Tampereen yliopisto

Mika Liukkonen

CYBER SECURITY OF MULTI-LOCATIONAL WORK IN MODERN ORGANISATION

Faculty of Information Technology and Communication Sciences
M. Sc. Thesis
April 2022

ABSTRACT

Mika Liukkonen: Cyber Security of Multi-Locational Work in Modern Organisation
M.Sc. Thesis
Tampere University
Master's Degree Programme in Human-Technology Interaction
April 2022

Multi-locational work has become an integral part of working life in recent decades, and during the Covid-19 pandemic, it has continued to increase. The probability of certain cyber security risks has increased with this change.

Based on the literature, this thesis presents the key cyber security risks in multi-locational work. The risks were categorized in four levels according to who is primarily responsible of the risk. The categories being primarily employee's responsibility, shared responsibility between the employee and the organisation, primarily organisation's responsibility and abstract responsibility. The risk analysis matrix was chosen to illustrate the level of risk as it considers both severity and probability of the risks.

The empirical part of the study was conducted as a case study focusing on cyber security in a modern Finnish organisation, and both interview and questionnaire were used. Risk analysis matrix was then used to identify the level of risk in the organisation. Based on the risk analysis, priority proposals for action were targeted at those risks that are intolerable or significant.

The risk assessment matrix was found to be a practical tool for assessing a company's cyber security risk. Once the level of risk has been identified, measures can be taken in the most appropriate way for the company, prioritizing the risks requiring immediate action or other necessary measures.

Key words and terms: cyber security, risk, multi-locational work, risk analysis matrix, case-study

Contents

1 Introduction

Working life has undergone major changes over the past decades. One of the key drivers of change is the development of digital tools and their adoption in working life. This has also led to an increasing number of people moving to work outside the workplace, as work can now more easily be done regardless of time and place. Over the last couple of years, the Covid-19 pandemic has fundamentally sped up the change. While multi-locational work using digital technologies and tools has brought flexibility to employers and employees alike, it has also significantly increased the potential for cyber security risks.

The change of working life requires continuous improvement from employees and workplaces. From a cyber security perspective, the role of workers' own actions is a key factor. However, it is also important to remember the responsibility of an employer to ensure employees are adequately trained and equipped for work with cyber security in mind. It is practically impossible to fully eliminate cyber security risks, but it is important to work towards identifying the most relevant risks and assess their significance.

This thesis examines cyber security in multi-locational work in a modern organisation. It begins with an introduction to the laws relating to cyber security, before moving on to describe the multi-locational work environment and the changes that have taken place recently. The following chapter discusses some relevant cyber security risks associated with multi-locational work, followed by presenting a risk analysis matrix. A case study focusing on views and practises on cyber security in a modern Finnish organisation was conducted and the cyber security risks that emerged are assessed using the risk analysis matrix.

2 Cyber security in Finnish legislation

There is no specific legislation on cyber security in Finland, but various laws include statutes regarding cyber security. Important document regarding the subject is also the Finnish cyber security strategy. These laws and the cyber security strategy will be addressed next.

2.1 EU General Data Protection Regulation

The law has not set any major requirements for organisations regarding risk management and cyber security in the past. This situation changed in 2016 with the EU general data protection regulation (GDPR) and the directive on security of network and information systems (NIS). They add new requirements for both cyber security and cyber security risk management in organisations. The requirements are applied to both European organisations that handle personal information within EU, and to organisations outside EU that conduct personal data management on people residing within EU. GDPR sets standards for organisations on collecting personal data, including strict requirements regarding storing and managing said data. With this, organisations of all types are required to protect the data collected from both employees and customers more carefully than in the past. [General Data Protection Regulation, 2016].

2.2 Act on the Protection of Privacy in Working Life

Purpose of the law is to carry out private life cover as well as protection of privacy to secure fundamental rights in working life. This law decrees technical monitoring at workplace as well as opening or searching for employees' emails. [Act on the Protection of Privacy in Working Life 759/2004].

2.3 Employment Contracts Act

Employment Contracts Act constitutes that employee must conduct their work with care, following the orders the employer has given according to their jurisdiction. Employment Contracts Act also includes a statement that during their employment employees are not allowed to take advantage or spread the trade and business secrets of their employers. The terms of employment are to be discussed in the contract of employment. In addition, it is possible to create separate professional secrecy agreements. [Employment Contracts Act 55/2001].

2.4 Criminal Law

Criminal Law has various sections related to information technology and its usage. For example, theft, embezzlement and unauthorized use all fall under the Criminal Law. It also includes information theft in section 38, which addresses for example confidentiality breaches. [Criminal Code of Finland 39/1889].

2.5 Cyber security strategy

Cyber security strategy 2019 constitutes the most important national goals regarding cyber domain. This strategy is also part of EU cyber security strategy implementation. According to strategy, every individual is an important cyber security operator who is responsible for improving cyber security for themselves and others with daily acts. Officials and organisations require very versatile knowledge from both employees and subcontractors to manage the risks regarding cyber security. National cyber security education and training programs are designed to develop the cyber security knowledge of public administrations, organisations, and individuals [Suomen kyberturvallisuusstrategia, 2019].

3 Multi-locational work

3.1 Change in working life

Multi-locational work has become an integral feature of working life in developed countries in recent decades [Eurofound and ILO, 2017]. According to Green [2006], there has been a strong international trend towards the intensification of working hours during the past decades. For knowledge workers, and otherwise highly skilled workers, evenings and weekends often include checking emails or being otherwise available in addition to their weekly working hours [Ojala *et al.,* 2014]. In addition to work hours increasing and intensifying, part of the reason for increase in multi-locational work is globalization of work-market [Haukkala, 2011]. The continued development of mobile devices and the general ability to work away from the employer's premises have enabled the growth of multi-locational work [Messenger and Gschwind, 2016].

3.2 Definitions

There is heterogeneity of the terminology and the definitions of multi-locational work. Messenger and Gschwind [2016] have presented an example of multi-dimensional framework of telework. The framework divides three generations of teleworking: home office, mobile office, and virtual office. In the framework there are three key elements: technology, organisation, and location. The framework is illustrated in figure 1.

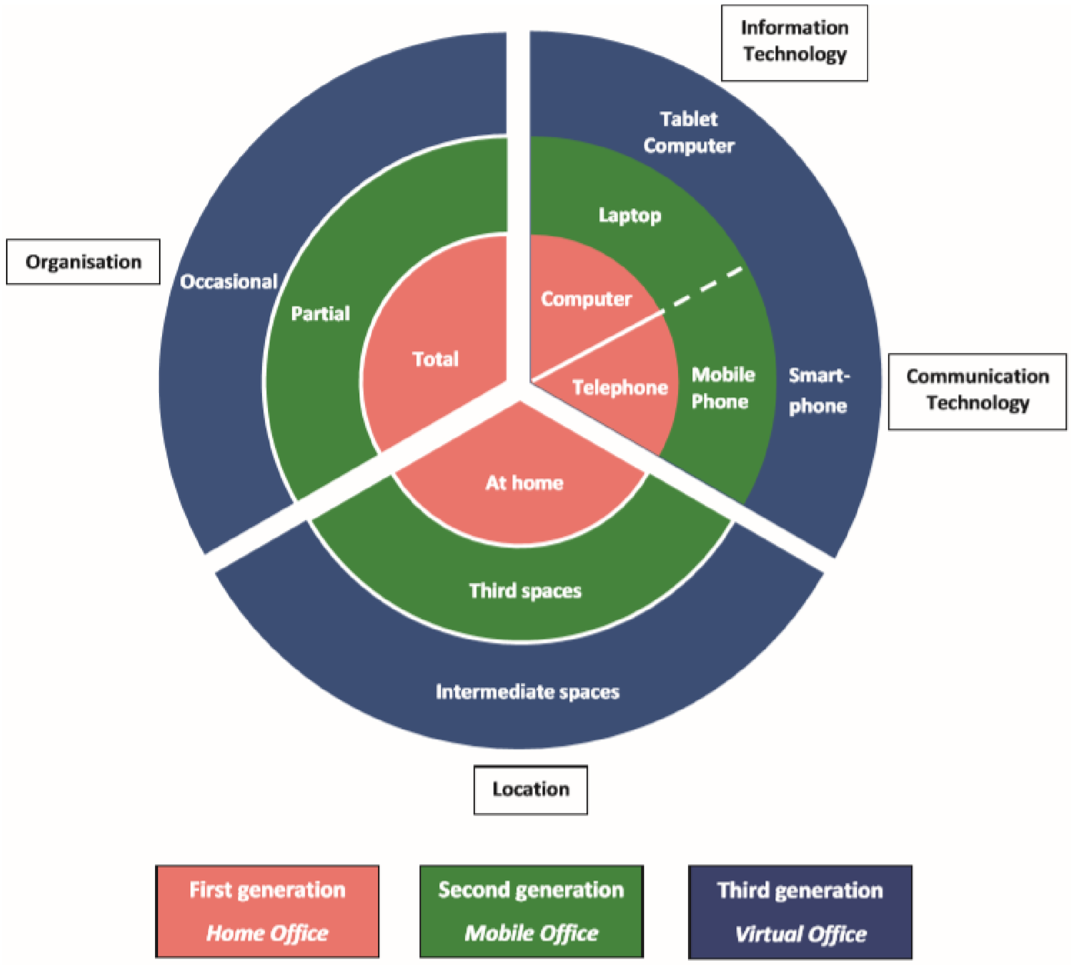
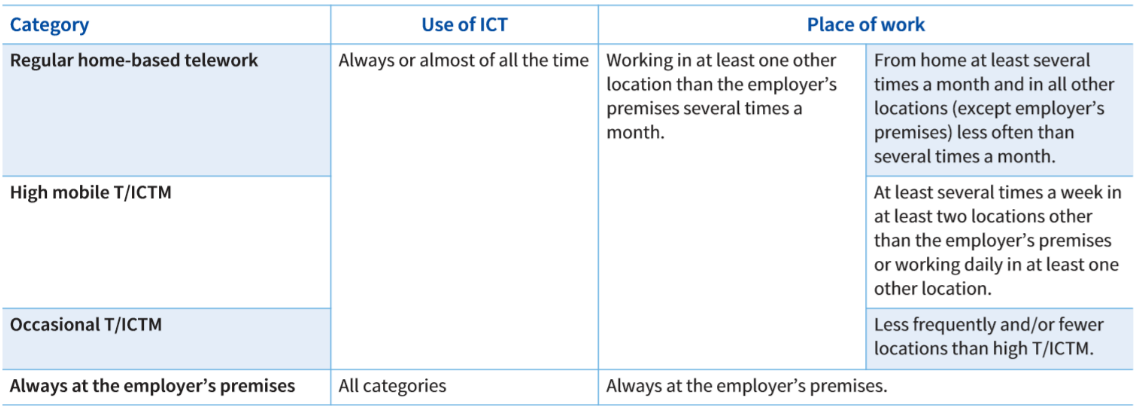


Figure 1. Conceptual Framework of the Evolution of Telework [Messenger and Gschwind, 2016].

Telework/ICT-Mobile Work (T/ICTM) used in a joint Eurofound and ILO report [2017] is another definition of multi-locational work. T/ICTM was defined as the use of ICTs, such as smartphones, tablets, laptops and PCs, for the purpose of working outside the employer's premises. In the report, T/ICTM was split in four different categories according to use of ICT and place of work. The categories are “Regular home-based telework”, “Occasional T/ICTM”, “High mobile T/ICTM” and “Always at employer’s premises”. All the groups, except those always working at the employer’s premises, use ICT always or almost all the time and they work in at least one other location than the employer’s premises several times a month. In addition, the places of work and the amount of time spent out of employer’s premises for these three groups were defined further in figure 2.



Category	Use of ICT	Place of work	
Regular home-based telework	Always or almost of all the time	Working in at least one other location than the employer’s premises several times a month.	From home at least several times a month and in all other locations (except employer’s premises) less often than several times a month.
High mobile T/ICTM			At least several times a week in at least two locations other than the employer’s premises or working daily in at least one other location.
Occasional T/ICTM			Less frequently and/or fewer locations than high T/ICTM.
Always at the employer’s premises	All categories	Always at the employer’s premises.	

Figure 2. Operationalization of categories of T/ICTM according to ‘use of ICT’ and ‘place of work’ items [Eurofound and ILO, 2017].

In this work, multi-locational work refers to both remote work and mobile work and the term is used as hypernym when referring to either one of them. Due to this, the definitions of mobile and remote work are established next. Remote work is work done at either home or at another remote work location agreed and executed with employer [Koroma *et al.,* 2011]. The previous definition of remote work refers to a pre-determined location, which is the main difference between remote and mobile work. Working remotely requires both compromise and careful planning from organisation and the individual, which also requires trust between these two parties. Mobile work is a form of employment, where employee works at least 10 hours per week away from predefined workplace. [Koroma *et al.,* 2011]. This can be public transportation, internet cafe’s or technically any location, where the employee is capable of working. While mobile work is widespread, the benefits of mobile work are unrealized in many organisations due to lack of support for this type of flexible work arrangement [Chen and Nath, 2008]. Mobile working may be comfortable solution for many, but it also means working away from the secure facilities of the company.

3.3 Prevalence and trends

In Finland, only two percent of employees worked at least partially remotely in 1990. The number had doubled to four percent in 1997 and by 2018 the number had already reached 28 percent (Figure 3). [Sutela *et al.,* 2019]. In 2020, before the Covid-19 Pandemic, 21 percent of all employees worked remotely regularly, and 11 percent partially [Keyriläinen, 2021].

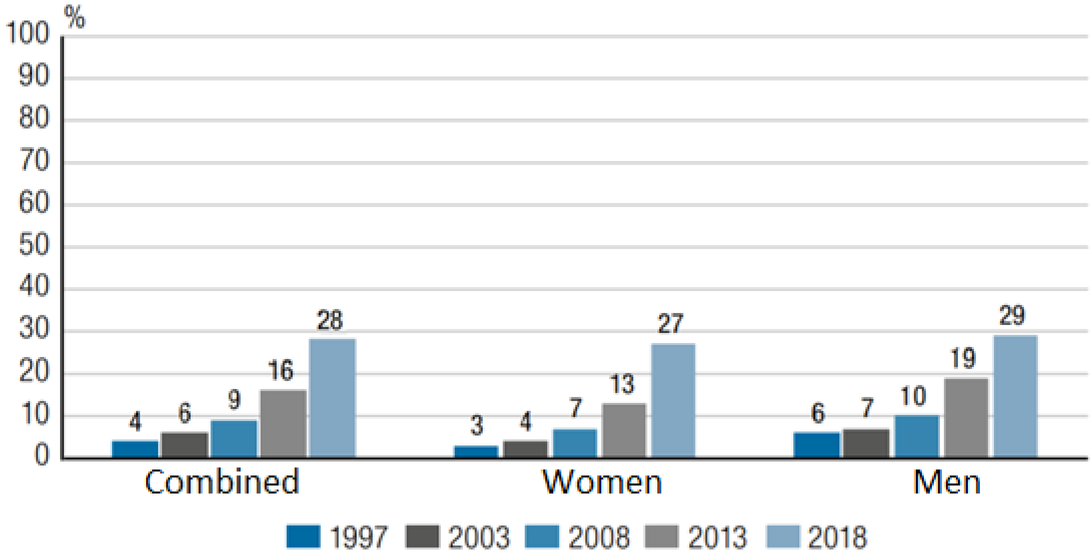


Figure 3. Remote work divided by gender in Finland [Sutela *et al.,* 2019].

In addition, in 2005 58% of Finnish paid workers work at least small part of their jobs somewhere else than at their home or at the employers' premises. These numbers are higher in northern countries, as in 2005 the EU27 average was clearly lower at 40%. For example, in Sweden the same number was 55%. [Haukkala, 2011]. According to Eurofound and ILO [2017], the incidence of T/ICTM varies greatly on the EU-level. This study also shows higher rates of T/ICTM on average within Nordic countries (Figure 4).

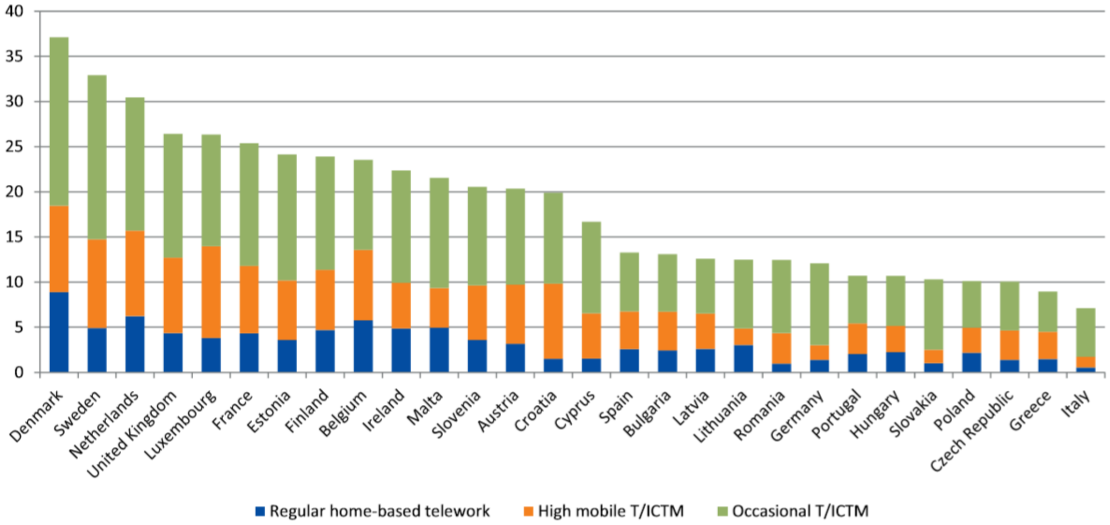
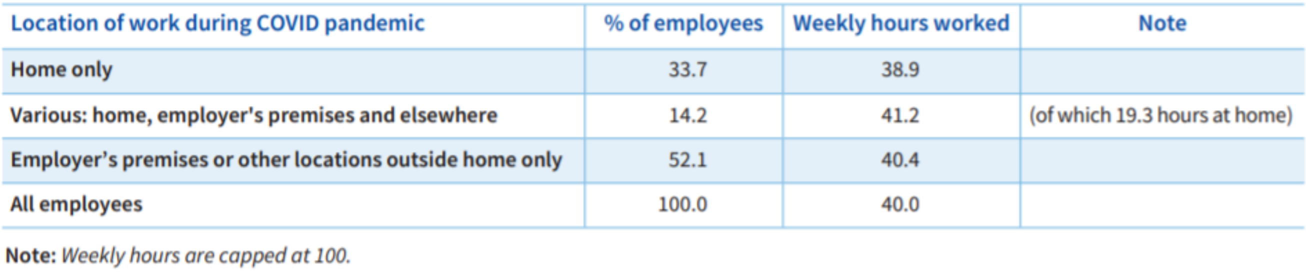


Figure 4. Percentage of employees engaged in T/ICTM in the EU28 (%), by category and country [Eurofound and ILO, 2017].

During the Covid-19 pandemic, multi-locational work increased across Europe due to government restrictions and suggestions. According to Hahne [2021], in Finland 59% of employees started to telework because of the pandemic. This was the highest figure in Europe, with an average of 37%. During the Covid-19 pandemic 52.1% of employees remained in employer's premises or other locations outside of home, 33.7% worked from home only and 14.2% did multi-locational work (Figure 5). [Eurofound, 2020].



Location of work during COVID pandemic	% of employees	Weekly hours worked	Note
Home only	33.7	38.9	
Various: home, employer's premises and elsewhere	14.2	41.2	(of which 19.3 hours at home)
Employer's premises or other locations outside home only	52.1	40.4	
All employees	100.0	40.0	

Note: *Weekly hours are capped at 100.*

Figure 5. Proportion of employees, by location of paid work during COVID pandemic, EU27 (%) [Eurofound, 2020].

4 Risks

From a risk analysis perspective, it is essential to understand what is meant by the term risk. As risk is an abstract concept, there are many different interpretations. Risk is described as the impact of uncertainty on objectives, or the deviation from the expected. Risk can be positive or negative relative to the expected value [Rousku, 2017]. According to Wheeler [2011], considering from the perspective of information security, risk management is about managing the risks associated with sensitive information and critical resources. Risk always depends on the target, and the risk itself is not necessarily the same for everyone.

Risk can be categorised in different ways, for example depending on the target and context. Hopkin [2017] divides risk in four categories in a generic level as compliance risks, hazard risks, control risks and opportunity risks. Raggad [2010] on the other hand divides risk in physical security (unauthorized physical access and device protection), network security (well designed and reviewed network architecture), application security (security compliance and minimal privilege requirement as a part of the system) and data security (preventing third party access and data loss by device malfunction with cryptography and backups). Cebula and Young [2010] present a categorization of operational cyber security risks in four categories: actions of people, systems and technology failures, failed internal processes and external events. Their definition is based on the effect these risks can have on the availability, confidentiality or integrity of information or information systems.

The simple risk categories described above neither focus exclusively on cyber security, nor are sufficient for complex and multi-layered threats facing modern organisations in the field of cyber security. Considering the risks are not the same for everyone nor apply in every situation in a similar manner, this work focuses further on cyber security risks that are amplified in multi-locational work and include a third party that aims to inflict damage or receive personal gain at the expense of an organisation or its employees. The categories are based on the origin and form of the attack, starting from those where responsibility lies most with the employee, continues with shared responsibility between the employee and the organisation, and ends with risks that are mostly the responsibility of the organisation or cannot necessarily even be affected on organisation level. Some of the risks are not related to only one category but are placed in the best describing one. Each risk is further explained in their own subcategory and further analysed in fifth chapter.

4.1 Employee responsibility

The risks primarily on employee's responsibility include shoulder surfing and man-in-the-middle that could be categorized under social engineering, as well as employee's mistakes, such as weak passwords and inadequate deletion of data.

Defining social engineering is not simple and there are various definitions by different authors and researchers. Nyamsuren and Choi [2007] defined social engineering as a category of cyber-attacks, where a person manipulates another person into giving up personal information. This definition allows the term to be used to describe various methods used by attackers to this day. In addition, by this definition social engineering targets the end user instead of device or software. People tend to trust each other and easily reveal important, private information [Junger *et al.,* 2017], which makes this cyber-attack efficient. The basic principle of social engineering is similar to traditional methods of hacking. The attacker's goal could be to gain unauthorized access to information or a system, or to use it as a tool to commit espionage or fraud. [Malwarebytes]. Mistakes in general includes user and superuser errors caused by lack of understanding, lack of education, lack of motivation or, in its simplest form, simple mistakes that can happen to anyone, but are still important part of cyber security.

4.1.1 Shoulder surfing

Shoulder surfing is a physical form of social engineering, which means collecting information by spying "over the shoulder". Shoulder surfing can be executed by being physically present and spying on the target, or it could be done by using a camera and recording the physical actions and screen of the victim. Shoulder surfing can be used to gain unauthorised access to system by using the most common authentication method, alphanumeric password. [Lashkari *et al.,* 2009].

4.1.2 Man-In-The-Middle

One form of data breaching and social engineering is Man-In-The-Middle attack. In this techno-social cybercrime, the attacker replaces the original HTTPS certificate of the victim's device and gains access to all the data sent and received by the victim. This attack can be done in any network the attacker has access to, prime example being an internet café. Using Man-In-The-Middle attack, the attacker is, for example, able to download all data the victim is browsing, replace any download with their own file such as malware to gain further access in the victim's machine, or simply read all the usernames, passwords and other sensitive information sent by the victim. [Gallegati *et al.,* 2009].

4.1.3 Weak or re-used passwords

A weak password is short and contains only lower-case letters or digits, or a combination of the two that can easily be found in a dictionary. Elements of a strong passwords include both upper-case and lower-case letters, digits, punctuation symbols and special characters. Strong password should include at least 4 out of 5 of these categories [Sarkar *et al.,* 2016]. Password reuse across different websites also remains a dire problem, despite attempts to stop users from doing that. Breaches of a password database or for example phishing attack can often lead to several accounts on various sites to be compromised [Wang *et al.,* 2019]. Using weak passwords or reusing the same passwords both at work and at home can result to unauthorized access to organisation's systems or information being stolen.

4.1.4 Data Remanence and inadequate deletion of data

Data remanence refers to the remains of data that can be found in the storage even after attempted deletion. All data and metadata should be deleted when invoking deletion. However, in many cases the data deletion might be incomplete and traceable back to its lineage or even completely restored using adequate tools. This might cause unwanted disclosure of sensitive data. [Gana *et al.,* 2020]. Mistakes such as saving the data in multiple locations and only deleting parts of it are also part of inadequate deletion of data. Therefore, the risks are not limited to technological failures.

4.2 Shared responsibility

The cyber security risks where responsibility is shared primarily between the employer and employee include a variety of malware, against which protection requires both company resources to acquire and train employees on cyber security applications and practices, and employee commitment to follow the organisation's policies and procedures. The risks are increased by Bring your own device (BYOD), which transfers parts of the normal employer's responsibility to the employee.

Malware or a malicious software is an umbrella term used to describe any malicious software, typically consisting of code intentionally designed to invade, damage, disable or even gain access to victim’s device. [Malwarebytes].

4.2.1 Ransomware

Ransomware is a form of malware that relies on extortion based on potential of disabling or damaging the victim’s data. Once the system is infected, the data is generally encrypted by the attacker, leaving victim with a choice to pay the ransom, in hopes of regaining access, or face the consequences. Ransomware is the fastest increasing malware threat to organizations, accounting for the majority of extortion-based attacks and billions in damages globally. The availability of backups and separate backups of critical systems stored separately should be evaluated to address the threat, being the last line of defence against this malware threat. [Thomas *et al.,* 2018].

4.2.2 Trojans and Remote Administration Trojan (RAT)

The word Trojan comes originally from an ancient Greek story of the Trojan horse, which was used by the Greeks to gain unauthorised access to an independent city named Troy during the siege, by hiding inside it. The very meaning still carries in today’s cyber security and the various attempts to breach it. Trojans and RATs are malicious pieces of code often embedded in legitimate programs to gain unauthorised access to victim’s machine [Chen *et al.,* 2008]. Trojans and RATs aim to stay hidden in the machine, eluding the detection of anti-viruses and firewalls by altering their name, location, size and behaviour on a regular basis, and ultimately modifying the system to hide their presence and to gain administration access in order to record the user’s keystrokes, passwords, gain access to webcam and overall usurp resources of victim's system. [Chen *et al.,* 2008]. Remote Administration Tool, which could also be referred as RAT, is a similar tool with similar functionality, with main difference of it being acknowledged by the system owner and being intentionally added to the system. These tools can be used for wide range of functions essential for system administrator, such as providing a cost-effective network access to multi-locational workers [Shubham *et al.,* 2015].

4.2.3 Personal devices

Bring your own device (BYOD) was created as a solution to the challenge of utilizing a company's shared infrastructure. Companies use this innovative practice to get a competitive edge by increasing their economy and the occupational comfort of their personnel. Personal devices, however, involve serious vulnerabilities, threats and risks such as problems created by insecure application usage that could infect the devices with malwares. Unauthorized access to devices is more likely due to theft, loss of the device or other use by third parties, allowing access to company's data or accidental sharing of information. Network risks can arise from being allowed to connect to any unprotected and unencrypted networks. Even if the personal device used is a mobile device instead of a computer, malwares are also capable of infecting and stealing information from mobile devices. [Herrera *et al.,* 2017].

4.3 Organisation responsibility

The cyber security risks in which the organisation mostly carries the responsibility for are largely related to keeping the local infrastructure secure and up to date to avoid vulnerabilities.

4.3.1 Vulnerabilities

Vulnerability according to dictionary is "the quality or state of being exposed to the possibility of being attacked or harmed". Vulnerabilities in computers are understood as the confluence of three elements; system flaw, attackers' knowledge of the flaw and their capability to exploit the flaw. All three elements result in successful utilization of the vulnerability that ultimately compromises system's information security, resulting in attack, for example, being able to delay, disrupt, corrupt, exploit, steal or modify information [Cavelty, 2014].

4.3.2 Outdated applications and operating systems

According to Mohan *et al.* [2020], cybercriminals often take advantage of holes in outdated software. Outdated applications and operating systems leave devices more vulnerable to exploits. To take advantage of vulnerabilities, the attacker must know the flaws in the system. Previously found and fixed issues can be published by various sources including the developer of the software. Failing to update software and operating systems can result in these publicly known flaws in the system to stay unpatched, leaving easy access to an attacker like leaving keys in the lock. Outdated software means unsecured software [Woldemichael, 2019].

4.3.3 Data breach

Data breach is an exposure of confidential information to unauthorized parties. They can be either intentional or inadvertent and caused by either an insider or outsider. Data breaches can pose serious threats to organisations, including financial damage and reputation loss. In addition to malicious insiders, data breaches could be caused by technical shortcomings, such as lack of appropriate access control or failure to investigate security warnings issued by security tools in place. [Cheng *et al.*, 2017]. Individuals, as well as organisations, can place a lot of trust in their service providers, making these issues often complicated and sometimes beyond the scope of organisations' responsibility.

4.4 Abstract responsibility

The risks under the last category have either an abstract origin of attack or an abstract responsibility that cannot be tied to either employee, organisation or their shared responsibility. The risks categorized in abstract responsibility involve hardware and service risks uncontrolled by the organisation. The likelihood and impact of these risks can, however, be reduced by taking appropriate actions on an employee or organisational level.

4.4.1 Hardware backdoors

Hardware is a physical part of a computing system, such as a graphics card or a processor. Hardware can have a built-in backdoor which Sparks *et al.,* [2009] have defined to be a rootkit, a malicious program attempting to hide its existence in the infected machine. According to King *et al.,* [2008], rather than constructing a single assault, an attacker might instead create hardware to enable attacks. To prove it, they designed a backdoored processor, occupying a layer below an entire software stack. This way the attacker has fundamental advantage over the regularly used defence systems, such as antiviruses and firewalls. They initiated an attack by sending an unsolicited network packet to the target system, which in turn is inspected by the operating system. Inspecting the package is necessary to decide if said packet should be dropped or not. This inspection of packet would trigger the backdoor in the hardware and load a firmware designed to let the attacker access the system without a password by returning true on a password checking function regardless of the password being correct. After a successful login attempt the firmware unloads itself to further prevent detection. The backdoored hardware can, for example, give unlimited access to the machine and steal passwords. [King *et al.,* 2008].

4.4.2 Physical interception

Physical interception refers to any method of physically acquiring a device owned by someone else, to gain unauthorized access to either the device or the data in it, for example through theft. Physical interception can result in unauthorized access to more than just the device. For example, logged in website and thus emails or passwords can be at risk. In general, sensitive information can be leaked in case of theft or loss of a device. [Abomhara and Køien, 2015]. Physical interception could also be performed in order to plant malicious software in the machine with the intent of returning it to its original owner, acting as a physical trojan horse to access a network without authorization.

4.4.3 Cloud services

Cloud services refers to a variety of web services delivered on demand to customers. They are meant to provide easy and affordable access to resources without having to invest in internal infrastructure. Partially due to their popularity, cloud services are targeted by variety of malicious actors. According to Rabai *et al.,* [2013] some of the on-focus security threats include administrators' rights to monitor or change virtual machines, attacker's possibility of gaining control over the whole network of virtual machines by infecting the host and risks caused by faulty or malicious virtual machine images. Cloud services are also susceptible to denial of service, data leaks and traffic hijacking. Registering to various cloud hosting services is also very easy, which causes them to be targeted by malicious users exploiting the resources. Mobility of cloud services, as well as virtual hosted machines, can also be cyber security threats, because all the data can be stolen without physically stealing the machine [Rabai *et al.,* 2013].

5 Risk analysis

The various potential risks can be analysed using various risk-assessment methods. Hopkin [2017] argues that both the likelihood and magnitude of risks must be accounted for in a risk analysis. The likelihood and magnitude are best demonstrated using a risk matrix, one of which they have presented in figure 6. Colour coding and shading can also be used to visualize the risk assessment [Hopkin, 2017].

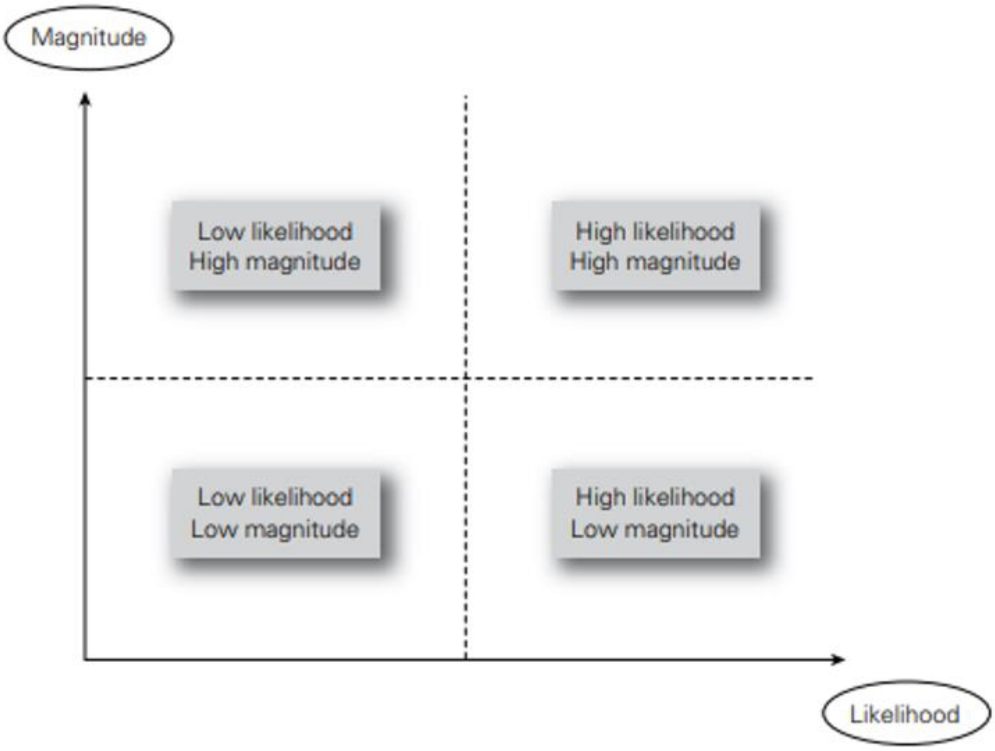
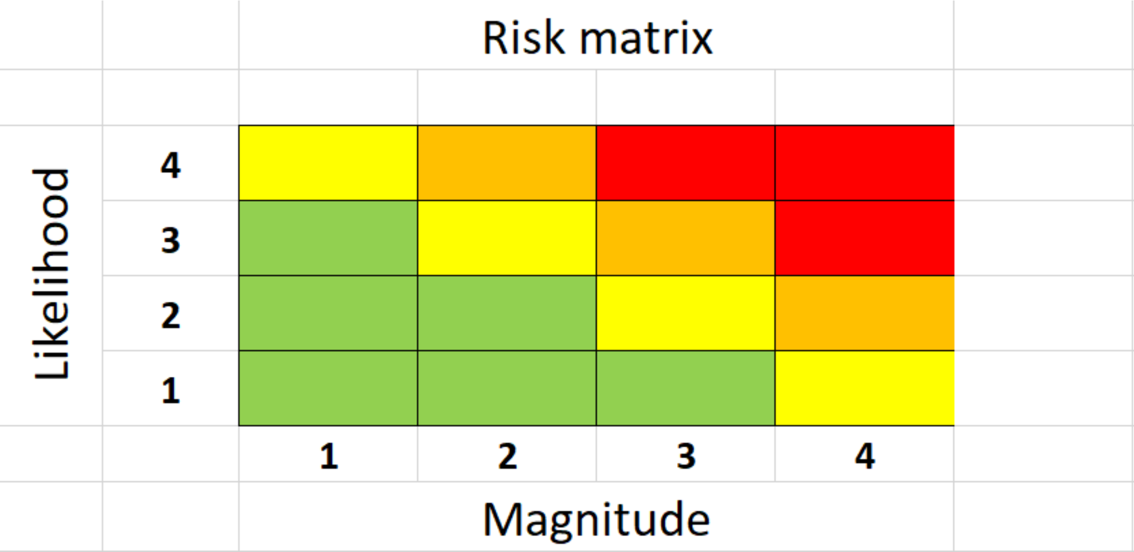


Figure 6. Risk likelihood and magnitude [Hopkin, 2017].

In Finland, the Ministry of Finance recommends the usage of a similar risk analysis matrix as Hopkin. They use a scale of four grades for likelihood and magnitude. In their matrix the likelihood is divided in unlikely, possible, probable and almost certain, while magnitude is divided in minor, mediocre, major and critical. The matrix also includes colour coding ranging from green to red, demonstrating the level of risk (Figure 7). [Rousku, 2017]. The risk assessment method used in this thesis is based on the risk classification matrix used in occupational health care [Pääkkönen *et al.,* 2005], which was originally based on the British standard BS 8800. Their matrix utilizes a scale of three grades and acknowledges pre-determined measures for each level of risk (table 1).



Likelihood				
4	🟨	🟧	🟥	🟥
3	🟩	🟨	🟧	🟥
2	🟩	🟩	🟨	🟧
1	🟩	🟩	🟩	🟨
	1	2	3	4
	Magnitude			

Figure 7. Risk matrix [Rousku, 2017].

Probability	Severity		
	Minor consequences	Adverse consequences	Serious consequences
Unlikely	1. Negligible risk No particular action needs to be taken	2. Tolerable risk Requires attention	3. Moderate risk Action must be taken to lower the risk
Possible	2. Tolerable risk Requires attention	3. Moderate risk Action must be taken to lower the risk	4. Significant risk Requires the necessary measures to lower the risk
Probable	3. Moderate risk Action must be taken to lower the risk	4. Significant risk Requires the necessary measures to lower the risk	5. Intolerable risk Requires immediate action

Table 1**.** Risk analysis matrix.

6 Case study

The empirical part of the thesis was chosen to be conducted as a qualitative case study, because a case study applies especially well when the aim is to deeply understand the target of development and produce new development ideas. A case study answers to questions “how” and “why”. In general, a case study studies an exact case, and the information of the case can be gathered using various methods including interviews, observations and tests. In many cases, the aim of a case study is to make generalised conclusions based on exact cases, which also counts as a con when considering the pros and cons of each method of study. The conclusions are also often based on personal interpretation of the researcher. In a case study the process includes defining the aim of the study and a preliminary analysis of the subject. After that the empirical analysis is made and analysed and development proposition is made [Oppariapu].

A semi-structured thematic interview was chosen as the data collection method. The aim was to allow the interviewees to speak about the topic in their own words, so that they could supplement any information already obtained. The interviews would be conducted one-to-one to make the situation feel freer and more natural [Hirsjärvi and Hurme, 2011].

The interview questions were designed to answer general questions about the organisation, their clients and the cyber security policies IT and management have (Appendix 1). After general questions the discussion moved towards the actual subject of the thesis, multi-locational work and the security measures the organisation takes and instructs their employees to take while working outside of the office and what are the employees access levels to organisations or their client’s data. Every question was open ended, and I avoided leading the respondent towards themes I expected to come up, such as their thoughts of how well employees follow the instructions and policies offered and required by the organisation while out of the office. The goal of this discussion was to establish a baseline understanding of the organisations expectations towards their employees, as well as the strength of their policies and cyber security training provided towards the individual employees. At the end of the interview there was a chance to provide questions they would be interested to be answered in the questionnaire presented for the employees. After the interview was completed, the questionnaire for employees was created based on it (Appendix 2). The main purpose of the questionnaire for employees is to understand the differences of the cyber security understanding and measures the employees take, compared to the expectations of IT and management. The answers of the questionnaire for employees were analysed using risk analysis model described in chapter 5 of this thesis.

The interviews for IT and management were planned to be conducted in a video conference due to Covid-19 pandemic preventing face-to-face meetings. The subject of the study is a Finnish office of a worldwide manufacturing and designing organisation with organisation-wide cyber security policies and over 6000 employees. The Finnish office is a medium sized office with roughly 50 employees overall. The study was conducted by first contacting both the IT lead as well as management of the Finnish office. The study, its goals and the initial questionnaire were presented to both departments, but only IT answered it (appendix 1). In addition, a confidential organisation's cyber security policy document was provided to be used as a guideline for designing the questionnaire and analysing the results.

The questionnaire for employees was based on the answers received from IT department as well as their requests regarding additional questions. The questionnaire was sent to 32 participants with two reminders over the course of one month. 18 answers total were received and analysed using SPSS Statistics version 27 for Windows, as well as the risk analysis model from chapter 5 of the thesis.

The background variables were age, highest level of education and length of employment in the organisation. The participants were allowed to pick one best suited answer to each question. Age was categorized into six age groups: under 20, 20-29, 30-39, 40-49, 50-59 and over 60. For the highest professional education, the categories included no vocational education, professional course of at least four months, vocational education, college, university, and something else which allowed the participant to elaborate with free writing. The selections for length of employment in the organisation were less than one year, one to five years, six to ten years, and more than eleven years.

6.1 Results

Questionnaire was sent to 32 participants and 18 answered in total, resulting in response rate of 56,25%. The participants were between the ages of 30 and 59 with six participants between the ages 30-39, five participants between the ages 40-49 and 7 participants between the ages of 50-59. Their highest level of education was dichotomized twelve participants with either university or college education and six participants with vocational education or none. 50% of the participants had been employed for more than 11 years within the organisation, while only two had been employed for less than a year.

Out of eighteen participants, nine work somewhere else in addition to workplace and home. Out of those who worked somewhere else, everyone mentioned working in a hotel room. Eight worked in a customer company's premises and five worked in public transport and restaurants or cafeterias. In addition, some worked in office-hotels, outside areas such as parks, or children's recreational activity areas. Thirteen reported to know what to do in case of lost or stolen work device. Ten knew about possibility of receiving a privacy filter for their computer and one had chosen to use it. Sixteen mentioned to have access to organisation's critical information. Only one reported having no access and one did not know if they did. Eight participants also reported they had to take confidential material out of the office, two did not know if they had to or not. However, only two reported to have access to a customer company's critical information while working with them. In addition, twelve used their work devices for non-work-related activities such as looking through personal emails and three had installed external applications not available from official sources.

When asking about cyber security training, twelve felt they had received it in sufficient level when they started working in the company. Fifteen felt they had received sufficient cyber security training during their years of work. Fourteen felt they had received sufficient information about cyber security while working outside of office. Regarding whether the participant had received a cyber security policy document, ten reported to have received it. Eight participants either had not received the document or did not know whether they had. Fifteen participants claimed to benefit from cyber security documents and instructions being translated into Finnish.

In addition to above statistics, participants were also asked open-ended questions where they were able to write freely. First, they were asked to describe possible cyber security risks in their current work. The most acknowledged risk was various forms of phishing and similar malicious collection of data, ten participants mentioned it within free-form responses. Physical events such as theft or fire and spying phone calls or laptop screen in public was recognized by six of the participants. Three participants recognized software issues such as inoperative VPN connections and malfunctioning or changing functionality of programs. Traditional forms of cyber-attacks such as malware were recognized as a threat by two participants. Human errors or mistakes such as sending information to wrong person, selecting wrong screens during screen share, incohesive practises and locations for saving data and mistakes made by frustration towards slowly operating software in order to speed up the work were recognized by three participants. One person does not recognize any risks regarding themselves as part of the organisation’s cyber security and two others did not mention any risks.

When the participants were asked to name the most important part in the organisation’s cyber security policy document regarding their own work, thirteen of the participants were able to mention at least one important part. Within their responses, they mentioned actions of the employees such as compliance with the guidelines given and secure usage of the work devices. In addition, secure data management practises, regular software and cyber security practise updates and clear instructions given regarding the cyber security practises were mentioned. Five did not specify any important part of the cyber security policy document, one of which specified being unable to find the document being the reason.

Next the participants were asked what kind of cyber security training they would like to receive in the future. Half of the participants were able to name desirable content of cyber security training within their answers. These answers included desire towards any new information or only towards specific topics, information regarding the most common and recently discovered threats, providing easily accessible and understandable guidelines in Finnish and concrete tips. Six participants did not mention anything, one participant didn’t see the need for increasing the amount of cyber security training and two participants did not recognize need for participating in any training themselves. The participants were then asked to select a desirable method of cyber security training in a multiple-choice question, which allowed selecting more than one option. Fifteen selected expert lectures, six workshops together with others, six gamification of the training, four self-learning material and four self-learning material followed with a test. It was also possible to select option “other” and write the answer. These answers included demonstrating cyber security threats via concrete examples and short “fifteen minutes of cyber security” sessions couple of times a year.

Finally, the participants were asked to describe any shortages in their organisation’s cyber security. Twelve participants did not recognize any shortages. Out of the six participants who answered the question, four considered employee as significant risk. In addition, the global access to data the intranet provides, and the difficulty of finding easy to understand, up-to-date information and guidelines were mentioned. Everyone evaluated their overall organisation cyber security to be perfect or near perfect and only one thought it was hard to take care of cyber security during their work.

6.2 Risk analysis on case study

In the final phase of the case study, risk analysis was conducted based on the interview and questionnaire presented previously and the organisation’s cyber security policy document. First, the probability and severity of the cyber security risks related to multi-locational work introduced in chapter four were analysed (Table 2). The risk analysis factors in the perspective of the work where risks are created by malicious third parties and half of the employees are working mobile. The order is based on the categories presented in chapter four, starting from the risks where responsibility lies most with the employee. After that the risk analysis matrix (Table 3) is used to visually demonstrate the combined severity and probability of each risk (negligible, tolerable, moderate, significant and intolerable risk). Finally, based on the previous risk analysis, the significant and intolerable risks were highlighted and a few necessary measures and immediate actions the organisation can take to remedy the issues were provided.

Risk	Probability	Consequences
Employee responsibility		
Shoulder Surfing	In a multi-locational work, the probability increases to probable due to mobile work locations and extremely low usage of privacy filters designed to prevent shoulder surfing.	Estimated to be adverse.
Man-In-The-Middle	Unlikely, even in multi-locational work.	Can be serious.
Weak passwords	Probable risk unless enforced by the organisation, which was not present in any information received.	Can be estimated to be adverse.
Data remanence and inadequate deletion	Probable without adequate tools to ensure safe deletion of data, which did not come up in the interview or policy document.	The consequences of malicious actor receiving a device with remnants of data remaining are at least adverse.
Shared responsibility		
Ransomwares	Possible risk. The employees of the organisation don't necessarily recognize the risk itself but are aware of suspicious links in emails.	Adverse consequences, resulting in either monetary losses or lost time recovering the data.
Trojans and Remote Administration Trojan	Possible risk based on same reasons as the other common type of malware, ransomware.	Varying between minor and serious depending on the purpose of the malware.
Personal devices	Increases the likelihood of all risks manifesting. The usage of personal devices for work related matters even if unauthorized is probable.	Adverse, depends largely on which risks it manifests as.

Organisation responsibility		
Vulnerabilities	Unlikely, as they require existence of the vulnerability as well as the attacker’s knowledge of the risk and ability to exploit it.	Serious.
Outdated applications and operating systems	Probable risk without proper management software. The existence of ensuring automatic updates did not come up in the interview, questionnaire or security policy document.	Serious, as the necessity of the attacker knowing about the vulnerability is removed, leaving only a confluence of two elements left instead of three. The system flaw and their capability to exploit the flaw.
Data breach	Normally unlikely risk. However, with vast majority of the employee’s having access to critical information of the organisation as well as their clients, the probability raises to possible.	Serious, able to cause both financial damage and reputation loss.
Abstract responsibility		
Hardware backdoors	Unlikely and hardly anything the organisation can do to prevent it, apart from using some common sense where to acquire devices and other hardware.	Adverse.
Physical interception	Unlikely in Finland.	Adverse consequences considering data remanence and no policies for password strength.
Cloud services	Unlikely if enough effort is placed selecting secure service providers.	Serious, includes data loss and risk of data leaking.

Table 2. Probability and consequences by risk.

Probability	Consequences		
	Minor consequences	Adverse consequences	Serious consequences
Unlikely	1. Negligible risk	2. Tolerable risk - Hardware backdoors - Physical interception	3. Moderate risk - Man-In-The-Middle - Vulnerabilities - Cloud services
Possible	2. Tolerable risk	3. Moderate risk - Ransomware - Remote administration trojan	4. Significant risk - Data breaches
Probable	3. Moderate risk	4. Significant risk - Shoulder Surfing - Weak passwords - Bring your own device - Data remanence and inadequate deletion of data.	5. Intolerable risk - Outdated software

Table 3. Risk analysis matrix for target organisation.

Based on the risk analysis, priority proposals for action are targeted at those risks that are intolerable or significant. The only risk that arose to intolerable risk category was outdated software which is in organisation’s responsibility. Five significant threats were found, including shoulder surfing, weak passwords, bring your own device, data remanence and inadequate deletion of data and data breaches. Shoulder surfing, weak passwords and data remanence are primarily in the employee’s responsibility, bring your own device is shared responsibility between the employee and the organisation and data breaches are primarily in the responsibility of the organisation.

7 Discussion

Multi-locational work has been on the rise for the past decades, with Covid-19 accelerating the change even further. Multi-locational work increases the probability, and to a degree severity of certain cyber security risks that were analysed during this work. The risks were categorized in four levels: being primarily employee's responsibility, shared responsibility between the employee and the organisation, primarily organisation's responsibility and abstract responsibility. Risk analysis matrix that considered both severity and probability of the risks was then introduced. The case study was conducted with a Finnish organisation and the results were analysed with the risk analysis matrix to find the significant and intolerable risks requiring immediate action or other necessary measures. The results are examined in detail next.

7.1 The prevalence of multi-location work

The case study was conducted during the beginning of the Covid-19 pandemic before the government recommendations for working out of office, results reflecting mostly pre-covid period. Half of the employees worked multi-locational in places that leave them more vulnerable to cyber security attacks than working in the office or at home, which were in-line with Finland's average already in 2005 [Haukkala, 2011]. However, these numbers vary greatly between studies conducted due to varying definitions of multi-locational work [Eurofound and ILO, 2017; Haukkala, 2011; Keyriläinen, 2021; Sutela *et al.,* 2019]. Studies conducted during Covid-19 pandemic have shown increase in multi-locational work in Europe. [Hahne, 2021]. Study conducted by Statistic Finland [Sutela and Pärnänen, 2021] finds that nearly 80% of those who tried remote work for the first time during the pandemic would like to continue working remotely after the pandemic. In addition, 66% of those who had worked remotely before the pandemic, and had increased the amount during it, preferred to continue remotely working more than before the pandemic.

7.2 Cyber security risks of the target organisation

According to results of the case study, a vast majority of the employees have access to critical information of their own organisation, and in some cases even their customers'.

In addition, the lack of using security filters and multiple employees reporting having to take confidential material out of the office, the severity of various risks such as shoulder surfing, data breaches and theft are increased significantly.

According to the interview, the organisation aims improving the cyber security knowledge of its employees by offering cyber security politics document, material related to cyber security as well as cyber security orientation and training including security practises out of office during the employment. Despite that majority of the employees felt they had received sufficient cyber security orientation and training, they reported difficulty of finding appropriate material and understanding it. Especially the unavailability of material in Finnish and the difficulty of cyber security vocabulary was perceived as a problem. In addition to this, the interest towards cyber security varied greatly. Only half of the participants claimed general interested towards cyber security practises, which also matches the number of participants who named the type of cyber security training they would like to receive in the future.

The ability to assess cyber security risks varied greatly between the respondents. Majority of employees were able to only acknowledge threats generally known by everyone such as phishing and physical threats like thievery. Only few employees recognize other common threats, such as malware or human errors as a problem, potentially implying the knowledge comes from publicly available sources, such as news and everyday life instead organisation's cyber security material. These in combination imply the effectiveness of the cyber security training the organisation provides is lacking and should be reviewed based on the results of the case study.

Despite all of this, everyone evaluated their overall organisation cyber security to be perfect or near perfect. One theme that might have resulted in this assessment was faith the employees had towards someone taking care of the cyber security and might feel the cyber security of the organisation requires little effort from themselves. For cyber security to work, the organisation is required to acquire effective cyber security strategy, teach it to the employees in a manner that promotes motivation, as well as employees committing to it.

7.3 Usability of the risk analysis matrix

The risk analysis matrix was chosen because it assesses both severity and probability of cyber security risks and illustrates the importance of each threat clearly [Hopkin, 2017;

Pääkkönen *et al.,* 2005; Rousku, 2017]. The usability of the matrix in context of an organisation was evaluated during the case study. The case study showed the risk analysis matrix can be used to target action by identifying the significant and intolerable risks requiring necessary measures or immediate actions. However, the risk analysis matrix doesn't attempt to assess the resources organisation requires to fix the identified issues. Both financial and human resources available at one time for the organisation are limited. Therefore, a separate method for evaluating the available resources compared to level of threat the matrix provides should be considered, raising or lowering the priority of a measure to take. For example, if the measures requiring human resources expend the availability, one that requires the organisation's financial resources instead should be prioritized.

7.4 Evaluating the work and further research proposal

The strengths of the study include broad view on the literature regarding multi-locational work, the cyber security risks related to it, and the ways to categorize them. However, the literature regarding the subject is limited and there is no unified vision within the field of research on the categorization of cyber security threats, which made it possible to present an alternative method that considers the distribution of responsibility withing the organisation. The work highlighted some of the more important risks related to cyber security of multi-locational work, but future work should be open for recognizing new risks as well. This categorization also makes future work that considers the available financial and human resources the organisation has for improving their cyber security possible.

One of the weaknesses of the study was the low number of participants and the lack of financial management perspective during the interview process. However, the case study included an interview with the IT lead responsible for applying the cyber security policy of the organisation, as well as a questionnaire for the employees. This made it possible to consider both the management and employee perspective on cyber security. The case study was carried out in only one organisation, so the results cannot be generalised, which is often considered the challenge of case studies in general. This case study, however, achieved its aim to deeply understand the target, which was essential to properly evaluate the risk categorisation and the risk assessment matrix. Another weakness is the lack of assessing workload and the potential effects it has on motivation in both the interview and questionnaires. Overloaded IT in general is both interesting and important topic currently overlooked in the literature.

Another greatly overlooked topic in literature regarding the subject is unauthorized multi-locational work. This means that an employee is taking the work out of office without permission from the employer and without the support from organisation’s IT. This prevents some precautions the organisation can take to reduce the risks of cyber security threats associated with multi-locational work. Studying this phenomenon using questionnaires or interviews is also ineffective due to its unauthorized nature, requiring means not present in this work. At the time this work was conducted, the availability of literature regarding the development of cyber security risks related to increase in multi-locational work due to Covid-19 pandemic was lacking.

7.5 Conclusions

Despite the increased number of attack vectors targeting those working out of office, the increase in multi-locational work is a permanent change in working life. The changed situation requires new approaches from organisations for recognizing these threats and taking measures within the limits of resources available to them. The risk analysis matrix, which identifies both the severity and probability of cyber security threats and clearly illustrates the impact of each threat, and categorization, which evaluates the allocation of responsibility across the organisation proved to be a possible solution.

8 References

Abomhara, M., and Køien, G. M. 2015. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility* 4(1), 65–88.

Act on the Protection of Privacy in Working Life (759/2004). Retrieved January 1, 2021, from https://www.finlex.fi/fi/laki/ajantasa/2004/20040759?search%5Btype%5D=pikaandsearch%5Bpika%5D=laki%20yksityisyyden%20suojasta

Cavelty, D, M. 2014. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics* 20(3), 701–715.

Cebula, J. J., and Young, L. R. 2010. *A Taxonomy of Operational Cyber Security Risks*. CERT ® Program.

Chen, L., and Nath, R. 2008. A socio-technical perspective of mobile work. *Information Knowledge Systems Management* 7(1,2), 41–60.

Chen, Z., Wei, P., and Delis, A. 2008. Catching Remote Administration Trojans (RATs). *Software - Practice and Experience* 38(7), 667–703.

Cheng, L., Liu, F., and Yao, D. D. 2017. Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7(5), e1211-.

Criminal Code of Finland 39/1889. Retrieved January 1, 2021, from https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L47

Employment Contracts Act (55/2001). Retrieved January 1, 2021, from https://www.finlex.fi/fi/laki/alkup/2001/20010055#Pidp446786944

Eurofound. 2020, *Living, working and COVID-19, COVID-19 series*. Publications Office of the European Union, Luxembourg.

Eurofound and ILO. 2017. *Working anytime, anywhere: The effects on the world of work*. Publications Office of the European Union, Luxembourg and Geneva, International Labour Office.

Gallegati, F., Cerroni, W., and Ramilli, M. 2009. Man-In-The-Middle Attack to the HTTPS Protocol. *IEEE Security and Privacy*. University of Bologna.

Gana, U., Jantan, A., Yusoff, N., Abdullahi, I., Kiru, U., and Kazuare, A. 2020. Towards Understanding the Challenges of Data Remanence in Cloud Computing: A Review. In: *Advances in Cyber Security. Second International Conference*, 497-507.

General Data Protection Regulation (GDPR) 2016/679 Retrieved April 4, 2021, from https://gdpr-info.eu

Green, F. 2006. *Demanding Work: The Paradox of Job Quality in the Affluent Economy*. Princeton University Press.

Hahne, A. 2021. *The impact of teleworking and digital work on workers and society - Case study on Finland (Annex III).* Publication for the committee on Employment and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

Haukkala, T. (eds.). 2011. *Monipaikkaisuus – ilmiö ja tulevaisuus*. Suomen itsenäisyyden juhlarahasto, Sitran selvityksiä 54. Helsinki.

Herrera, A. V., Ron, M., and Rabadao, C. 2017. National cyber-security policies oriented to BYOD (bring your own device): Systematic review. In: *Iberian Conference on Information Systems and Technologies*, 644–648.

Hirsjärvi, S., and Hurme, H. 2011. *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö*. Helsinki: Yliopistopaino.

Hopkin, P. 2017. *Fundamentals of Risk Management - Understanding, evaluating and implementing effective risk management*. Kogan Page Limited.

Junger, M., Montoya, L., and Overink, F.-J. 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behaviour* 66, 75-87.

Keyriläinen, M. 2021. *Työolobarometri 2020.* Työ- ja elinkeinoministeriön julkaisuja. Työ- ja elinkeinoministeriö Helsinki.

King, S., Tucek, J., Cozzie, A., Grier, C., Jiang, W., and Zhou, Y. 2008. Designing and Implementing Malicious Hardware. *Leet'08* 5, 1–18.

Koroma, J., Anttola, M., Hyrkkänen, U., and Rauramo, P. 2011. *Mobiili työ: työhyvinvointi liikkuvassa ja monipaikkaisessa tietotyössä.* Työturvallisuuskeskus TTK, palveluryhmä: Työterveyslaitos.

Lashkari, A., Farmand, S., Zakaria, O., and Saleh R. 2009. Shoulder surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security.* 6(2), 145-154.

Malwarebytes. Retrieved March 22, 2022, from https://www.malwarebytes.com/malware and *https://www.malwarebytes.com/social-engineering*

Messenger, J. and Gschwind, L. 2016. Three generations of telework: New ICTs and the (r)evolution from home office to virtual office. *New Technology, Work and Employment,* 31(3), 195–208.

Mohan, D., Sagar Gowda, S., and Vikyath I. 2020. Cyber Security in Health Care. *International Journal of Research in Engineering, Science and Management* 3(1), 551-553.

Nyamsuren, E. and Choi, H.-J. 2007. Preventing social engineering in ubiquitous environment. *Future Generation Communication and Networking* 2, 573-577.

Ojala, S., Nätti, J., and Anttila, T. 2014. Informal overtime at home instead of telework: Increase in negative work–family interface. *International Journal of Sociology and Social Policy* 34(1–2), 69–87.

Oppariapu, Retrieved March 8, 2020, from https://oppariapu.wordpress.com/tapaustutkimus/

Pääkkönen, R., Rantanen, S., and Uitti, J. 2005. *Työn terveysvaarojen tunnistaminen.* Työterveyslaitos, Sosiaali- ja terveysministeriö.

Rabai, L., Jouini, M., Aissa, B., and Mili, A. 2013. A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences* 25(1), 63–75.

Raggad, B. 2010. The Information Security Life Cycle. *Information Security Management: Concepts and Practice*. Taylor & Francis Group, 67-103.

Rousku, K. (eds.). 2017. *Ohje riskienhallintaan.* Valtiovarainministeriön julkaisuja 22/2017. Valtiovarainministeriö, Julkisen hallinnon ICT, Helsinki.

Sarkar, S., Sarkar, S., Sarkar, K., and Ghosh, S. 2016. Cyber security password policy for industrial control networks. In: *Proceedings on 2015 1st International Conference on Next Generation Computing Technologies*, 408–413.

Shubham, Acharya, C., and Prabu, M. 2015. Remote Administration Tool (Rat). *International Journal of Advance Research and Innovative Ideas in Education* 3(5), 1041–1045.

Sparks, S., Embleton, S., and Zou, C. 2009. A chipset level network backdoor: Bypassing host-based firewall and IDS. In: *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security*, 125–134.

Suomen kyberturvallisuusstrategia 2019. 2019. Valtioneuvoston periaatepäätös. Retrieved January 3, 2022, from https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Sutela, H. and Pärnänen, A. 2021. *Koronakriisin vaikutus palkansaajien työoloihin*. Työpaperi 1/2021. Tilastokeskus.

Sutela, H., Pärnänen, A., and Keyriläinen, M. 2019. *Digiajan työelämä: Työolotutkimuksen tuloksia 1977–2018*. Tilastokeskus.

Thomas, J. 2018. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management* 13(6), 1-24.

Wang, K. and Reiter, M. 2019. How to End Password Reuse on the Web. In: *Network and Distributed Systems Security (NDSS) Symposium 2019*, 1–16.

Wheeler, E. 2011. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Elsevier Science.

Woldemichael, H. 2019. Emerging Cyber Security Threats in Organisation. *International Journal of Scientific Research in Network Security and Communication* 7(6), 7-10.

9 Appendices

9.1 Appendix 1: Interview for IT and Management

Organisation description

What does your organisation do and who are your clients?

In how many countries does your organisation operate?

How many employees are working in your organisation?

How many of your employees engage in multi-locational work?

Do you know which facilities host the multi-locational work of your employees?

Which cyber security threats do you consider the most dangerous for your organisation?

How many of your employees have access to critical information that could make the risks mentioned in last question possible?

Are the employees of your organisation able to access critical information of your customers?

Organisation cyber security politics

Does your organisation have document regarding your cyber security politics? Is it possible for me to access said document for master's thesis?

Describe your cyber security politics

How is the responsibility of cyber security divided between different organisation levels?

How does your organisation estimate cyber security risks?

How secure would you describe your cyber security politics?

Did your organisation have case of leaked critical information?

Is multi-locational work taken into account in your organisation's cyber security politics?

Does your cyber security politics determine in which locations can your employees engage to multi-locational work? Would, for example, public cafeteria be allowed?

Is there instructions regarding inner cyber security (For example moving confidential documents out of organisation premise or copying them to external drives)?

Does your organisation enforce cyber security politics? If yes, how?

Do you believe that your employees follow the instructions given, mostly regarding multi-locational work?

Employee cyber security practice

Are employees background checked during recruiting? (For example criminal background or security clearance).

Does your employment contract or some other contract made in the beginning of employment include cyber security decrees?

Does your organisation have procedure regarding saved files or documents at the end of employment?

What are your employee's rights regarding their own devices and the software installed to them?

Are employees allowed to use removable media such as USB-drives?

What is the procedure regarding lost or stolen devices?

Training

Is there a prepared training packet for new employees or is the training done in case-to-case basis?

Are the employees given cyber security training during their employment?

How is cyber security training done in your organisation?

Does your training plan include individual skills or special needs?

How does your organisation improve employee's cyber security knowledge? Does this include motivation and attitude training?

Anything else?

Do you have anything else you would like to bring up regarding cyber security or multi-locational work?

Do you have any requests towards the questionnaire for employees?

9.2 Appendix 2: Questionnaire for the employees

1.Age (in years)

○ Under 20

○ 20-29

○ 30-39

● 40-49

○ 50-59

○ 60+

2.The highest professional education

○ No vocational education

○ Professional course of at least 4 months

○ Vocational education

○ College

○ University

○ Something else, what?

3.How long have you been employed in your current workplace?

○ Less than one year

○ 1-5 years

○ 6-10 years

○ more than 11 years

4.Do you work outside your office or home office?

○ Yes

○ No

5.If you answered “yes”, could you describe in which? You can select multiple choices.

□ public transport: bus, train, plane

□ hotel

□ cafeteria, restaurant

□ customer company

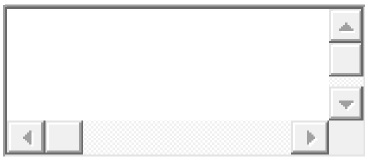
□ office hotel

□ children’s recreational activity area

□ outside areas such as park

□ Something else, what?

6.Which cyber security threats you deem possible in your current work?



7.Do you have access to your organisation’s critical information? Critical information means information that is potentially hazardous for your organisation if fallen to wrong hands.

○ Yes

○ No

○ I don’t know

8.Do you have access to your customer company’s critical information while working with them?

○ Yes

○ No

○ I don’t know

9.Wavin corporation provides Wavin Finland’s security management document. Have you seen it?

○ Yes

○ No

○ I don’t know

10.What in your opinion is the most important part of Wavin Finland cyber security policy regarding your own work?

11.How secure would you rate your organisation’s cyber security?

*****

12.If your organisation’s cyber security has shortages in your opinion, could you describe them?

13.Have you been given instructions regarding the work outside your office or home office?

○ Yes

○ No

14.Do you need to take classified information outside your office in your work?

○ Yes

○ No

○ I don’t know

15.How easy would you agree taking care of cyber security is when working outside of your office or home office?

○ Very easy

○ Easy

○ Moderately easy

○ Hard

○ Very hard

16.Do you know how to act in the event of losing your work mobile phone or computer? (Or if it is stolen?).

○ Yes

○ I don’t know

17.Did you receive adequate orientation regarding cyber security in the beginning of your employment?

○ Yes

○ No

18.Have you been given enough cyber security training during your employment?

○ Yes

○ No

19.What kind of cyber security training would you like to receive in future?

20.What type of cyber security training would be most meaningful to you? You can select more than one option.

□ Self-learning material

□ Lecture given by expert

□ Self-learning material and multiple-choice questionnaire

□ Workshop together with other employees

□ Educational game, that could include for example virtual reward for good performance or friendly competition between employees

□ Something else, what?

21.Would you benefit from cyber security instructions translated in Finnish? (Most of your cyber security instructions are currently handed out in English).

○ Yes

○ No

22.Did you know about the possibility of receiving privacy filter in your computer?

○ Yes

○ I did not

23.Have you acquired privacy filter?

○ Yes

○ No

24.If you didn’t, why?

25.Do you use your work computer for any recreational activity during your free time? For example, reading your email or searching for information?

26. Have you installed any 3rd party software to your work mobile phone outside of official appstore?

○ Yes

○ No