Organisations have to enforce their information security policies in

telecommuting in order to avoid cyber attacks and information leakages (Al Shammari et al, 2021, 1).

1.2 Research gap

Cyber security and telecommuting are addressed in the information security research. Al Shammari et al. (2021, 1) recognized that cyber attacks have increased during Covid-19. They also identified that organisations need clear guidelines and policies to prevent cyber security vulnerabilities in telecommuting. Also, Medina-Rodríguez et al. (2020, 5) acknowledges the importance of cyber security. However, in the article it is discussed how Covid-19 has increased telecommuting but it still remains unclear how well organisations have prepared the cyber security standards to this. In addition, some telecommuters have not been provided telecommuting guidelines or instructions. This may be, for example, because telecommuting has conflicts with organisation's common policies. (Obada-Obieh et al., 2021, 682.)

To conclude, the research on how organisations are managing cyber security in telecommuting, and which kind of guidelines are needed is missing. This shows the gap in the research which should be further investigated. In order to have secure telecommuting practices there should be clear guidelines for employees on secure ways of working. Some fields and organisations are unwilling to allow or expand telecommuting due to security risks (Gordon, 2020, 14). Thus, it is important to know the needed security measures in order to be more flexible about telecommuting.

1.3 Study design

In this research it is studied how telecommuting is addressed in cyber security guidelines. Reporting of this research follows a linear-analytic structure. Linear-analytic structure means that the study starts with presenting the problem and research questions, continuing to previous literature and theoretical framework, proceeding to methodology and analysis and finally findings are presented. (Yin, 2009, 176.) This study is organized as followingly. First, short introduction to the topic is presented. It includes description of the background for this research and the research gap. These elaborate why this research is important to be conducted and what are the main issues in the previous research. After that, the previous literature is presented. The previous literature includes cyber security threats in telecommuting and cyber security guidelines and policies. Theoretical

framework is constructed on the basis of the previous literature. The theoretical framework summarizes the different cyber security threats in telecommuting and suggests guidelines for managing them. Empirical data is analysed reflecting to the theoretical framework. Empirical data consists of cyber security or telecommuting guidelines and policies collected from Finnish universities. Similarities and differences between cases are studied as well as similarities and differences between the cases and the theoretical framework. The purpose is to find out how well universities' guidelines and policies apply to telecommuting environment and what kind of improvements are needed.

1.4 Objective and contribution

The objective of this research is to fill the research gap about guidelines and practices organisations must have relating to cyber security in telecommuting. In addition, this study contributes to practical IT management, as it reveals which factors should be taken into consideration from cyber security perspective in telecommuting environment. This research shows what kind of cyber security threats there exist in telecommuting and how organisations manage those. This research reveals different cyber security guidelines and principles organisations should have relating to telecommuting. This research is also important to society because cyber security breaches can affect each of us. With proper management, those breaches could be minimized. Research question for this study is: How to address telecommuting in cyber security guidelines and policies?

2 Cyber security in telecommuting

2.1 Definition of telecommuting

Telecommuting has become more popular over time. However, telecommuting has its roots as early as the 1970s. Already in the 1970s, private companies realised that telecommuting could be a way to hire more computer programmers. (Allen et al., 2015, 41.) Thus, it is clear that technology has been an important aspect of telecommuting early on. Telecommuting was also seen as a way to achieve an adequate work-life balance as in more families both of the parents were working. Personal computers increased the amount of telecommuting as it came more convenient to work from home. Even before Covid-19 pandemic, many companies have offered telecommuting in some form. (Allen et al., 2015, 41.) Through digitalization and digital tools telecommuting has become widespread as people are working together regardless of their physical location (Skryl, 2021, 202).

Telecommuting has been a controversial topic as it differs from traditional work and creates opportunities such as flexibility as well as problems such as professional isolation (Allen et al., 2015, 46; 52). Some other benefits of telecommuting include less transportation issues, better job opportunities as physical location matters less and working with disabilities is easier (Skryl, 2021, 205). One of the important benefits of telecommuting is business continuity. People can continue working regardless of weather conditions or emergencies. (Allen et al., 2015, 57.) This does not apply for all situations but for example during Covid-19 pandemic employees have been able to continue their work and protect themselves better from the disease.

Telecommuting has many synonyms such as telework, remote work and virtual work. The different terms can have slightly different meanings but in this study the term telecommuting is used because the definition of telecommuting by Allen et al. (2015, 44) fits best for this study's purpose. Telecommuting refers to working outside of the organisation's worksite, usually at home (Allen et al., 2015, 41-44). Skryl (2021, 202) defines that telecommuting is work that is done outside the actual workplace with the help of digital tools and solutions. Especially the communication happens through digital channels. Allen et al. (2015, 44) defines telecommuting in a similar way:

> "Telecommuting is a work practice that involves members of an organisation substituting a portion of their typical work hours (ranging from a few hours per week to nearly full-time) to work away from a central workplace—typically principally from home—using technology to interact with others as needed to conduct work tasks"

This definition describes fairly well also the telecommuting situation during the pandemic as people are working from home with the help of technological solutions. However, different terms referring to telecommuting have the same base meaning (Allen et al., 2015, 44). Thus, all the different terms were taken into consideration when conducting this research.

2.2 Definition of cyber security

Cyber security consists of guidelines, tools, policies, training, risk management, best practises, security concepts and technologies that exist in cyber environment and protect important assets. Cyber security deals with a variety of issues relating to different assets of users and organisation. These assets include systems, infrastructure, personnel, applications, devices, services as well as information stored and transmitted in the cyber environment. (ITU, 2008, cited in Solms & Niekerk, 2013, 97-98.)

Bayuk et al. (2012, 2-3) divides cyber security in three parts. These parts explain the goals of cyber security, the methods of cyber security and the security objectives of information. The goals are to prevent, detect, and respond. These goals apply both to physical security and cyber security. First goal is to prevent possible cyber security threats, however, cyber security professionals realise that it is impossible to prevent all attacks. Thus, it is important to detect the attacks or other threats and respond to them. Often term recover is used instead of respond as it has more positive meaning. The methods or actors of cyber security are people, processes, and technology. This describes that in cyber security management multiple aspects should be taken into consideration. Neither technology nor cyber security professionals alone can ensure cyber security. Also, human behaviour without clear processes, will not lead to security. Cyber security management should take into consideration all these three aspects. The security objectives of information that apply in cyber security are integrity, availability, and confidentiality. Integrity meaning that the data is accurate, and it has not been changed by unauthorized ways. Availability meaning that the data is available for those who have permission to access it. Confidentiality means that the data can be viewed only by authorized people. (James, 2011, 134.)

Cyber security and information security are often used interchangeably, and their definitions are close to each other even though they do not mean the same thing. Information security can be defined to protect information availability, confidentiality, and integrity of important information assets. It is important to notice that information security is not only a technology but a process. Cyber security can be seen not only the protection of information assets but protection of cyberspace, those in it and their assets. (Solms & Niekerk, 2013, 98; 101.) When conducting this research both terms information security and cyber security were taken into consideration when applicable as they are very similar to each other.

In this research the definition by Bayuk et al. (2012, 3) is used:

> "Cyber security refers in general to methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace."

Cyber security attacks are becoming more popular because they are cheaper, easier, and less risky to execute than physical attacks. Cyber attacks cost massive amounts of money to organisations every year, in addition it takes time to repair the damage caused by cyber attacks. (Jang-Jaccard & Nepal, 2014, 973-974.) Organisation's assets can also be stolen and reputation damaged. Reputational damage can further on affect to organisation's stock value and shareholder value. (Smith et al., 2019, 56.) Thus, cyber security seems to be an important for organisations to maintain in order to avoid unwanted consequences.

2.3 Mass telecommuting era

Covid-19 caused a massive movement towards telecommuting. Even though telecommuting has existed before, the scale is now totally different. During the pandemic, many employees have not had any other options than to work remotely. Employees have not been able to see people face-to-face even for meetings or events. This has meant wide adaption of organisations' digital solutions in order to efficiently work from home with people located all over the world. Luckily, organisations have already before the pandemic used different tools and solutions that are crucial in telecommuting environment. Organisations are prepared for telecommuting better than ever, even though organisations have not necessarily been aiming for it. If the pandemic had happened years earlier there might have been much more difficulties relating to information technology utilised in telecommuting. (Papagiannidis et al., 2020, 1-2.)

Even though organisations might be better prepared for this sudden shift to telecommuting now than before, it was still a profound change for many organisations. Not all employees were familiar with telecommuting and its unique characteristics. In addition, because the shift to telecommuting was so sudden, organisations did not have time to do all the necessary steps before implementing telecommuting widely. (Godoy et al., 2021, 673.)

Employees have experienced difficulties as well as opportunities in working remotely. Lack of contact with co-workers, keeping up the work-life balance and constant disruptions are some difficulties that telecommuting has created for employees. However, flexibility, lack of commuting and more freedom with physical appearance have been things employees have appreciated. The role of technology is quite contradictory. On one hand, all the technological devices and need for technology can cause stress to employees. On the other hand, with virtual tools training can be provided for employees relating to various aspects of telecommuting. (Godoy et al., 2021, 675; 676.)

2.4 Increase in cyber security threats

As telecommuting has become mandatory way of working for many people, different cyber security threats and risks have occurred (Ramadan et al., 2021, 4). This mass telecommuting era caused by Covid-19 pandemic have some special features. These include that different technology and information systems have become extremely important in people's everyday life as well as in work. Communication tools such as Zoom and Microsoft Teams have enabled better communication between people in remote locations. (Dwivedi et al., 2020, 2.)

Nurse et al. (2021, 4-5) divides the cyber security risks relating to telecommuting into two categories. First, risks relating to employees that work remotely and second risks relating to the used technologies. Threats employees may cause can be intentional or unintentional. These threats are (Nurse et al., 2021, 4)

- Falling for scams such as phishing, because of lack of concentration due to of distractions at home.
- Poor cyber security training for telecommuting.
- Prioritising other things than security because of stress and anxiety.

- Poor access to security information due to, for example, the physical distance to colleagues.
- Outsiders' presence in the working environment.
- Minimal monitoring over employees may encourage malicious actions.

Technology-related risks are (Nurse et al., 2021, 4-5)

- Too quick transition to wide adoption of new technology due to pandemic.
- Lack of knowledge of different technologies and tools.
- Security issues with the telecommuting communication tools.
- Using work devices for personal purposes.
- Work devices may be stolen if not appropriately guarded and stored.
- Bringing devices used in home networks to corporate network can pose a threat and cause damage.

Above mentioned threats show that there are many factors in telecommuting security that should be taken into consideration. Employees' lack of knowledge is one aspect but there are also telecommuting specific features such as unsecure physical environment. Telecommuting environment differs from the traditional office environment which should be considered from the cyber security perspective. As human behaviour creates cyber security threats in telecommuting environment countermeasures should aim to affect employees' behaviour.

Multiple cyber security threats in telecommuting are recognized by Ramadan et al. (2021, 4-6). Working from home presents new threats to cyber security. These include unsecure home networks, different technologies, personal devices, unauthorized access, and irresponsible behaviour. Ramadan et al. (2021, 4-6) explains these as followingly. Without proper antivirus software and firewall, networks are not secure. In addition, in order to work from home, different technologies are needed. However, the problem occurs when people are not experienced in using these devices. Also, asking for help might not happen as easily as in office. Georgiadou et al. (2021, 13) discovered that some employees were forced to use unfamiliar applications while working remotely. Lack of knowledge or an incapability of using different technologies can also lead to neglecting security measures such as security updates (Obada-Obieh et al., 2021, 681).

Ramadan et al. (2021, 4-6) continues that use of personal devices may also pose a threat because of lack of performance of the devices and possible untrusted programs in the devices. Devices provided by the workplace are more standardized and there is nothing extra embedded in them. Unauthorized access may occur because of poor passwords and security controls. Lastly, irresponsible behaviour can pose a threat when employees do not follow the provided policies. Employees could, for example, use public WiFis instead of protected ones. Unsecure networks and the use of personal devices are mentioned as a threat also by Chigada and Madzinga (2021, 3).

In addition to threats regarding especially telecommuting, Ramadan et al. (2021, 5) mentions other cyber security threats that can occur. These include social engineering attacks, ransomware attacks, phishing attacks, denial of service (DoS) attacks and other unethical attacks and behaviour. Different cyber attacks are a threat in telecommuting as well as in traditional work. Attacks that have been very typical and dangerous in the pandemic and in mass telecommuting are malware, DoS (denial of service) and ransomware attacks (Khan et al., 2020, 2-3). Cyber attacks can be conducted, for example by cyber criminals or governments (Ramadan et al., 2021, 1; Van't Wout, 2019, 458). Especially cyber criminals have tried to benefit from the pandemic (Chigada & Madzinga, 2021, 1).

The cyber security threats or factors causing issues in cyber security mentioned in this chapter are gathered in Table 1. As these threats seem to be most essential ones in telecommuting, this research concentrates more closely on them.

Table 1 Common cyber security threats in telecommuting

Cyber security threats in telecommuting
Cyber attacks
Personal devices
Social engineering
Irresponsible behaviour
Unsecure networks
Unauthorized access
Physical security

2.5 Cyber attacks

2.5.1 Malware

Malware can be any harmful software or code which can penetrate, destroy, or disable victim's device, its operations, and data. As a result, device and its programs do not function as they are meant to be. (Ramadan et al. 2021, 3; 7.) Thus, data confidentiality, availability and integrity can be violated. Different types of malwares include viruses, worms, Trojan horses, and spyware. Malware attacks evolve over time and novel approaches include social media, smart phones, and cloud computing. For example, it is attempting for the attackers to utilize social media as the malware can be spread widely in the social media network. This is appealing to attackers as social media is an important part of many people's lives, and it connects millions of people. Nowadays, malware's purpose is often to steal personal, financial, or business information. (Jang-Jaccard & Nepal, 2014, 974.)

During the pandemic black hat hackers, in other words criminals who are conducting cyber attacks for malicious intents and self-interest have tried to benefit from the pandemic (Ramadan et al., 2021, 1). Malware attacks can be performed on personal devices when they are connected to organisation's network. Mobile devices are especially in danger to these attacks and mobile malwares have increased over the years. (Chigada & Madzinga, 2021, 6; Jang-Jaccard & Nepal, 2014, 990.) Malware is often spread by spam emails, phishing, or downloads from the internet (Jang-Jaccard & Nepal, 2014, 976). Malware attacks often start with one user who downloads malicious content and then the malware spreads around (Van't Wout, 2019, 458). Users can be tricked into downloading malware, but the attacker can also exploit vulnerabilities of the devices and remotely access the device (Bello Garba et al., 2015, 1280).

2.5.2 DoS attacks

In DoS attack user's services and devices are disabled. The purpose is to create a lot of traffic to the user's services and device and this way the resources will be unavailable to the user. (Ramadan et al., 2021, 3.) This can lead to huge financial losses for the organisation under DoS attack. In addition, the organisation can suffer from low productivity and reputational damages. (Kaur Chahal, 2019, 56.) Distributed denial of service attack (DDoS) is a specific DoS attack where traffic is created from multiple

different sources at the same time (Ramadan et al., 2021, 3). The motivation behind DDoS attack can vary. Financial gain is one of the reason DDoS attacks are executed. Other reasons can be personal revenge against organisation, the publicity gained from the attack, seeing the attack as an experiment or a challenge, using the attack in cyber warfare or executing the attack because of ideological beliefs. (Kaur Chahal, 2019, 36.)

During the pandemic DDoS attacks have been common and telecommuting can increase DDoS attacks even more (Chigada & Madzinga, 2021, 6). Mobile devices are vulnerable to DDoS attacks (Kaur Chahal, 2019, 88). Personal devices, which include mobile devices, are used in telecommuting frequently (Ramadan et al., 2021, 5; Bello Garba et al., 2015, 1279). Thus, DDoS attacks are a serious threat in telecommuting.

2.5.3 Ransomware

Ransomware can be seen as a type of malware where ransom is demanded. In a ransomware attack the attacker can disable services or threaten to distribute confidential information gathered inside the organisation. The attacker demands ransom in return for restoring the systems. Bitcoin is strongly associated with these ransomware attacks because it is hard to trace, and the transactions are quick. The ransomware attacks have become even more popular during Covid-19 and especially health care is targeted. Attackers will make it extremely difficult to continue business operations or they threaten to expose confidential information. Thus, organisations feel that it is necessary to pay the ransom. (Ramadan et al., 2021, 6-7.)

Ransomware attacks can happen, for example, through an email attachment (Chigada & Madzinga, 2021,4). Email phishing is the primary source of ransomware (PwC 2020, cited in Chigada & Madzinga, 2021, 4). During widely spread telecommuting and remote use of organisations' networks there have been ransomware attacks. As employees are working remotely, they have remote access to organisations network. This enables the hackers to block employees from the systems and demand ransom. (Chigada & Madzinga, 2021, 7.) In addition, employees may communicate via unauthorized email and communication systems. These systems may not have proper filtering for spam email which increases the possibility to become a target for ransomware. (Curran, 2020, 11.)

2.6 Personal and mobile devices

One important aspect of telecommuting are the used devices. Working from home increases BYOD (bring your own device) phenomena which in turn creates security risks (Chigada & Madzinga, 2021, 5). BYOD means that employees are using their own personal devices instead of those provided by the organisation. These devices can be mobile devices such as smart phone or tablet, or personal computers. (Bello Garba et al., 2015, 1279.) As the Covid-19 pandemic forced employees to work from home, some organisations allowed employees to use personal devices for enterprise applications. This creates a significant threat if adequate security measures are not in place. (Dwivedi et al., 2020, 10.) Using personal devices poses a threat to cyber security also when employees connect multiple devices to organisation's network. In addition, these devices are sometimes used by multiple users such as family and friends. (Chigada & Madzinga, 2021, 5.) If multiple people use these devices, someone may compromise the device on purpose or by accident. For example, the device could be infected by a malicious software. (James, 2011, 133.)

Use of personal devices may also pose a threat because personal devices may have worse performance than organisations' devices. In addition, there may be untrusted programs installed in personal devices and these devices may not have proper backup mechanisms. (Ramadan et al., 2021, 5.) Especially mobile devices are a security risk in BYOD phenomena. Mobile devices' physical security is hard to maintain, and they can be easily lost or stolen. In addition, using the device for both personal and work-related needs can expose the information in danger. Mobile applications can be a threat as well if their security is not ensured. For example, mobile applications can contain malware. (Ganiyu & Jimoh, 2018, 52.)

Bello Garba et al. (2015, 1280) recognizes seven threats for BYOD devices. Some of these threats exist on other devices as well but the risk increases with BYOD. The first threat is malware. Malware is a great risk to mobile devices. It can be used to steal or spy user's information. Mobile devices are a usual target to malware attacks. Second threat mentioned is phishing and social engineering. Phishing and social engineering can lead, for example, to malware. People are tricked to give confidential information or download malware. Third threat is direct attacks which can cause severe damage by accessing,

modifying, or destroying corporate information. Thus, data confidentiality, integrity and availability can be at risk.

Bello Garba et al. (2015, 1280) continues with fourth threat which is data communication interception and spoofing. Spoofing is an act where malicious actor impersonates a valid IP address in order to gain access to information (Nandal & Kajal, 2020, 5389). Spoofing can lead, for example, to malware and stealing data (Wang & Alexander, 2021, 147). Bello Garba et al. (2015, 1280) continues that these threats concern especially wireless networks. Data sent through wireless networks can be spied, stolen, or modified. This can happen even through encryption. Again, data confidentiality, integrity and availability are at risk.

Fifth threat mentioned by Bello Garba et al. (2015, 1280) concerns the physical security of the device, in other words a loss or theft of the device. If personal device is stolen or misplaced, valuable information may be at risk. Especially with mobile devices the physical environment where the devices are used can vary. Physical security of devices may be less safe in public spaces than in home or office environment. (Ganiyu & Jimoh, 2018, 53.) As a sixth threat Bello Garba et al. (2015, 1280) mentions malicious insiders. These insiders can execute malicious acts, for example, malware attacks, phishing and stealing devices. Mobile devices and personal devices are more vulnerable to malicious actors as the acts performed may not be visible in the organisation.

The final threat mentioned by Bello Garba et al. (2015, 1280) is user policy violations. These can happen by accident, but it is still profoundly serious threat that can lead to malware or exposing valuable information. Also, when employees are using personal devices, corporate and personal information is mixed and can risk the integrity of corporate information (Flores et al., 2016, 1010). It was also mentioned by Bello Garba et al. (2015) that using BYOD can make it more difficult for organisations to monitor policy compliance. Different cyber security threats faced by personal devices are gathered in Table 2.

Table 2 Cyber security threats for personal devices

Cyber security threats of personal devices
Malware
Phishing and social engineering
Direct attacks
Data communication interception/spoofing
Lost or theft of device
Malicious insiders
User policy violations
Monitoring is more difficult
Multiple users
Lack of performance of devices
Untrusted programs installed
Lack of proper backup mechanisms
Mixed use of personal and organisational information

Table 2 and previous literature show how especially mobile devices are vulnerable to cyber security threats. Mobile devices are an easy target for theft, and they are easily lost. Policies are also harder to implement for mobile devices. (Bello Garba et al., 2015, 1280-1281.)

2.7 Irresponsible behaviour

Human errors should be taken into consideration when addressing cyber security in telecommuting. Human behaviour can be seen as a crucial part of organisation's information security (Bhaharin, 2019, 1). Human error is an important aspect in telecommuting as well as in traditional work. Human errors can be divided into unintentional actions and intentional actions. (Lee, 2012, 2.)

Slips and lapses occur in tasks that do not require much conscious effort. Slips and lapses happen when a wrong action is executed, some part of the action is unconsciously ignored, or task is done in wrong order. Mistakes occur in more challenging tasks. Mistakes happen when task is executed by following wrong steps due to lack of knowledge or understanding. Violations, however, happen when action is executed incorrectly on purpose. (Lee, 2012, 2.) Lee (2012, 5) discovered that most human errors were slips done by insiders with good intentions.

There are multiple risky cyber security behaviours employees can practice. Wang and Alexander (2021, 146) have recognized nine of those and they are shown in the Table 3. These unsecure behaviours include downloading unsecure materials or software, unsecure password usage, using unsecure networks and different kind of unsecure handling of confidential information

Table 3 Risky cyber security behaviours (Wang & Alexander, 2021, 146)

Items
Clicking on links attached in suspicious emails
Using the same password on multiple places
Downloading anti-virus program from suspicious source
Entering payment details on unsecure websites
Downloading material on a work computer without knowing its authenticity
Downloading digital media from unknown sources
Using free and public WiFis
Using online storing systems to store and exchange sensitive information
Saving corporate information on a personal device

The activities shown in Table 3 are something that employees can affect with their own behaviour. Thus, awareness and knowledge can be seen crucial in order to mitigate these risky behaviours as these activities can lead to cyber attacks. Many of the activities shown in Table 3 are related to social engineering and phishing which are discussed in chapter 2.8.

2.8 Social engineering

Cyber security threats are not concentrating anymore only on technological aspects. Attacks that are based on human interactions have become very common. (Aldawood & Skinner, 2019, 2.) Social engineering is closely related to humans and their actions, and it can put organisation's information assets at risk. The purpose of social engineering is to gain access to organisation's information by exploiting human interaction. Social engineering can be divided into two categories which are attacks based on physical location and attacks based on psychological methods. Both methods require background information for the attacker. This information can be gathered, for example, from social media. (Ghafir et al., 2016, 145-146.) For example, malware can be spread by social engineering techniques. There are variety of social engineering techniques which makes

it easy to spread malware. (Jang-Jaccard & Nepal, 2014, 986.) In telecommuting, social engineering is a potential threat facing employees as well as their families (Chigada & Madzinga, 2021, 3). After the attackers have gained valuable information, they can use that to perform another attack and modify or delete organisation's valuable information (Aldawood & Skinner, 2019, 3).

Attacks that are based on physical location are done in workplace, by telephone or online. In the workplace the attacker can impersonate someone that has access to the workplace. This way attacker can eavesdrop and spy on the information that they need. Attacks done by telephone are often targeted at organisation's help desk. The attacker may appear calling from inside the organisation and that way they can inquire the information they want. Third social engineering method relying on physical location is an attack done online. The attack can happen, for example, by email or social media. The attacker may use phishing methods or malware in order to acquire the information. (Ghafir et al., 2016, 146.) Attackers also use fake websites for phishing and spreading malware. This has been especially common during the pandemic. (Chigada & Madzinga, 2021, 6.)

Attacks based on psychological methods exploit human behaviour in order to gather valuable information. The attacker can exploit authority, human need to help others, similarity with the target and attacker, commitment and consistency, reciprocation, or target's low involvement to the subject. People may be willing to give information such as passwords if someone with authority demands for it. Especially, if the attacker intimidates the subject. People also have tendency to help. Thus, the attacker can impersonate, for example a delivery man who needs to get into the building or a remote worker who calls for help desk. The attacker may also try to develop a personal connection with the target and this way gain access to information. (Ghafir et al., 2016, 147.)

The attacker can also exploit people's tendency of wanting to be seen as committed and trustworthy. This way the attacker can ask the target to execute some tasks, for example, to follow a security guideline but in the process the attacker acquires target's password. One method is reverse engineering where the attacker creates a situation where the target must ask help from the attacker. After this, the attacker can inquire information from the target. The attackers can also exploit target's low involvement to the information they wish to acquire. Asking from cleaning staff or receptionist can be easy way to acquire the

needed information. (Ghafir et al., 2016, 147.) In this research those social engineering attacks that happen physically on workplace are not taken into consideration. However, other social engineering attacks are as relevant in telecommuting as in traditional work.

Phishing attacks have been highly effective during the pandemic (Al Shammari et al., 2021, 1). Phishing is usually SMS phishing, email phishing or phishing scams. The aim is to get useful information from the victim, for example, passwords, bank details or address. This can happen via link which leads to fake website or by attached file that contains malware. Phishing scams can, for example, trick people into giving information by promising a reward. Spam emails have been common during Covid-19. Emails have contained, for example, false information about Covid-19 and this way tricked people. (Ramadan et al., 2021, 9.)

Aldawood and Skinner (2019, 10) sees social phishing, spear phishing, brand theft and typo squatting and email frauds as the key issues of social engineering. Social phishing is phishing that happens on social media. Spear phishing on the other hand means a phishing attack which is targeted to a specific audience. In brand theft employees believe they are interacting with a real brand even though it is fake. In typo squatting the attackers create domains with minor misspellings and this way tricks people to wrong websites. Email frauds can include all kinds of fake emails that are made to look like legit ones.

2.9 Unsecure networks

Working from home increases the threat of unsecure networks. People are using their home network for work, and this can cause problems if proper safety measures are not in place. Home networks may not have firewalls, antivirus programs, intrusion detection systems or intrusion prevention systems. Antivirus program could detect malicious programs or files and this way prevent them from harming the device and systems. Firewall monitors network traffic usually from Internet. Harmful traffic can be blocked. Intrusion detection system will detect intrusions from network traffic such as ransomware. Intrusion prevention system will prevent those activities. (Ramadan et al., 2021, 4.)

Virtual private networks (VPN) are important in telecommuting (Wang & Alexander, 2021, 147). Employees can connect organisation’s network remotely with VPN, privileged access management (PAM) or vendor privileged access management (VPAM).

However, these can be vulnerable to hacking without any additional security protocols. (Chigada & Madzinga, 2021, 5.) If the security measures are not in place, the use of VPN can lead to leakage of confidential information and further on to a DoS attack. Organisations should make sure that their VPN services are entirely secure. (Baz et al., 2021, 644.)

Threats can also occur when employees do not follow the protocols for using organisation network safely. Employees, for example, go to unsecure websites while using organisation's network. For example, during Covid-19, hackers have created a lot of fake domains relating to Covid-19 in order to get information and deceive users. Using public WiFi's can also expose organisation's network to viruses and data leakages. Use of public WiFi's is risky for the device itself as well as to corporate information. (Chigada & Madzinga, 2021, 5.) Especially during the pandemic, when the transition to telecommuting has been fast, people may not have proper facilities and resources to work. Thus, they trust on public places and free internet access. (Baz et al., 2021, 645.)

2.10 Unauthorized access

Unauthorized access is a significant threat in telecommuting. Malicious actors can have access to organisation's systems and data simply by using employee's poor passwords. As organisations had to switch to telecommuting, new infrastructures and new employee accounts were established. However, many employees choose easy passwords which makes it easy for an attacker to penetrate the systems. Organisations also had to create some new network infrastructure which may include vulnerabilities. Malicious actors can exploit these vulnerabilities found in VPN or communication tools such as Zoom or Microsoft teams. (Ramadan et al., 2021, 6.) Unauthorized access can also happen physically as employees are not working in office environment (Obada-Obieh et al. 2021, 680). This is discussed more in chapter 2.11.

During the pandemic social distancing has been mandatory for safety reasons. Thus, communication tools and different applications have been crucial. (Papagiannidis et al., 2020, 1.) These tools could be important in telecommuting also after the pandemic. However, there have been attacks against telecommuting tools such as communication tools e.g., Zoom and Microsoft Teams due to increased number of telecommuters and the increased need to use these communication tools. Malicious actors have exploited this situation and the lack of security measures such as passwords by hijacking online

meetings. (Ramadan et al., 2021, 6.) Attackers have also exploited the possibility to record and screenshot online meetings (Al Shammari et al., 2021, 2). In telecommuting, employees may use unauthorized ways of communication when communicating on work-related things. Authorized ways may be too complicated and not usable for the purpose, or people will use communication tools familiar to them, such as Facebook Messenger or personal email. This, of course, is a threat to information confidentiality. (Obada-Obieh, et al. 2021, 678.)

2.11 Physical security

The lack of physical security can lead to previously mentioned threats and thus it is discussed as its own chapter. Already mentioned physical security threats include lost or theft of device, outsiders' presence or physical access to confidential material which can include electronic as well as physical material. Poor physical security, including the environment where work is executed, can create cyber security threats.

Obada-Obieh et al. (2021, 680) noticed that while telecommuting other household members may hear and see things that are confidential. People in the same household may share working space or some cases the apartment can have such thin walls that you could hear discussions through them. In addition, household members could see computer screens with work-related information. The lack of secure working environment can risk organisation's as well as clients' data confidentiality. Obada-Obieh et al. (2021, 680) discussed also how some people feared that their house might be broken into. Work laptop could be stolen which could lead to loss of data availability, integrity, and confidentiality. In chapter 2.6 physical security risks for personal devices, especially mobile devices were discussed. These devices might be misplaced or stolen. It was also mentioned that public places can risk the physical security of devices. (Ganiyu & Jimoh, 2018, 52; 53.)

3 Cyber security guidelines as countermeasures

3.1 Cyber security policies and guidelines

Implementing information security policy (ISP) improves the overall security of an organisation (Aldawood & Skinner, 2018, 5). Information security policy can be seen even as the foundation for information security or something that combines all the security measures together (Lopes & Sá-Soarez, 2012, 2). Policies, standards, and guidelines have somewhat different meaning. One view is that's standards are something very specific, usually technical in nature. Policies and guidelines are the same in content, but policies are seen as mandatory and guidelines as voluntary in nature. (Wood, 1999, cited in Baskerville & Siponen, 2002, 338.)

Another view is that there are three types of policies. First, corporate security policy which represents the top management view. Second, organisational security policy which represents the users' view. Third, technical security policy which represents the designers' view. (Abrams and Bailey, 1995, cited in Baskerville & Siponen, 2002, 337.) There are also higher- and lower-level policies. High-level policies describe the security measure on more abstract level and low-level policies fulfil the high-level policies but are more specific and practical in nature. (Baskerville & Siponen, 2002, 339.)

This research concentrates on organisational security policy, in other words on the users' view. In addition, only the low-level policies are studied in this research. These low-level policies are called guidelines in this research as they provide guidance for the users rather than steer the organisations' whole cyber security management. No other separation between guidelines and policies is conducted in this research. In this research the word policy is mentioned more when reviewing the previous literature and the word guideline is used more when conducting theoretical framework and analysing empirical data. This is because the literature usually uses the word policy which can be, however, confusing when discussing on low-level guidance provided by the organisation to their employees.

In this research the low-level policies, in other words guidelines, act as an example of possible control measures for cyber security threats. This research investigates guidelines provided for employees, because many cyber security threats arise from the lack of knowledge of users. However, it is important to remember that information security policy must be modified to organisation's culture and working habits. However, some

basic principles are mentioned in almost every information security policy. (Höne & Eloff, 2002, 404.)

3.2 Telecommuting guidelines

The amount of cyber security threats increases but users lack the knowledge to make reasonable security choices. The end users may not understand security-related features systems and programs have and thus users neglect the necessary security measures. The usability of devices and systems should be improved. (Jang-Jaccard & Nepal, 2014, 990.) Better awareness could solve this problem. Organisations should prepare for cyber security threats by educating employees on the attacks and scams they may encounter. In addition, different technological solutions should be applied. These solutions should be easy to adopt and implement. (Dwivedi et al., 2020, 10-11.) However, information security cannot be manged only by using technological solutions. Appropriate human behaviour is crucial in order to maintain security which means that management and policies are important. (Bhaharin et al., 2019, 1.)

In telecommuting policy there should be mentioned how to take into account other policies as well, such as information security policy (Papagiannidis et al, 2020, 4). Organisations should make employees aware of the threats they may encounter in telecommuting. This way employees could secure their devices with the help of organisation's IT department. Necessary security software should be installed, and devices should be kept updated. IT department could filter and monitors spam emails. (Naidoo, 2020, 317.) However, in the survey of Georgiadou et al. (2021, 10) over half of the people working remotely due to pandemic were not given any security guidelines to follow. One solution would be to include telecommuting guidelines into information security policy.

In traditional information security policy, there should be mentioned the overall definition of information security as the policy is meant for people with different background without proper knowledge on information security. (Höne & Eloff, 2002, 403.) Because telecommuting has affected so widely, this can be seen important in telecommuting guidelines as well. The ability to adapt to this new telecommuting era also depends on the organisation's maturity. Some organisations have already had telecommuters in the past and they are more prepared to it than others. Thus, it depends on the organisation how

much adjustments and updates to company policies and actions are needed. (Conger, 2020, 329.)

For telecommuting, adequate cyber security guidelines are needed. For example, adequate policies can be one of the most effective ways to minimize social engineering attacks (Aldawood & Skinner, 2019, 6). In addition, as telecommuting differs from traditional work, it needs updated security policies from those that have been applied in secure office spaces (Lee & Lee, 2021, 2). So, it is important to decide guidelines and principles for telecommuting. One important aspect is that security guidelines for telecommuting should be mandatory. Strict, compulsory policies should be provided for telecommuting. (Lee & Lee, 2021, 11.)

Policies offer employees clear guidelines on how to behave and what are the consequences if those guidelines are neglected. In addition, without proper policies, employees do not understand their role in preventing cyber security threats. (Aldawood & Skinner, 2019, 6; 11.) James (2011, 134) concludes that telecommuting requires a specific security model. Different actions to include in a security policy were mentioned. These include network encryption, authentication, access control, data encryption, and separation and protection of temporary data. Also, additional security measures should be used with critical functions where telecommuting is not usually applied (Chigada & Madzinga, 2021, 9).

According to Georgiadou et al. (2021, 10) most common guidelines given to employees were the use of VPN, ensuring password safety, being aware of phishing, avoiding unsecure networks, locking workstation and ensuring daily updates. Taking into consideration the literature shown earlier, these seem adequate guidelines for telecommuters. Wang and Alexander (2021, 147) also perceive that one security measure for telecommuting are the policies. These policies should include not sharing work devices with other people, not accessing organisation systems on public WiFi and not saving corporate information on external cloud services or personal devices. Employees should also be taught how to handle information securely in home and the use of VPN.

D'arcy and Hovav (2009, 59) suggests that countermeasures for employees unwanted behaviour can be technical or procedural in nature. Procedural countermeasures include information security policy, usage guidelines, education, training, and awareness programs. However, telecommuters seem to be less affected by security policies, security

education, training and awareness (SETA) than those employees who work more in the office. This indicates that telecommuting would require specific actions in order to have adequate security guidelines. After the pandemic or as the situation becomes steadier, governments will probably also provide some policies and regulations relating to cyber security (Dwivedi et al., 2020, 11).

3.3 Mitigating common cyber security threats in telecommuting

3.3.1 Guidelines for personal and mobile devices

There are multiple countermeasures for maintaining the security of personal and mobile devices. One way mitigating the risks of BYOD are regular scans to employees' devices (Ramadan et al., 2021, 16). However, Bello Garba et al. (2015, 1281) addressed that monitoring BYOD devices and their usage can risk the user's privacy. Important for BYOD security are adequate policies, training and procedures. Papagiannidis et al. (2020, 3) state that mobile device management (MDM) is needed for any organisation that allows BYOD. MDM is a management system which helps in monitoring, keeping track of and configuring services. It helps IT to manage mobile devices and data. (Ganiyu & Jimoh, 2018, 54.)

Organisations have allowed employees to use their personal devices more flexible during the pandemic. However, organisations have not prepared for the wide use of personal devices. Simple actions such as backing up your information and using caution when downloading programs are also important in order to mitigate the risks when using personal devices. If physical security of device is compromised when the device is, for example, lost or stolen, employees should have clear protocol how to proceed. Employees should know who they have to report the incident and how. (Ramadan et al., 2021, 16-17.)

For those employees who work with functions that need high security, additional security measures should be applied. They should only use devices provided by the organisation. These devices should be highly secured. (Chigada & Madzinga, 2021, 9.) Technical countermeasures for personal devices include, for example, encryption, GPS system, firewalls and antivirus programs. GPS and encryption can help maintaining the security also if the device is lost or stolen. (Ganiyu & Jimoh, 2018, 50.) It seems that countermeasures include technical as well as managerial solutions. Adequate policies and

protocols for employees are an important aspect in mitigating these threats. Organisation could even have explicit BYOD policy for personal device usage in order to manage the threats relating to BYOD (Bello Garba et al., 2015, 1285).

Bello Garba et al. (2015, 1285) highlights the importance of clear policy in mitigating cyber security risks relating to personal devices and BYOD phenomena. They propose requirements for creating a BYOD policy. These requirements include but are not limited to the following (Bello Garba et al., 2015, 1285):

- Corporate information can be stored, modified and accessed only by those personal devices that have been officially enrolled.
- Highly confidential information as well as large quantities of data cannot be stored, modified or accessed from a personal device.
- Personal devices must have lock-screen that comes on automatically.
- Organisation can control what corporate information is accessed from the personal device.
- Downloading applications or malicious content is discouraged.
- Device should have updated antivirus program installed.
- Users should back-up their data but only to trusted hard drives.
- Lost or stolen device should be reported in 24 hours.
- Device should be able to be remotely wiped in the case of lost, theft or other security breach.

Different policies for mitigating the risks caused by the use of personal and mobile devices have been gathered in Table 4. As mentioned before, every organisation has somewhat different needs regarding information security policy, thus organisations should adapt different guidelines according to their needs.

Table 4 Guidelines for personal and mobile device usage

Guidelines for personal and mobile devices
Backing up information but only on trusted places
Using caution when downloading programs and applications
Protocol on how to proceed in case of lost or stolen device
Using devices provided by the organisation
Having updated antivirus program and firewall
Organisation can control what corporate information is accessed from the device
Having GPS system in case of lost or stolen device
Highly confidential information and large quantities of data should not be handled on personal device
Official enrolment of the device
Automatic lock-screen
Device should be able to be remotely wiped

Table 4 shows that the policies include actions towards the device as well as to employee behaviour. Devices should be as secured as possible but in addition employees should use caution in their everyday actions in order to keep the devices safe. Keeping the devices safe will also secure organisation's information and systems.

3.3.2 Guidelines for social engineering

The measures against social engineering tactics such as phishing include guidelines raising employees' awareness as well as more technical measures. Social engineering security measures include contacting IT department if devices are not working properly. In addition, antivirus program should be kept updated. Also, caution with passwords should be used. Countermeasures for phishing include caution with unknown links and attachments and caution with unknown email addresses and phone numbers. (Ramadan et al., 2021, 16-17.)

Ghafir et al. (2016, 147-148) suggest multiple defence mechanisms against social engineering. These include enforcing the information security policy. The policy should include guidelines, for example, to information release, passwords, help desk and destroying confidential documents. Regarding to information release, policy should clearly state which information can be publicly released. Guidelines for passwords should include how a strong password is created, such as using special characters and lower- and upper-case letters. Help desk should be clearly guided on password protocols and

information release. Destroying confidential material is important in telecommuting also as this study has shown that there may be outsiders present in telecommuting. Email security is also one of the most important things when preventing social engineering and phishing. Important aspect is also employees' awareness. (Aldawood & Skinner, 2018, 1; 3.)

Guidelines and policies are one of the most effective ways to minimize the cyber security threat caused by social engineering. Employees will be more aware of their actions and secure behaviour. (Aldawood & Skinner, 2019, 6-7.) Some proposed policies for social engineering are (Aldawood & Skinner, 2019, 7-8)

- Shredding all files with confidential information.
- Limiting the accessibility to confidential information.
- Guidelines on how to label confidential data.
- Auditing protocols for checking the security awareness of employees.
- Not allowing plug-in devices on workstations.
- Restricting the access to social media platforms.
- Monitoring employees' compliance.

Data confidentiality is maintained by shredding files with sensitive information. Also, when limiting the access to sensitive information, data leakages can be minimized. By regular audits, security culture is maintained in the organisation. By disallowing plug-in devices, unauthorized access can be prevented. Social engineering exploiting social media can be prevented by restricting employees' access to social media platforms. Monitoring employees' compliance supports organisation's security culture. (Aldawood & Skinner, 2019, 7-8.) Even though awareness is an important factor in mitigating social engineering and phishing, sometimes organisations' awareness programs can confuse people. Obada-Obieh et al. (2021, 682) recognized that when employees received fake phishing emails from the organisation as part of security awareness program, employees begin to think that some real emails from the organisation were phishing emails. Thus, awareness programs have to be well conducted in order them to work. Table 5 gathers the different guidelines for social engineering found in this study.

Table 5 Guidelines for social engineering

Guidelines for social engineering
Contacting IT department if device is not working properly
Updated antivirus program
Caution with unknown links and attachments
Guidelines for information release
Password guidelines
Destroying confidential material
Email security
Guidelines on labelling confidential data
Auditing protocol for employees' awareness
No plug-in devices
Social media protocols
Monitoring employees' compliance

Table 5 shows that guidelines for social engineering mostly deal with employees' behaviour. Employees need specific guidelines on how to behave in different situations.

3.3.3 Guidelines for cyber attacks

Countermeasures for DoS attacks include different security software such as antivirus program, intrusion detection and intrusion prevention systems. Countermeasures for ransomware attacks include backups of important files, email security guidelines and downloading only trusted software. As ransomware attacks can happen through phishing the safety measures for phishing attempt also mitigate the risk of ransomware attack. (Ramadan et al., 2021, 16-17.) Malware as well can spread through social engineering, thus the same safety measures apply also here. Different guidelines for mitigating cyber attacks have been gathered in Table 6.

Table 6 Guidelines for cyber attacks

Guidelines for cyber attacks
Antivirus, intrusion detection and prevention systems
Backing up information
Email security
Downloading only trusted software
Caution with social engineering

As Table 6 shows the risk of cyber attacks can be mitigated by technical measures as well as by human behaviour. Policies like backing up information is aimed to mitigate the consequences of an attack if it has already happened.

3.3.4 Guidelines for unauthorized access

Online meetings could be protected from attackers by keeping the meeting ID private, having waiting rooms for participators, having passwords for the meetings, and keeping the communication tools updated. (Curran, 2020, 11.) Other security measures or possible policies for unauthorized access are using strong passwords, changing them regularly and disabling third parties that are not relevant anymore (Ramadan et al., 2021, 16). Possible guidelines for mitigating the risks of unauthorized access have been gathered in Table 7. In Table 7 guidelines are divided to guidelines for online meetings and guidelines for other unauthorized access.

Table 7 Guidelines for unauthorized access

Guidelines for online meetings
Keeping online meeting ID private
Using passwords in online meetings
Keeping communication tools updated
Guidelines for other unauthorized access
General password protocols
Disabling unnecessary third parties

The cyber security for online meetings has been important during the pandemic as discussed in the chapter 2.10. Otherwise, strong updated passwords seem to be essential in mitigating unauthorized access. Unauthorized access can also be prevented by physical measures which are discussed in chapter 3.3.6.

3.3.5 Guidelines for unsecure networks

In order to maintain security while using other than organisation's network, employees should avoid risking the security of devices and information. As the previous literature have shown, public WiFis, not using VPN and not having proper security systems in your network can cause all kind of security risks such as DoS attack. Policies and guidelines should therefore clearly state that employees should avoid those factors while

telecommuting. Employees should use VPN and avoid public WiFis. Also, VPN should be secured otherwise it could lead to additional cyber security threats. (Chigada & Madzinga, 2021, 9.) The policies for network threats have been gathered in Table 8.

Table 8 Guidelines for network threats

Guidelines for network threats
Using VPN
Avoiding public WiFis
VPN should be secured

Table 8 shows that network security can be affected with employee actions which indicates that employees' awareness as well as complying to organisation policies are important.

3.3.6 Guidelines for physical security

Physical security guidelines focus on protecting devices from lost or theft and preventing outsiders from hearing or seeing organisation's confidential data. As explained in the chapter 2.11 physical security may be difficult to maintain if you have roommates or family in the house when you are working. Employers should be aware of diverse working environments employees may have when telecommuting. Not all employees have separate sound-proof rooms in their apartment. (Obada-Obieh, 2021, 685.) Employees could still be guided to work in a quiet and secure environment in order them to understand the threat of outsiders. As previous literature has shown confidentiality of online meetings is at risk if outsiders can hear employees work calls.

Theft or loss of device is also a threat to physical security. In case of a lost or stolen device, employees should know who to contact or where to report the incident in the organisation (Ramadan et al., 2021, 17). Locking your workstation is also recommended (Georgiadou et al. 2021, 10). Locking your workstation could prevent unauthorized access either accidental or done in purpose. Table 9 summarizes the possible guidelines for improving cyber security.

Table 9 Guidelines for physical security

Guidelines for physical security
Finding a quiet and secure place to work
Being cautious of theft or loss of your device
Contacting to organisation in case of an incident
Locking your workstation

Guidelines regarding to physical security concentrate on preventing unauthorized access. Confidential information is protected by preventing outsiders overseeing or overhearing things. It is also good to remember that unauthorized access may happen on malicious reasons or by accident.

3.4 Telecommuters' compliance with policies

Godlove (2012, 226) recognized that people working remotely agreed that information security in organisation is important. Employees were more eager to protect data and security when they were given the proper guidelines to do that. In addition, employees believed that they were able to follow security policies and guidelines. They also felt obligated to do that. The study, however, found only a weak to moderate link between employee's beliefs of information security (personal attitude, social pressure, sense of control) and compliance with security policies. However, it was stated that employees with the strongest personal attitude, feeling of social pressure, and sense of control were more likely to comply with the security guidelines. Employees' lack of compliance does not mean that they are not interested in security or protecting valuable corporate information. Usually, employees do not have proper cyber security awareness. This might be because of lack of policies or training. However, organisations should also take into consideration that strict policies can make employees feel like they are controlled which can increase the suspicion towards cyber security measures. (Kemper, 2019, 11-13.)

If the tools used for telecommuting are too complicated or they make working more difficult, employees may not comply with the assigned protocols. In addition, if employees feel that the usability of tools is low, they make workarounds which can cause a major security risk. Even organisation's IT may neglect the protocols because employees have usability issues due to security measures. (Obada-Obieh et al., 2021, 679-680). It seems that in some cases tightened security measures can lead to low usability of

tools. Further on this can lead to negligence of protocols and alarming cyber security risks.

4 Theoretical framework

In this research multiple cyber security threats occurring in telecommuting have been recognized. These can be more technical or social in nature but common for all of them is that they can be mitigated by proper guidelines provided for the employees. In this section main points from the previous literature have been gathered to create a theoretical framework shown in Table 10 and Table 11. The structure of the theoretical framework differs a little from the research's overall structure. In Table 10 personal devices have not been included as a threat but as predisposing factor as they are not a threat on their own but rather cause different cyber security threats. This applies to unsecure networks as well. The framework includes main cyber security threats in telecommuting as well as the factors causing them. Framework also offers guidelines for managing these threats.

Table 10 does offers higher-level topics where specific guidelines should be applied. For example, countermeasure for social engineering are guidelines for social engineering. Solution is not as straightforward in all the issues, because the guidelines for every threat are formed on the base of the predisposing factors. As previous literature on information security policy or guidelines have shown, organisations need to modify the policies for their culture and working habits. That is the reason Table 10 does not offer specific guidelines but rather general themes.

Table 10 Cyber security threats in telecommuting

Threat	Predisposing factor in telecommuting	Guideline
Malware	-Use of personal and mobile devices -Successful social engineering attempts	-Guidelines for personal and mobile devices -Guidelines for social engineering
DoS/DDoS-attack	-Unsecure networks -Use of mobile devices	-Network guidelines -Guidelines for personal and mobile devices
Ransomware	-Remote access to network -Successful phishing attempts	-Network guidelines -Guidelines for social engineering
Social engineering	-Lack of knowledge on manipulation techniques -Human error -Use of personal devices	-Guidelines for social engineering -Guidelines for personal and mobile devices
Unauthorized access	-Lack of security measures in communication tools -Poor password and security controls -Outsiders' presence in telecommuting environment	-Password guidelines -Online meeting guidelines -Guidelines for physical security
Physical security	-Use of mobile devices (as they are easily lost or stolen) -Outsiders' presence in telecommuting environment	-Password guidelines -Guidelines for physical security

Table 10 shows the most important high-level guidelines identified in this research which should be adapted in telecommuting. These are guidelines for personal and mobile devices, guidelines for social engineering, password guidelines, guidelines for physical security, online meeting guidelines, and network guidelines.

In Table 11 more specific guidelines are offered. Table 11 summarizes the findings of previous literature on different cyber security guidelines for telecommuting. Some guidelines may appear both as a guideline set and as specific guidelines, such as password guidelines do. This is because, for example password guidelines are important as their own but also an important control measure for other topics as well.

Table 11 Guidelines for telecommuting security

Guideline topic	Specific guidelines
Network guidelines	-Using VPN -Ensuring VPN security -Avoiding public WiFis
Guidelines for social engineering	-Contacting IT department if device is not working properly -Updated antivirus program -Caution with unknown links and attachments -Guidelines for information release -Password guidelines -Destroying confidential material -Email security -Guidelines on labelling confidential data -Auditing protocol for employees' awareness -No plug-in devices -Social media protocols -Monitoring employees' compliance
Guidelines for personal and mobile devices	-Backing up information but only on trusted places -Using caution when downloading programs and applications -Protocol on how to proceed in case of lost or stolen device -Using devices provided by the organisation -Having updated antivirus program and firewall -Organisation can control what corporate information is accessed from the device -Having GPS system in case of lost or stolen device -Highly confidential information and large quantities of data should not be handled on personal device -Official enrolment of the device -Automatic lock-screen -Device should be able to be remotely wiped
Password guidelines	-Passwords should be changed regularly -Passwords should include special characters, lower- and upper-case letters
Online meeting guidelines	-Keeping meeting ID private -Having passwords for meetings -Having waiting rooms for meetings -Having updates on the system
Guidelines for physical security	-Finding a quiet and secure place to work -Caution with theft or loss of your device -Contacting to organisation in case of an incident -Locking your workstation

Table 10 and Table 11 will be used as a base when analysing the cyber security and telecommuting guidelines and policies from universities. Table 10 shows the high-level guideline sets for telecommuting. These describe the topics which organisation's telecommuting or cyber security guidelines should address. Table 11 shows more specific controls for each guideline set. These are gathered to work as an example of practical controls. However, as discussed earlier, organisations need to modify policies for their operations and needs. Thus, these specific controls should not be interpreted as rules organisations must follow. The specific controls work as an example and baseline.

5 Methodology

5.1 Case study as a research method

This research is formed as qualitative research. The research method used is case study research. Case study can be conducted as a single-case study or as a multiple-case study. The method used in this research is the case study of multiple cases. More closely extensive case study research. This means that multiple cases are studied, and the objective is to find common patterns among them in order to make some generalisation. (Eriksson & Kovalainen, 2016, 133; 136.) In multiple-case study data can be analysed between cases. Even though single-case study may provide more in-depth analysis, multiple-case study allows the comparison and validation of data between different cases. (Cavaye, 1996, 237.)

Case study has different characteristics. Three key characteristics according to Benbasat et al. (1987, 370) are natural setting, why and how questions and little previous research on the subject. First of all, in case research the subject is studied in its natural environment, thus no manipulation is involved. Secondly, case study is especially suitable for how and why questions, as they are used when searching for profound answers. Thirdly, case study is an adequate research method when there is only little previous research on the subject. Case studies are used when deeper knowledge and understanding is needed. In addition, case study is a good method when dealing with different sources of information (Yin, 2009, 11.) This is useful if data from multiple sources is needed. Multiple-case study is used for description of phenomena, theory building or theory testing (Benbasat et al., 1987, 373). Case study can be exploratory, descriptive, or explanatory (Yin, 2009, 8). This research is most closely descriptive as the purpose is to describe the current state of organisations' cyber security management and guidelines in telecommuting.

Reflecting to the three key characteristic by Benbasat et al. (1987, 370), case study seems a suitable method for this research. First of all, the main research question is a how question. The purpose of this research is to understand widely and profoundly how cyber security can be managed in telecommuting. Secondly, research happens on a natural setting and no manipulation is involved partly because documentation is used as a data source. Documentation is not created specifically for this research, thus the setting is as

natural as possible. Previous literature on cyber security and telecommuting exists but as noticed from the previous literature, it has gaps.

The cases of this research are seven Finnish universities. In case study it is important to clarify what is the unit of analysis. Unit of analysis refers to what will the study focus on. Unit of analysis can be, for example, an individual or a whole organisation. In this study the unit of analysis is cyber security and telecommuting guidelines which each university provides for their employees. Site selection is also important. Site selection refers to what kind of organisations the data will be collected. (Benbasat et al., 1987, 372-373.) In this research universities were selected as the site. Universities are suitable target for this research as they are affected by the societal changes and movements. They also follow government regulations and recommendations closely. Because of these reasons universities have been affected by the pandemic and mass telecommuting which makes them an adequate target to analyse. Universities are also suitable for this as universities are big enough and have many employees. Small organisations may not have enough data to analyse.

5.2 Data collection

Case study often utilizes multiple data collection methods (Benbasat et al., 1987, 374). In this study documentation is used as the data source. There are multiple strengths for having documentation as your data. Data can be reviewed as often as it is necessary. In addition, documentation is not created specifically for the needs of the research. Documentation is also usually exact, including exact names, dates, and details. Documentation can also have broad coverage over different events and subjects. However, using documentations in case study research also includes some problems. Documentation can be hard to find and have access to. The data can be biased if the collection is incomplete. In addition, reporting the bias will reflect the researcher's bias. (Yin, 2009, 102.) In this research, especially problematic is the bias aspect because data collection cannot be guaranteed to be completely comprehensive.

The documentation data for this research consists of different guidelines universities have for their employees regarding telecommuting and cyber security. For this research guidelines from seven universities in Finland have been gathered. The objective is to find out what instruction universities have for their employees on secure behaviour in telecommuting. The cases are analysed based on theoretical framework showed in chapter

4. Seven universities cover half of the universities in Finland. These seven universities were picked because there was enough information on cyber security guidelines in order to create a clear image on cyber security and telecommuting. Different documents were analysed from each of the seven universities in order to find out how well cyber security is communicated to employees.

Some documents used in this study are gathered from universities' public websites and are public for everybody to see. Other documents have been gathered by contacting persons responsible for the information security in the university. Thus, some of the documents used are internal and cannot be find publicly. For some universities more than one document is analysed. Likely, this increases the richness of data even though all data is from documentation. Data richness is important in case study research for valid results (Benbasat, 1987, 374). Some documents are named as guidelines or tips and others as official instructions. Guidelines and policies are not necessarily aimed directly at telecommuters but in this study, it is analysed how these guidelines and policies work in telecommuting environment.

5.3 Data analysis

The data is analysed according to the qualitative research methods. Yin (2009, 130) suggests as one general analysis strategy to reflect the gathered data to chosen framework and theoretical background. The point is to use the same theoretical background that has guided the whole research. This is a good strategy for this study also as it makes the structure coherent and creates a clear link between theory and empirical data. Theoretical framework is conducted on the basis of previous literature on cyber security in telecommuting. In the analysis phase the structure of theoretical framework guides the analysis and data is reflected to it.

Even though no additional research on universities was conducted to determine the qualities of these organisations besides the documentation analysis, the results offer a view on how well cyber security is considered in the universities relating to telecommuting. No additional information of the universities was needed as the previous literature identified general cyber security threats in telecommuting and those threats are not limited to a specific field or organisation. Thus, these threats should be taken into account in various organisations regardless of the field or size of organisation, of course adjusting the actions to the context of the organisation.

The analysis for this research begun by reading through the gathered documentation. Second, guidelines were divided under the topics identified in this research and theoretical framework. Topics are guidelines for network security guidelines for social engineering, guidelines for personal and mobile devices, guidelines for physical security and password guidelines. Next, most common guidelines were identified. After the guidelines had been recognized and divided between topics, the guidelines were analysed reflecting to previous literature and theoretical framework. As a result, common features as well as conflicts were identified between university guidelines and previous literature.

In Table 12 all universities and their guidelines are introduced. Universities have alias names for confidentiality. Table 12 shows that some universities had more than one guideline for analysis. Some documents referred specifically to telecommuting and others were general cyber security guidelines. Nevertheless, in the analysis section of this research it is recognized that general cyber security guidelines also included guidelines for telecommuting. Table 12 includes page numbers of different guidelines as well as the source of the guidelines. Sources are divided to private/public and document/text. Public guidelines are public for everybody in university's extranet. Private guidelines on the other hand are not accessible for everyone because they are accessible from intranet or other internal sources. Guidelines are shared with employees in plain text in website or as a separate document. The separation between documents and plain text helps to understand the source or type of data. If guideline is marked as text, it is not a separate document. Sources marked as documents are separate documents linked in websites or shared internally with university's employees.

Table 12 Universities' guidelines

University	Guideline	Pages	Source
University A	Tietoturvan top-10 vinkit	5	Private/Document
University B	Staff's information security guide	16	Public/Document
University C	Tietoturva ja tietosuoja etätyössä	3	Public/Text
	Tietoturvan pikaohje henkilöstölle	1	Public/Text
University D	Henkilöstön tietoturvaopas	16	Public/Document
University E	Telework	5	Private/Document
	Tietoturvan pikaohje	2	Public/Text
University F	Lyhyt tietoturvaopas	7	Private/Text
University G	Tietoturvaohje	7	Private/Document
	Tietoturvan muistilista	1	Private/Document
	Turvallisuusvinkit etätyöhön	2	Private/Document

6 Analysis

6.1 General

In the analysis it was discovered that four universities had the same base for their cyber security handbook. It is conducted together with several universities in Finland. Some universities have altered the handbook a little for their organisation, however the handbooks are very similar. This can be seen practical as universities operate on the same field and have rather similar process and requirements for information handling. However, this can be seen as problematic for this research as it may create bias.

Six of seven universities had addressed telecommuting directly in their guidelines. Only university F did not address telecommuting specifically in its guidelines. These specific telecommuting guidelines were analysed under the topic areas identified in previous literature and theoretical framework. Security of online meeting were addressed little or not at all, however there were some general guidelines that can be applied such as not letting outsiders hear your phone calls. Nevertheless, secure online meeting protocols should be communicated with staff as outsiders' presence is a real threat in telecommuting, especially during the Covid-19 when many people are working from home.

Generally, universities' guidelines cover the different threats of telecommuting well. All universities had some guidelines regarding to networks, social engineering, personal and mobile devices, passwords, and email security. Some of these topics were addressed better than others and there is still a room for improvement. These are discussed more closely on the next chapters where guidelines are analysed based on the structure of the theoretical framework.

6.2 Network security

Each of the seven universities that were studied in this research had some guidelines regarding network security. Most common guidelines were the use of VPN, avoiding wireless connections and disabling them when not in-use. However, some conflicts between the guidelines occurred. University C guided their employees not to use VPN when browsing personal purposes on internet as this burdens the VPN service when it is already in high use due to pandemic. In addition, some universities stated that it is not

necessary to use VPN when using already encrypted websites (https). This can confuse employees as the use of VPN where otherwise encouraged. Guidelines provided by the universities line well with previous literature. First of all, use of VPN is seen important in the previous literature as well (Wang & Alexander, 2021, 147). In addition, previous literature recognized using public wireless connections risky as they can expose organisation's network to viruses and data leakages (Chigada & Madzinga, 2021, 5).

Even though, universities had addressed network security well in their guidelines, there is still some room for improvement. Universities advise their employees not to use public wireless connections. However, only university E give more specific advice. University E guided its employees to consider using mobile phone's connection if there is no secure connection available. This seems like a good advice especially if university has a smart phone with good internet connection as a fringe benefit. University E also stated that public WiFi could be used if it has a password, and employee's computer is fully updated. As shown in the previous literature, people may use public connections because they do not have proper resources (Baz et al., 2021, 645). Thus, it would important that organisations would offer these resources, for example, by providing a phone benefit with internet access and guiding employees to use it when there are no secure networks available.

Overall, the findings from university guidelines match with the recommendations given in the previous literature. However, there is something organisations should take into account when providing guidelines for their employee. As it was said by Obada-Obieh (2021, 681) employees' lack of technical knowledge can lead to misunderstandings on security measures. In the paper some employee believed that VPN secures the whole computer as they did not understand what VPN was. Thus, it would be important to explain to employees why different countermeasures are in place. This could raise the awareness of employees and probably improve cyber security.

6.3 Social engineering

Guidelines for social engineering were overlapping with email security guidelines. Thus, organisation's email guidelines are analysed together with social engineering guidelines where applicable. For example, university A had guidelines regarding social engineering under the email security guidelines. Most common guidelines relating to social engineering were advising users to be cautious with fake websites, advertisements and

popups, spam emails, phishing scams asking for personal data such as passwords and user IDs, and suspicious links. Many of these guidelines were addressed in the previous literature. For example, learning to identify fake websites were mentioned in the guidelines of six universities. Ramadan et al. (2021, 9) mentions fake websites as a method for scams. In addition, Chigada and Madzinga (2021, 6) noticed that during Covid-19 attackers have exploited fake websites. Caution with links and attachments were also recognized by Ramadan et al. (2021, 16). All the seven universities advised their employees to be cautious with links. Phishing scams and spam emails were also emphasized in the previous literature. Previous literature also showed how attackers try to gain users passwords and other identification information, thus it is good to inform employees on these.

Even though universities had relevant guidelines that were also addressed in the previous literature, some things differed from the previous literature. Scams relating to specifically Covid-19 were mentioned only by university E. Ramadan et al. (2021, 9) had identified that attackers have exploited the pandemic. Spam emails including Covid-19-related information have been common during the last few years. However, only one university provided Covid-19 specific guidance which is interesting as updating cyber security policies is recommended when major changes happen in the operating environment (ISO / IEC 27002, 2013, 3). It seems that most of the universities have not adequately updated their policies. This can be seen alarming, and it would be important for organisations to update their guidelines more actively if something as major as worldwide pandemic occurs.

Another thing previous literature addressed but university guidelines did not was labelling and releasing information. Previous literature had recognized labelling information and instructions for information release important in preventing social engineering. As this would be important in cyber security generally, it is interesting that universities do not mention information labelling or information release at all. Ghafir et al. (2016, 147-148) mentioned how information security policy should include guidance on information release in order to prevent social engineering. Social engineering exploits information on organisations and employees which makes it important to protect confidential information adequately. Universities may address data classification and information release in a different document. However, it should still be referred in the guidelines as it is relevant when mitigating the risks of social engineering. University C mentioned some rules for

data handling in different services. University C had a table where it was described what kind of data is acceptable to handle in different services. Different classifications of data were shown, but description of the classification was not included. Thus, guidelines for data labelling and information release are something universities should improve and make more visible.

All in all, it seems that universities have diverse and applicable social engineering guidelines for their employees. Some topics were not addressed in the guidelines such as data labelling and information release, and Covid-19 specific threats. These are improvement areas for universities, but overall universities had provided comprehensive guidelines on social engineering for their employees. As previous literature has shown specific policies and guidelines must be modified for each organisation, thus, guidelines may differ from the ones literature has recognized (Höne & Eloff, 2002, 404). In addition, as raising awareness among employees is one important factor in mitigating the threat of social engineering, diverse guidelines would seem to be adequate for the purpose.

6.4 Security of personal and mobile devices

Most common guidelines regarding the use of personal and mobile devices were using antivirus programs and firewalls, avoiding downloading unnecessary and unsecure applications, keeping devices updated, avoiding sharing location, doing regular backups, having a password in your mobile device in addition to PIN-code, primarily using devices provided by the employer and making sure no one else have access to you work devices. Some of these guidelines were also mentioned in the previous literature such as information backups, antivirus and firewall programs, caution when downloading software and using the devices provided by the organisation. However, some guidelines were conflicting. On one hand, previous literature has suggested using GPS on for locating your device in case of loss or theft (Ganiyu & Jimoh, 2018, 50). On the other hand, five universities advised their employees not to share location. There is justification for both. Not sharing your location protects your privacy but keeping your GPS on helps to find a stolen or lost device. Universities' guidelines concentrated on not sharing your location in online services. Thus, users could keep their GPS on but not allow online services to use that location.

Five universities advised their employees to use devices provided by the organisation. This would seem to be efficient countermeasure for cyber security threats of personal

devices. However, if the device provided by the organisation is a mobile device, it is still vulnerable to those mobile device threats identified in previous literature. Especially mobile devices are easily stolen or lost. Universities have taken this into account by advising their employees to use additional password in mobile devices. Regular backups are also important for securing the availability of data if the device is lost or stolen. However, universities did not communicate any clear protocol for employees in case of loss or theft of a device. Previous literature suggested that a protocol is needed for those situations. Universities did guide their employees to contact IT when suspecting something, but this related more to scams and cyber security violations. Thus, more clear protocol should be in place.

Universities did not fully restrict the use of personal devices for work-related purposes. No official enrolments of the personal devices were required, and the security of personal devices were mainly in the responsibility of the user. Bello Garba et al. (2015, 1285) addressed that official enrolment of personal devices should be in place. Official enrolments of devices are something organisations should consider if allowing the use of personal devices in work.

In addition to the common guidelines almost every university had, there were some other interesting findings. University E had guidelines on connecting devices to university network regularly in order to update the device. This supports the guideline of having devices updated all the time. It also takes the responsibility away from employees as updates are installed automatically when connecting to university network.

Another interesting finding was that some universities advised employees to create separate accounts for administrative tasks and other tasks. This is important for personal devices as employer cannot restrict the administrative rights of users. Administrative accounts are a wanted target for attackers as attackers can make the accounts more vulnerable to other attacks or add accounts. Users with administrative access rights should have different accounts for administrative tasks and other tasks. (Center for Internet Security, 2021a, 21.) This was addressed by four universities. However, this is not relevant if employees use organisation’s devices, and employees are not granted administrative access rights. As mentioned earlier, most of the universities at least encouraged employees to use devices provided by the university for work-related purposes. However, university A did not advise its employees either having separate

accounts for administrative tasks or using only devices provided by the organisation. Without any additional information this seems like a vulnerability for university A.

Overall, cyber security guidelines relating to personal and mobile devices were comprehensive. For example, proper security programs were suggested, use of university's devices were recommended, and separation of administrative and other accounts was mentioned. However, some improvements should be considered such as official enrolment of personal devices.

6.5 Password security

The most common issues mentioned in the guidelines regarding password security were avoiding writing down your password anywhere to be seen, not letting anyone to know your password, changing password regularly and if the password has been compromised, choosing a password you remember easily but which is hard for others to guess, and using different password in external services.

Some of these guidelines were also addressed in the previous literature. Wang and Alexander (2021, 146) recognized that in different services different passwords should be used. Other things mentioned in the previous literature were changing password regularly and using strong passwords (Ramadan et al., 2021, 16). Ghafir et al. (2016, 148) suggested the use of lower- and upper-case letters and special character. Even though the guidelines arisen in the previous literature were addressed well, little specific guidance on choosing your password were given to university employees. More specific guidance was provided only by few universities. University G advised its employees to use password sentences rather than simple words. Long passwords were recommended by university G and A. University E advised not to use words related to you in passwords.

All the guidelines provided by the universities highlight the importance of keeping your password private. As this may seem obvious, attackers exploit simple ways to acquire people's passwords such as simple asking them (Ghafir et al., 2016, 147). Thus, it is important to clarify for employees that no one, even the system administrative, needs your password. Employees should not be using easy passwords as attackers can figure them out and then penetrate the organisation's systems (Ramadan et al., 2021, 6). However, password should not be too difficult for the user to remember because that can lead to writing it down which is strongly warned in the universities' guidelines.

As passwords may be hard to remember users have the same password in multiple systems which creates a risk if one of these systems is compromised (Mulligan & Elbirt, 2005, 11). In addition, because remembering multiple passwords is hard, regular and mandatory password change is not recommended. Users may use more predictable passwords if they are forced to change them often, for example choosing a very similar password to the old one. However, password changes should be demanded if password is suspected to be compromised, user roles are changing, or the user leaves the organisation. (Center for Internet Security, 2021b, 9.)

Although the four most common guidelines universities have provided tackle password-related problems in theory, users may not follow the guidelines. As a solution, universities could advise their employees to use a password management system to manage their passwords. Password management system will store all the users' passwords securely using cryptography. These passwords are accessed by using one master password. This way user does not need to remember multiple passwords. (Mulligan & Elbirt, 2005, 12.) If the password management system controls the passwords, users do not have to create risky workarounds in order to remember all passwords they use. Only university A advised its employees to use a password management system.

All in all, universities had comprehensive guidelines on secure passwords. The guidelines lined well with previous literature and even exceeded them. Universities, and organisations in general, could still consider other measures for password security such as password management systems which was introduced in the chapter.

6.6 Physical and online meeting security

As previous literature showed, physical security is important in telecommuting. The security of online meetings is discussed in this same chapter as acknowledgements regarding online security relate to physical security. Most common things mentioned relating to physical security were locking your screen when leaving the workstation, protecting device from lost or theft and storing printouts in a secure way. Employees were advised, for example, to encrypt their device's hard drives for protecting their devices from loss or theft. However, as identified earlier with personal and mobile devices, no clear protocol was provided. Previous literature highlighted outsiders seeing and hearing confidential information, locking your screen and loss or theft of devices. The university guidelines addressed these but not in very comprehensive way.

Outsiders hearing or seeing confidential information was addressed poorly. Only three universities guided employees to keep device's screen safe from outsiders. University E even mentioned that employees should not have their screens facing to windows. Previous literature has shown that employers may assume that everyone has the same telecommuting environment: home which is shared with family, and which has separate rooms (Obada-Obieh, 2021, 685). However, as this is not the case with everyone, employers should also consider the possibility of outsiders' presence in employees telecommuting environment.

Online meetings have been very common during Covid-19 pandemic. However, university guidelines addressed online meetings or calls very little. Four universities mentioned that employees should ensure that outsiders do not hear work-related calls or confidential information. University E addressed issues relating to online meeting security most widely. University E guided employees to use headset instead of speaker and avoid saying names when making confidential phone calls. In addition, sound proofing was suggested. Use of encrypted emails is encouraged over calls if confidential matters cannot be discussed in a safe environment. University guidelines did not mention any of those guidelines that were addressed in the previous literature such as keeping meeting ID private and having passwords for online meetings.

All in all, physical and online meeting security were not addressed very widely in the university guidelines. The previous literature on the topic was also limited. Thus, it can be that physical security is not a major problem in cyber security or the importance of the topic is not understood. Second assumption seems more believable as previous literature had identified problems relating to the physical security in telecommuting.

6.7 Topics outside the theoretical framework

Universities had some other guidelines in addition to the theoretical framework of this research. Most universities mentioned that employees should not use USB sticks as a primary storage place for data as they are easily lost and accessed. However, if employees are using USB sticks, they should be encrypted ones. Another guideline relating to storing data advised employees to use university file storage or cloud services provided by the university when storing data. The guidelines for storing data in a secure way are relevant as universities also advised their employee to take backups.

All universities stated that employees should inform IT if they suspected a security breach. It was also mentioned in previous literature that employees should know who to contact in case of incident (Ramadan et al., 2021, 17). Incident can be also a loss or theft of device. It is important that employees know who to contact in such cases. Previous literature also mentioned that organisation IT should be contacted if device is not working properly, referring to situations where social engineering and scams are possible or suspected. (Ramadan et al., 2021, 17.)

7 Evaluation and conclusion

7.1 Evaluation of the quality and reliability of the research

Qualitative research cannot be necessarily evaluated the same way as quantitative research. Qualitative research can be evaluated by four aspects. These are dependability, transferability, credibility, and conformability. Dependability means that the research process has been logical, traceable, and documented. Transferability refers to showing similarities between previous research and the research in question. Credibility inspects whether the research claims are logical relating to the data and if someone else could interpret same issues with the same data. Conformability refers to situation that findings are linked to the data in an easily explainable way. (Eriksson & Kovalainen. 2016, 307-308.)

Yin (2009, 40-42) proposes four tests to guarantee the quality of case study research. These are construct validity, internal validity, external validity, and reliability. Construct validity means that the research should use specific measures to study the phenomenon. This way, it is guaranteed that the results of the research are not only subjective impressions of the researcher. This test is especially difficult to execute in case study research. However, there are ways to improve construct validity in case studies. These tactics are using multiple sources of evidence, establishing chain of evidence, and having key informants review draft of case study.

In this research especially the principle of chain of evidence is followed. The key point in chain of evidence is that an external reader can follow how the conclusions have been made from the used data and how the initial research question is addressed (Yin, 2009, 122). In this research conclusions relate closely to the collected data and the data clearly is referred. Also, relevant information from empirical data is given to the reader, such as names and sources of the documentation. Analysis is formed from the theoretical framework which in turn reflects the research question: How to address telecommuting in cyber security guidelines and policies?

Internal validity is studied only for explanatory and causal studies, thus it is non-applicable for this descriptive study. External validity is about the generalization of the results. External validity can be a problem especially in single-case studies. For multiple-case study replication logic should be used in order to increase external validity.

Replication logic means that research should be tested by replicating the findings for other cases where the findings should apply according to the initial research. (Yin, 2009, 42-43.) This research could be tested by replicating the findings in other organisations.

Reliability means that the research could be executed again with the same results. The key point is that the errors and biases would not affect to the findings. The different steps of the research should be documented in order to achieve reliability. (Yin, 2009, 45.) The steps of conducting this research have been described in introduction and methodology sections. In addition, there is some documentation on the different stages of conducting the research and handling the data, for example, the phases for analysing the data. All in all, relevant aspects for the evaluation of the quality and reliability of this research have been taken into account.

7.2 Conclusion

Telecommuting includes various cyber security threats which organisations should address in their cyber security guidelines. This research found cyber attacks, social engineering, unauthorized access, and unsecure physical environment as the most critical ones. Identified factors causing those threats are use of personal and mobile devices, social engineering, unsecure networks, unsecure online communication, poor password security, human error and outsiders' presence in the working environment. Previous literature has shown that policies and guidelines are important in maintaining cyber security in organisations (Aldawood & Skinner, 2018, 5). Thus, relevant guidelines were identified in order to mitigate the common cyber security risks occurring in telecommuting. These cyber security guidelines are guidelines for personal and mobile devices, guidelines for social engineering, network guidelines, guidelines for physical security and online meetings, and password guidelines.

Overall, the content of university guidelines was wide and thus proper for guiding employees and raising the cyber security awareness. However, some specific concepts were not addressed adequately, such as choosing a secure network or password, which could lead to negligence of guidelines or unintended unsecure behaviour. All universities had guidelines for social engineering, personal and mobile devices, network security, passwords, and physical security. Online meeting security was not addressed by every university. Only university F did not address telecommuting specifically in its guidelines. General cyber security guidelines apply partly to telecommuting as well, but

telecommuting has also some special features that should be addressed and communicated to employees. Thus, it would be important to have also specific telecommuting guidelines. University E clearly stands out from others by having more specific and wider guidelines. University E did have a separate document on telecommuting security which explains the comprehensive guidelines. Separate telecommuting guideline seems to be effective for addressing all relevant cyber security threats.

Network security and social engineering were addressed comprehensively reflecting to theoretical framework and previous literature. For social engineering, multiple guidelines relating to email security were mentioned as well as general guidelines on suspicious activity on internet or other sources. As attackers use multiple methods for gaining valuable information, it is important to educate employees on different scams such as fake websites or phishing via telephone. For network security use of VPN was mentioned by six universities and avoiding wireless connections were mentioned by five universities. Password security and use of personal devices were also addressed rather well. Some improvements for addressing these topics were identified. Password management system and official enrolment of personal devices are something organisations could considered.

Physical security was addressed poorly among the universities. This would need more recognition in the organisations' cyber security guidelines. Physical security is identified to be important in the telecommuting. It is also identified that employers may not understand the actual working environment some employees have when telecommuting. (Obada-Obieh, 2021, 685.) Thus, it would be important to address this issue more and create guidelines which work in different working environments. Online meeting security was also addressed poorly. Organisations should create specific guidelines for online meetings. In addition to general guidelines preventing outsiders overhearing or seeing confidential information, guidelines could include keeping the meeting ID private, having passwords to meetings, having waiting rooms and keeping applications updated (Curran, 2020, 11).

Data labelling and information release is another topic that should be addressed better. Universities did not address data classification or labelling of data in their guidelines. Outside attacks and vulnerabilities are recognized fairly well but employees are not advised how to behave with confidential material. There are some exceptions. Email

encryption is mentioned by five universities. However, if data classification is not communicated to employees, they may not know what classifies as sensitive data. Covid-19-related threats were also addressed in the guidelines very little. As the previous literature has shown the pandemic have changed working environment and working habits widely (Papagiannidis et al., 2020, 1-2). As this has been a major change in many organisations, guidelines should be updated accordingly (ISO / IEC 27002, 2013, 3). Relevant threats should be communicated to employees in order to maintain secure working habits.

Physical security, online meeting security and Covid-19 specific threats were addressed poorly, and they all have been relevant especially during the pandemic and mass telecommuting. Physical environment where employees work is drastically different from office environment, especially if employees do not have any separate room dedicated to working. Online meetings have been crucial when face-to-face communication has been impossible or at least minimized. Even though universities addressed many issues comprehensively, these topics were not.

It seems that university guidelines are not updated for the current situation. As mentioned before, policies and guidelines should be reviewed and updated regularly. In addition, if a major change occurs in the operating environment, reviews and updates should be conducted. Conclusion from this research is that universities have mostly adequate cyber security guidelines for telecommuting, but these guidelines are not completely up to date. Organisations should review and update their policies and guidelines regularly and in case of a major change. This is not yet happening.

8 Limitations and future research

8.1 Limitations

There are some limitations to this research. First of all, studying only universities is a limitation that can cause bias. Even though, it was necessary to define the scope of this study narrow enough, the results may not be completely applicable to another organisational concept. However, studying universities provides a good baseline for future research as common issues and strengths are recognized.

Another limitation refers to previous literature. As literature uses terms policy, standard and guidelines mixed, it was necessary for this research to decide that all low-level instructions are defined as guidelines. However, this is partly confusing as literature does not make a clear line between these terms even though in practice policies often refer to high level decisions and act as the basis for standards and guidelines. This can cause different interpretations from the literature and this research. In order to avoid those, distinction and similarities between terms are tried to be explained very clearly in this research. Out of scope topics also create some limitations to this research. Those are discussed in the chapter 8.2 as possible topics for future research.

8.2 Future research

This study does not take into account SETA-programs: cyber security training and awareness building among employees. These could also mitigate the cyber security threats occurring in telecommuting. D'arcy and Hovav (2009, 59) mentions that SETA-programs may not affect telecommuters as efficiently as other employees. This would be an interesting future research topic. In addition, this study does not consider other security measures for telecommuting such as technical measures. Relevant technical controls for improving the cyber security in telecommuting could be studied.

Data protection, such as GDPR, and privacy of employees were not taken into consideration in this research. For future research employees' privacy in telecommuting could be studied. Nurse et al. (2021, 5-6) mentions that telecommuting may create a threat to employees' privacy. Privacy can be at risk due to monitoring from the employer, information gathered by different smart devices used in work and incautious usage of communication tools.

Another subject for future research could be employees' compliance. This research concluded that universities have overall adequate cyber security guidelines in telecommuting. However, as previous literature showed cyber security breaches in telecommuting are common. This raises a question if employees are complying with the provided guidelines. It would be also interesting to study how compliance differs in telecommuting environment compared to traditional office environment. In addition, this research does not take into account how well the guidelines reach employees. Employees may be unaware of the existence of those guidelines, or the guidelines are not applied in practice. This and general awareness of telecommuters is something that should be studied more deeply. Future research could also study what positive effects telecommuting has for cyber security, if any. Could, for example, the convenience of telecommuting give employees more time to educate themselves on secure ways of working?

These are all relevant future research topics for increasing the coverage of the literature on cyber security in telecommuting. As telecommuting is a big trend and at the same time cyber security threats are becoming more common, these topics should be addressed in literature as well as recognized by organisations.

References

Al Shammari, A. – Maiti, R. R. – Hammer, B. (2021). Organisational security policy and management during Covid-19. *In SoutheastCon 2021,* 1-4.

Aldawood, H. A. – Skinner, G. (2018). A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications. *In 2018 26th International Conference on Systems Engineering (ICSEng),* 1-6.

Aldawood, H., – Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security (IJS)*, Vol. 10(1), 1-15.

Allen, T. D. – Golden, T. D. – Shockley, K. M. (2015). How effective is telecommuting? Assessing the status of our scientific findings. *Psychological science in the public interest*, Vol. 16(2), 40-68.

Baskerville, R. – Siponen, M. (2002). An information security meta-policy for emergent organisations. *Logistics information management*, Vol. 15(5/6), 337-346.

Bayuk, J. L. – Healey, J. – Rohmeyer, P. – Sachs, M. H. – Schmidt, J. – Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons, New Jersey.

Baz, M. – Alhakami, H. – Agrawal, A. – Baz, A. – Khan, R. A. (2021). Impact of COVID-19 Pandemic: A Cybersecurity Perspective. *Intelligent Automation and Soft Computing*, Vol. 27(3), 641-652.

Bello Garba, A. – Armarego, J. – Murray, D. (2015). Bring your own device organisational information security and privacy. *ARPN Journal of Engineering and Applied Sciences*, Vol. 10(3), 1279-1287.

Benbasat, I. – Goldstein, D. K. – Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, Vol 11(3), 369-386.

Bhaharin, S. H. – Asma'Mokhtar, U. – Sulaiman, R. – Yusof, M. M. (2019). Issues and trends in information security policy compliance. *In 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. 1-6.

Cavaye, A. L. (1996). Case study research: a multi-faceted research approach for IS. *Information systems journal*, Vol. 6(3), 227-242.

Center for Internet Security (2021a). CIS Critical Security Controls. https://www.cisecurity.org/controls, retrieved 13.3.2022

Center for Internet Security (2021b). CIS Password Policy Guide. https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide, retrieved 24.2.2022

Chigada, J. – Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, Vol. 23(1), 1-11.

CNN (20.3.2020). Millions of Americans are suddenly working from home. That's a huge security risk https://edition.cnn.com/2020/03/20/tech/telework-security/index.html, retrieved 28.10.2021.

Conger, S. (2020). The impact of the COVID-19 pandemic on information systems management. *Information Systems Management*, Vol. 37(4), 327-331.

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security*, Vol. 2020(6), 11-12.

D'Arcy, J. – Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, Vol. 89(1), 59-71.

Dwivedi, Y. K. – Hughes, D. L. – Coombs, C. – Constantiou, I. – Duan, Y. – Edwards, J. S. – Gupta, B. – Lal, B. – Misra, S. – Prashant, P. – Raman, R. – Rana, N.P. – Sharma, S.P. – Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, Vol. 55. 1-20.

Eriksson, P. – Kovalainen, A. (2016) *Qualitative methods in business research*. 2nd edition. SAGE publications, California.

Flores, D. A. – Qazi, F. – Jhumka, A. (2016). Bring your own disclosure: analysing BYOD threats to corporate information. *In 2016 IEEE Trustcom/BigDataSE/ISPA*, 1008-1015.

Ganiyu, S. O. – Jimoh, R. G. (2018). Characterising risk factors and countermeasures for risk evaluation of bring your own device strategy. *International Journal of Information Security Science*, Vol. 7(1), 49-59.

Gartner.com (2021) The Top 8 Security and Risk Trends We're Watching. https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021/, retrieved 28.10.2021.

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

Ghafir, I. – Prenosil, V. – Alhejailan, A. – Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. *In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, 145-149.

Godlove, T. (2012). Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective*, Vol. 21(4), 216-229.

Godoy, L., de – Ferreira, M. G. G. – Robertson, M. M. (2021). COVID-19 and Teleworking from Home: Understanding New Issues from a Macroergonomic Perspective. *In 21st Congress of the International Ergonomics Association*, 672-679.

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

Höne, K. – Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & Security*, Vol. 21(5), 402-409.

ISO / IEC 27002 (2013). Information technology – Security techniques – Code of practice for information security controls

James, P. (2011). Are existing security models suitable for teleworking? *9th Australian Information Security Management Conference*, 130-139.

Jang-Jaccard, J. – Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, Vol. 80(5), 973-993.

Kaspersky.com (2021). Top Ten Cybersecurity Trends. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends, retrieved 28.10.2021.

Kaur Chahal, J. – Bhandari, A. – Behal, S. (2019). Distributed Denial of service attacks: a threat or challenge. *New Review of Information Networking*, Vol. 24(1), 31-103.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, Vol. 2019(8), 11-14.

Khan, N. – Brohi, S. – Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic*, TechRxiv*, 1-6.

Lee, C. – Lee, K. (2021). Factors Affecting Corporate Security Policy Effectiveness in Telecommuting. *Security and Communication Networks*, 1-13.

Lee, M. G. (2012). Securing the human to protect the system: Human factors in cyber security. *In 7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, 1-5.

Lopes, I. M. – Sá-Soares, F. D. (2012). Information security policies: a content analysis. *In PACIS-The Pacific Asia Conference on Information Systems*, 1-15.

Medina-Rodríguez, C. E. – Casas-Valadez, M. A. – Faz-Mendoza, A. – Castañeda-Miranda, R. – Gamboa-Rosales, N. K. – López-Robles, J. R. (2020). The cyber security in the age of telework: A descriptive research framework through science mapping. *In 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI)*, 1-5.

Mulligan, J – Elbirt, A. J. (2005). Desktop security and usability trade-offs: An evaluation of password management systems. *Information Systems Security*, Vol. 14(2), 10–19.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, Vol. 29(3), 306-321.

Nandal, S. K. – Kajal, A. (2020). Cyber Security against DDoS, Malware, Spoofing attacks using Machine Learning with Genetic Algorithm. *International Journal of Advanced Science and Technology*, Vol. 29(5), 5388 – 5400.

Northeastern.edu (2021). Cybersecurity Trends Emerging in 2022. https://www.northeastern.edu/graduate/blog/trends-in-cybersecurity/ retrieved 28.10.2021.

Nurse, J. R. – Williams, N. – Collins, E. – Panteli, N. – Blythe, J. – Koppelman, B. (2021). Remote working Pre-and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy. *In 23rd International Conference on Human-Computer Interaction*, 1-8.

Obada-Obieh, B. – Huang, Y. – Beznosov, K. (2021). Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers. *In Seventeenth Symposium on Usable Privacy and Security ({SOUPS} 2021)*, 675-694.

Papagiannidis, S. – Harris, J. – Morton, D. (2020). WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic. *International Journal of Information Management*, Vol. 55, 1-5.

Ramadan, R. A. – Aboshosha, B. W. – Alshudukhi, J. S. – Alzahrani, A. J. – El-Sayed, A. – Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, 1-19.

Skryl, T. V. (2021). The Role of Telework in Digital Economy. *In Complex Systems: Innovation and Sustainability in the Digital Age*, 201-208

Smith, K.T. – Jones, A. – Johnson, L. – Smith, L.M. (2019). Examination of cybercrime and its effects on corporate stock value. J*ournal of Information, Communication and Ethics in Society*, Vol. 17(1), 42-60.

Solms, R., von –Niekerk, J., van (2013). From information security to cyber security. *Computers & Security*, Vol. 38, 97-102.

Van‘t Wout, C. (2019). Develop and maintain a cybersecurity organisational culture. *In ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS*, Vol. 457.

Wang, L. – Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. *AIMS Electronics and Electrical Engineering*, Vol. 5(2), 146-157.

Yin, R. (2009). *Case study research: Design and methods*. 4th edition. SAGE publications, Los Angeles.