Master Degree Project

UNIVERSITY OF SKÖVDE

Working from Home: The New Norm in a Post-COVID-19 World

Information and Cyber Security in the Digital Work from Home Environment

Masters Degree Project in Informatics

Second Cycle 30 credits

Spring term 2023

Student: Sebastian Ringström

Supervisor: Ali Padyab

Examiner: Rose-Mharie Åhlfeldt

ACKNOWLEDGEMENTS

I would like to extend my thanks and appreciation to my supervisor Ali Padyab for your support and insights in writing this thesis. Your guidance and support throughout the entire process has been invaluable. I would also like to extend thanks and appreciation to my examiner Rose-Mharie Åhlfeldt who provided comments and suggestions to how the thesis could be improved.

Finally, appreciation and thanks goes out to all the faculty and students at the PICS Masters Program for giving me the oppertunity to learn and grow.

A special and eternal thanks goes out as always to my family for always believing in me and always standing behind me and supporting me in all my endeavours. Words cannot even begin to describe what you all mean to me.

ABSTRACT

Work from Home (WFH) gained momentum as a result of the pandemic. When large portions of the world were under government mandated lockdowns, and forced to institute WFH, companies began to slowly realize that the WFH model come with significant benefits such as the possibility to reduce office space or obtaining access to talent globally. Employees too are incentivized to WFH as it allows them more freedom in where to live, reduce commuting costs, and allow employees to space out work during the day and better manage energy levels.

The thesis investigated cybersecurity and information security risks connected to the WFH model through collecting qualitative data by conducting a systematic literature review to gain background knowledge on the topic which was then used to create the interview guide that was used to carry out semi-structured interviews with four heterogeneous Swedish companies of various sizes, working in different fields.

The SLR identified social engineering attacks in general, and phishing attacks in particular, to be the greatest threat to employees working in a WFH model suggesting employee security awareness training to be the key security measure in protecting the WFH model. The semi-structured interviews revealed that companies working in a WFH model have also drawn the same conclusion and have made significant efforts to raise security awareness through employee training programs.

Keywords: Telework, Work from Home, WFH, Remote Work, Cybersecurity, Information Security, Incentives, Cyberattacks, Security Awareness, Security Culture

Table of Contents

1 Introduction

As a result of the global COVID-19 pandemic and the subsequent lockdowns, companies and authorities had to implement large changes in short order to continue working. One of these large changes was the shift to a teleworking, remote working or quite simply "Work from Home" (WFH) paradigm. While working from home is by no stretch of the imagination a new concept and has been around for a very long time, what changed with the pandemic was the scale by which it was being practiced. Employees in EU member states working from home full-time rose to 33.7 per cent with an additional 14.2 percent working hybrid at home and in the office (Eurofound, 2020) as a direct result of the COVID-19 pandemic. Similar figures can be found in different regions across the globe with estimations that Work from Home accounted for roughly 50 percent of paid work hours between April and December 2020 in the United States of America (Barrero et al., 2021) for instance.

Despite the pandemic having been declared as no longer representing a global health emergency by the WHO (WHO, 2023) and with the lockdowns and recommendations for non-essential personnel to stay at home being a thing of the past, a substantial increase in WFH figures remain when compared to pre-COVID numbers. The EU, for instance, saw an increase in people working regularly from home by an average of 8 percent between 2019 and 2021, with the Swedish capital of Stockholm standing out with 40 percent of employees now mostly working from home having increased by a 32.8 percent when compared to pre-pandemic figures according to Eurostat (2022). These increases would suggest that WFH is not just a temporary measure temporarily implemented to deal with the pandemic but rather something that is here to stay going into the future.

There are several incentives for most companies to want to push for a shift towards WFH for employees who occupy roles within the company that do not require physical access to company resources and several large companies have already made a complete transition towards full-time WFH. The WFH model present companies with the opportunity to decrease utility costs, and give improved access to a large international talent pool when hiring people, with perhaps the largest incentive behind making the shift being the opportunity to reduce office space.

While the cost for office space varies widely between companies, countries, and cities it is undoubtably one of the more significant expenses that companies face with. According to Statista (2023), the average annual cost to rent office space in Europe was approximately 1200 USD per square meter, with highest average

cost located in the west end district of London with annual cost of approximately 2400 USD in the third quarter of (Q3) 2022.

From an employee perspective, the WFH model provides the employees with improved flexibility in deciding where to live, grants the ability to stretch the workload over a longer time period and removes the costs in time, money and energy that is normally spent on commuting to and from the physical office. The WFH model also contributes generally to improved work-life balance as the time and energy that is freed up for employees can be spent on relaxation, hobbies, and other recharging activities. The PGi 2020 survey reported that 60 percent of the respondents would quit their current position for a similar job and pay if it meant that they could work from home full-time (O'Brien, 2020).

While there are many benefits to wanting to implement a WFH model, there exists considerable challenges too that need to be considered. From a cybersecurity and information security perspective, employee home IT environments in a WFH model are turned into attractive targets for threat actors to exploit as they are increasingly being used to process and store sensitive data connected to their jobs and can, through their connection into the corporate IT infrastructure, serve as a starting point for future attacks against companies. The FBI in their IC3 report (2020) reported a global increase of 300 percent in successful cyberattacks in 2020 that were directly attributed to the shift towards Work from Home.

If WFH is to become the new norm moving into the future, the challenges and risks associated with the model must be identified and dealt with in a satisfactory manner to ensure that the model remains sustainable and attractive moving into the future.

1.1 Problem Description

The COVID-19 pandemic brought on a radical change in how people work, and this change is highly unlikely to revert within the foreseeable future. Employers and employees alike are enjoying significant benefits from no longer having to work from a physical office as employers are no longer forced to rent office space and employees are no longer required to commute to and from the office.

The shift from the physical office to the home of the employees does, however, create significant information security and cybersecurity challenges. Standard cybersecurity and information security best practices are typically not utilized in a private IT infrastructure found in individual homes and the average employee lacks the resources, knowledge, and experience to implement the security controls that would otherwise be expected to be found in a professional environment.

With the blurred lines between the professional and private domains caused by the shift in how people work that often occurred as a result of the COVID-19 pandemic, the need to improve cybersecurity and information security in the home IT infrastructure has increased radically.

Home IT infrastructures are now directly connected to the corporate IT infrastructure and can serve as a backdoor that can be used as a stepping stone to launch cyberattacks against the company IT infrastructure. Additionally, as employees are conducting their jobs from home, more sensitive information and data gets stored on the private IT infrastructure which not only makes the employees attractive targets for cyberattacks but also challenges the company compliance of laws such as the GDPR and puts the company at risk of punitive legal actions.

1.2 Research Motivation

WFH is becoming widely implemented across the entire world which has unsurprisingly led to an increase in attacks targeting home users as they become more attractive targets for cyberattacks. As with most large societal shifts, with WFH comes an acclimatization period before the surrounding conditions have caught up and sufficient trial and error has molded and optimized the model.

The shift from working out of a physical office with established cybersecurity and information security measures in place and with easy access to supporting resources provided by, i.e., the IT department, to working in a place where employees are largely left to take responsibility for most, if not all, aspects of their own digital environments put both the employee and, in extension, the organization in a heightened state of risk. Employees are highly unlikely to follow or even know how to follow security best practices which creates an acute and serious need to identify and solve the problems that have risen from the WFH shift so that practitioners of the WFH model can better assign responsibility, make resources available and deploy the necessary solutions to combat the problems associated with and practice a safer form of WFH.

While the WFH phenomenon has flared up as a hot topic in academia, and while the topic is old, a lot of changes that came during the COVID-19 pandemic is still largely left unsettled. Considering that WFH means a complete and radical shift in how people work which affects many different aspects and research areas it should come as no surprise that there exist large gaps in the research on the topic. From a cybersecurity and information security perspective, quite a lot of prior work have been conducted on the research topic. Prior work has typically been focused on identifying and addressing the security challenges associated with the WFH model and while discussing the many risks associated with the WFH model and even offer remedies, is a good step on the way no paper

found weight risk and reward by considering the underlying incentives when suggesting security controls. Security without the consideration of the value of what is being protected is far from optimal. Theoretically, given infinite resources, anything can be protected. It is only when the security response is proportionate to the value of what is being protected that cybersecurity and information security is carried out correctly.

By identifying and leveraging the incentives that exist behind shifting towards a WFH model against the necessary security controls needed to achieve an acceptable level of security and looking at these factors both from an academic perspective through the literature body of work and through the eyes of companies working with a work from the home model this thesis seeks to provide the conditions required for the work model to be implemented on a large scale and provide it with longevity.

1.3 Research Questions

This study aims to identify the problems and challenges that companies and employees in Sweden are confronted with when attempting to secure themselves from cyberattacks in a WFH environment and enhance the state of cybersecurity and information security for both employees and the companies they work for.

To address the issues stated above, the following research questions (RQ) are asked:

- **RQ1** What problems do users and companies face when attempting to improve the security of their respective IT infrastructures in a WFH model?
- **RQ2** What do users and companies currently do to mitigate or eliminate the problems they face in a WFH model?
- **RQ3** What can be done to further enhance the security state of employees and employers employing a WFH model going forward?

Additionally, because security does not exist within a vacuum, and investments into security controls should be done so with the value of what they are protecting in mind, a financial dimension in the last research question is considered when considering the mitigation/elimination techniques available to solve the identified problems. For this to be done appropriately, elements such as cost savings implemented in tandem with the institution of the WFH model or increased productivity/sales are elements considered when answering the RQ.

1.4 Research Delimitations

The WFH shift has revolutionized the way people work and as such touch on many different aspects belonging to many different research disciplines. Given the limited time to complete this thesis, the work has been delimited to only focus on the WFH aspects that relate to cybersecurity, information security and some of the underlying incentives that make companies and their employees want to institute a WFH model.

The thesis gives no deeper considerations towards issues such as the potential environmental impacts that could be attributed to having less people commuting to and from a physical office. Neither does the work consider financial impacts other than that of the employer, or company, and the employee. Governmental perspectives, for example, such as the potential losses of tax revenue associated with having fewer companies pay for office space or cost savings associated with reduced road maintenance are not investigated in the paper.

Further, the financial aspects and incentives associated with the WFH model is not pursued explicitly in the SLR process for time-saving reasons and because these aspects were deemed to be better investigated through semi-structured interviews conducted with companies working with a WFH model. With that said, a short summary of employee and employer incentives are introduced in the background section.

1.5 Thesis Structure

The thesis is structured as follows: Chapter 2 is used to provide background information relevant to the research area, Chapter 3 is used to provide information on the methodology employed by the paper, Chapter 4 presents the results, Chapter 5 is used to discuss the findings as well as ethical and societal aspects and Chapter 6 is used to conclude the work and suggest future research.

2 Background

This chapter identifies, introduces, and discusses key concepts related to the research topic and goal. The purpose of this chapter is to serve as useful background information when reading the thesis. The chapter covers the WFH model, cybersecurity, information security, common cyberattacks and common security controls.

2.1 Work From Home

To achieve the research goal and answer the research questions, it is important to first establish a basic understanding of how WFH is generally implemented in the real world when connecting employee homes to the necessary company resources needed to carry out their jobs.

Additionally, it is important to understand why the WFH model is still implemented today despite the government mandated lockdowns having concluded and why it is likely to continue its existence moving into the future.

This section will provide some background information on the WFH model, how it is generally technically implemented, and what incentives that exists from an employer and employee perspective to want to implement a WFH model.

2.1.1 WFH Model

WFH is not a new concept but rather something that has been around since the 1970s (Medina-Rodriguez et al., 2020) when researchers and companies started experimenting with the ability to work remotely. The original term used to describe the WFH phenomenon was “Telework” which was used to describe employees working remotely outside the office using a telephone. This form of working was commonly associated with low-skilled labor that typically did not need access to any other equipment than a telephone.

Since the 1970s the WFH phenomenon has grown into something new entirely that no longer resemble the Teleworking of the 1970s. Significant technological advances have made it possible for companies to share advanced technological resources with their employees which makes the WFH model possible for more advanced work roles.

Virtual Private Network (VPN) that facilitate the connecting of employee to organizations securely over the internet and Cloud services that provide employees with additional computing power and ease of access to company servers are but two of the technological advances that have taken place and has created a situation which makes it possible for most office jobs to be carried out entirely remotely from the employee home without having to access the office.

Another aspect that plays a big part in the spread and viability of the WFH model is the significant advances and improvements made to internet infrastructure across the globe. Internet connectivity has become far more accessible and with better technical specifications than ever before as fiber connections with gigabit bandwidth replace modem connections with kilobit speeds. Internet users in 2022, for instance, was measured to 5,54 billion (Internetworldstats, 2022) which can be compared to the 16 million users that had access to the internet in 1995.

2.1.2 Employer Incentives

The WFH model have long been associated with a long list of incentives with benefits to both worker productivity and morale as well as a number of cost saving measures being made available. Studies show that productivity amongst employees working from home is increased due to a combination of factors such as the decreased time and energy used commuting, fewer sick days, more suitable work environment and more flexibility making it easier to manage energy levels and divide work over longer parts of the day (Bloom et al., 2012: Bloom, 2020).

Shifting to a WFH model open up for several cost saving measures from the employer perspective such as the ability to reduce physical office space or remove it entirely (Borkovich and Skovira, 2020). While the cost of office space is highly dependent on geographical location, there is little doubt that it constitutes a significant expense for any company with the average cost of rent set at approximately 1200 USD per square meter (Statista, 2022).

The shift towards the WFH model means that the company is no longer bound by geographical restraints which means that it becomes possible for the employer to access the global labor market rather than one local to the physical office when attempting to hire talent (Borkovich and Skovira, 2020). This means that wages can be pushed and/or special expertise becomes easier to find. Additionally, as WFH is a highly popular form of working with 60 percent of the respondents in the PGi 2020 survey stating would quit their current position for a similar job and pay if it meant that they could work from home full-time (O'Brien, 2020), the WFH model can be leveraged to hire someone that would otherwise have rejected the job offer.

2.1.3 Employee Incentives

Hackney et al., (2022) points to WFH as often being associated with positive factors such as the need for fewer breaks, less sick days, improved focus with less distractions, increased job autonomy, improved job satisfaction, and flexibility to work around life commitments.

While WFH from the employee perspective is still largely associated with positive aspects, it is not as unambiguous as it is from the employer perspective and

suggest that for the positives to remain positive, it is necessary for employers to respect the boundaries between the professional and private sphere and not encroach on employee spare time with employees citing the inability to unplug and the blurred lines between work and private life leading to increased stress and reduced work satisfaction and performance.

Hackney et al., (2022) established a timeline of academic papers written on the work from home phenomenon and drew the conclusion that a shift occurred during the COVID-19 pandemic. Out of the papers written before the COVID-19 pandemic on the WFH model, 79 percent were overwhelmingly positive and pointing to increased productivity and performance amongst employees with no articles having reported a decrease. Some of the factors analyzed were reduced turnover rates and stress, increased cost savings, higher work engagement and morale, increased job satisfaction, better work-life balance, reduced absenteeism, greater organizational commitment, and increased motivation.

When Hackney et al., (2022) investigated papers written during the COVID-19 pandemic, the results began to become mixed with only 23 percent of the articles having reported positive impacts on productivity and performance, 38 percent showing mixed results and 38 percent showing negative results. Out of the papers that highlighted negative results on productivity and performance, increased work intensification and stress being a key factor and it became evident that employers had taken advantage of the improved access to their employees and encroached on leisure time necessary to for employees to rewind and recharge.

The image of mixed results with employers having taken advantage of the improved access to their employees and demanding a higher work output was confirmed by Patanjali and Bhatta (2022) who found that, while roughly twice as many respondents were positive to the WFH model (39,22 percent to 20,59 percent) and felt that the WFH shift had resulted in increased productivity, out of the respondents that had a negative sentiment towards the WFH model the most common reasoning given were increased stress levels and increased work hours.

Another element of WFH to consider is the work environment. Smite et al., (2023) suggested that a large contributing factor to why WFH could be considered less comfortable than working out of the office was that employers take responsibility for the ergonomics of the office space but not for the home office which was an aspect also lifted by Patanjali and Bhatta.

The factor of ergonomics could help to explain why studies reviewed by Hackney et al., (2022) written before the pandemic were overwhelmingly positive as the WFH model has moved from being a niche work model that was only made available to a privileged select few employees to becoming a more mainstream

model. Employees working from home prior to the pandemic were more likely to have established for themselves a home office in their homes and were less likely to have to share their workspace with other people such as family members.

2.2 Legal Considerations

This section discusses the legal considerations that must be made when implementing the WFH model in Sweden. The section discusses the Swedish Arbetsmiljölagen, or the work environment act (SFS 1977:1160), and the EU mandated General Data Protection Regulation (European Parliament and Council of the European Union, 2016) and NIS/NIS2 directive.

2.2.1 Work Environment Act

The work environment act is a Swedish law whose purpose is to prevent illness and accidents in the workplace and achieve a good working environment (SFS 1977:1160). The work environment act regulates factors such as ergonomics, sound, lighting, and temperature. While the work environment act is exclusive to Sweden, many other countries have their equivalent laws designed to regulate similar aspects of employee working conditions. The work environment act regulates working conditions for employees regardless of whether they work out of the office or from their homes. This means that employees and employers who have instituted WFH arrangements are not excluded from the work environment act and employers are still responsible to ensure that the work environment that their employees work out of fulfil certain prerequisites with the aim of ensuring that employee illness and accidents are avoided (Arbetsmiljöverket, 2023). In a WFH environment where employers may not be aware of the working conditions of the employees, the employees and employer are encouraged to work together to achieve a good working environment. Concretely, this means that the employee is responsible for notifying and making their employer aware of any shortcomings in the current work environment arrangements.

2.2.2 General Data Protection Regulation

The General Data Protection Regulation, more commonly referred to as “GDPR” (European Parliament and Council of the European Union, 2016), is an EU law that all EU member states and all companies processing data for EU residents must comply with. GDPR is a set of data protection rules that regulate how Personally Identifiable Information (PII) concerning EU citizens are stored, processed, and protected. Under GDPR, informed consent must be given by the user. In a WFH setting, GDPR mandates that every employee handling PII data on their private IT infrastructure also takes the necessary steps to protect said data both in transit and storage. In a WFH setting this is typically done through

establishing a secure VPN-connection between the corporate IT infrastructure and the private IT infrastructure and encrypting data stored in the private IT infrastructure.

2.2.3 The Network and Information Security Directive

The Network and Information Security Directive (NIS) is the first EU legislation on cybersecurity with the intention of achieving a high common level of cybersecurity across the union (Groothuis et al., 2021) and improve cooperation between EU member states on the exchange of strategic information. The NIS directive was recently replaced with the NIS2 directive which will affect all large and medium sized organizations within the sectors of banking, transportation, energy, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructures operating within the EU.

The NIS2 directives outlines that member states shall ensure that companies operating in the previous mentioned sectors shall include the following according to Article 21 of the NIS2 directives (NIS2, 2022);

(a) Policies on risk analysis and information system security.

(b) Incident handling.

(c) Business continuity, such as backup management, disaster recovery and crisis management.

(d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

(e) Security in network and information system acquisition, development and maintenance, including vulnerability handling and disclosure.

(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

(g) Basic cyber hygiene practices and cybersecurity training.

(h) Policies on procedures regarding the use of cryptography and, where appropriate, encryption.

(i) Human resource security, access control policies and asset management.

(j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

The NIS2 directive requires all EU member states to have implemented the requirements outlined by the directive before the 24th of September 2024.

2.3 Information Security and Cybersecurity

Given that the work attempts to analyze security issues in the WFH model from both the field of cybersecurity as well as the field of information security, it is important to establish a working definition of what cybersecurity and information security means. This working definition is especially important as cybersecurity and information security are often used interchangeably due to the significant overlap that exists between the two fields which can cause confusion.

While it is true that both information security and cybersecurity attempt to protect company IT resources, the terms are used to describe two distinctly different research disciplines and professional practices. For instance, information security often views the human factor from the perspective of the roles they play within the security process whereas cybersecurity views the human factor in terms of a target for potential attacks (von Solms and van Niekerk, 2013).

This section will provide a working definition for the terms information security and cybersecurity and give a short introduction to the respective terms as they relate to the WFH model.

2.3.1 Information Security

The concept of information security is defined by the International Organization for Standardization (ISO) as the "preservation of confidentiality, integrity and availability" (ISO, 2018, 3.28). Confidentiality, Integrity, and Availability make up the three pillars of the CIA triad;

- Confidentiality is a measurement for how confidential data is. In information security terms, the confidentiality part of the CIA triangle seeks to ensure that information/data is not revealed or accessible to individuals that lack the authorization.
- Integrity is a measurement for how immutable data is. In information security terms, the integrity part of the CIA triangle seeks to protect information/data from being modified or altered by unauthorized individuals.
- Availability is a measurement for how accessible the data is. In information security terms, the availability part of the CIA triangle seeks to protect information/data from being accessed by unauthorized individuals while remaining accessible to those with the right authorization on demand.

The concepts that make up the CIA triad can be viewed to, at least in part, stand in contrast to each other. Increases in availability will inevitably make it more difficult to maintain the confidentiality and integrity of the information or data which makes the triad a constant balancing act between making information available while still preserving its integrity and confidentiality. Understanding

that the CIA triad is a balancing act is important as it is one of the reasons why usability of security controls is becoming an increasingly important feature as users tend to sidestep security controls that are overly complex and require a large time commitment in implementing and maintaining.

The information security field started out as a very technical field but due to heavily criticism for its narrow focus on achieving the technical aspects of the CIA triad and its inability to consider the socio-organizational and socio-technical aspects of the field (Dhillon and Blackhouse, 2001; Dhillon and Torkzadeh, 2006, Staub and Welke, 1998), information security has since evolved to include many so-called soft issues such as organizational, cultural, ethical, policy and legal aspects (Lundgren and Möller, 2019).

While information security can be analyzed from several different perspectives, in the context of this thesis, it is important to consider information security as it relates to organizations and the people within them, which parts change when employees are no longer working out of the office and which remain the same. Åhlfeldt et al. (2007) developed the TFI model that suggest that an information system can be viewed as consisting of three distinct parts; the technical, formal, and informal parts. By adding accountability to the core characteristics of information security (Confidentiality, Integrity, Availability, and Accountability) and holding the individual to account for their actions as well as considering the part that the organization play in information security, such as through the implementation of security controls (technical), the establishment of steering documents (formal) and the influencing of corporate culture and individual behavior (informal) as it pertains to information security, Åhlfeldt et al. suggest that information security can be extended to include the organizational level and improve overall information security.

This extended way of looking at information security is both highly relevant and reasonable when working in a WFH model as employees may behave very differently to how they normally would when working from the office and where security culture and awareness is increasingly important due to the shift away from the established corporate security infrastructure to the private IT infrastructure. In such a climate, accountability is inarguably a key characteristic necessary among the employees of the company for the model to work.

Kritzinger and von Solms (2010) also highlighted the need to extend the information security structure into the home when they pointed out that employees no longer working out of the office were more prone to take greater security risks with company resources and deviate from normative security behavior as a result of the lack of security steering documents used to regulate user behavior.

2.3.2 Cybersecurity

The concept of cybersecurity is explained by the International Organization for Standardization as “the safeguarding of people, society, organizations and nations from cyber risks” (ISO, 2020, 3.2). Where information security focuses on the protection of information assets, cybersecurity focuses on the defense of the IT infrastructure and the devices that resides within it against threats from cyberspace (von Solms and van Niekerk, 2013).

The term cybersecurity is used in this work when discussing the different cyberattacks that make up the online threat landscape and the technical security controls that exist to protect against them.

In a WFH setting, the term cybersecurity can be used to describe the technical security measures implemented to connect the private and corporate IT infrastructures securely and protect the data in transit between networks, i.e., through a VPN-tunnel, and what security controls have been implemented in the respective IT infrastructures.

2.4 Common Cyberattacks

For the context of this thesis work, it is relevant to discuss some of the more common cyberattacks that exist today that threaten WFH employees and, by extension, their organizations.

This list is by no means exhaustive but only serves to paint a basic image of what the threat landscape looks like today and what threats are prevalent in a WFH context. There are far more sophisticated attacks out there, such as zero-day exploits, that are not covered here as they are unlikely to be levied against WFH employees.

2.4.1 Social Engineering Attacks

Social Engineering is described by Grassi et al. as “the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust” (Grassi et al., 2017 p. 54) and is becoming increasingly more common on the internet. Social engineering attacks are attacks that target the human factor through manipulation.

Social engineering attacks has risen as one of the more prominent threats facing employees working in a WFH model as WFH employees are more likely to spend time on non-work related activities than they were while working out of the office under the supervision of managers and IT personnel. This increase propensity to spend time on leisure activities increase the risk of the employees being exposed to and clicking on malicious links (Carpenter, 2020). While there are several more Social Engineering attacks, for the purpose of this thesis

Phishing attacks and Scareware attacks are relevant to discuss as they are the most likely social engineering attacks to be levied against WFH employees.

Phishing

Phishing attacks are perhaps the most common types of social engineering attacks currently and are defined by NIST (Nieles et al., 2017, p.81) as "a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or a website, in which the perpetrator masquerades as a legitimate business or reputable person".

During the COVID-19 pandemic, phishing attacks increased by 220 percent (Warburton, 2020) as threat actors rushed to take advantage of the unstable global situation. Phishing can be further subdivided into multiple categories; Spear phishing, Vishing, Pharming, Watering Hole, Evil Twin, Whaling, and Smishing to name but a few.

Spear Phishing

Spear phishing attacks differentiate from normal phishing attacks by being highly personalized and having been designed to target specific individuals, companies, or organizations. During the COVID-19 pandemic, it became incredibly popular for attackers to use information regarding the pandemic to launch spear phishing attacks at specific organizations with 88 percent of organizations worldwide facing spear phishing attacks in 2019 (Egan, 2020).

Vishing

Vishing attacks are also known as 'voice phishing' and is, as it sounds, a phishing attack where a phone call or voicemail is used to trick the victim into sharing sensitive information. Vishing has existed for over 30 years and despites efforts by law enforcement continues to be one of the best ways for hackers to steal information (Macej, 2022).

Pharming

Pharming is a phishing attack where fraudulent websites are used to masquerade as legitimate ones to silently gather personal information such as emails and passwords from the visiting users as well as downloading malware onto their end devices (Bodnar, 2022).

Watering Hole

A watering hole attack is very similar to a spear phishing attack, where the typical target is a company or organization. The way a watering hole attack differentiates from a spear phishing attack is that, unlike a spear phishing attack which is done through email, a watering hole attack is carried out by taking control of

and infecting a website or forum that is frequented by the company employees (R, 2018).

Evil Twin

An evil twin attack is an attack where the attacker attempts to trick users into connecting to a malicious wireless access point which in turn makes it possible for the attacker to monitor the network traffic on the access point and collect sensitive information (Ghimiray, 2022).

Whaling

Whaling is a highly personalized and targeted attack that targets senior executives through fraudulent email messages. Whaling is sometimes referred to as 'CEO fraud' as it targets exclusively the c-suite executives of the company. Whaling messages are often harder to distinguish from normal phishing attacks and even spear phishing attacks due to the language employed typically being advanced and business like (Bodnar, 2022).

Smishing

Smishing, or SMS phishing, takes advantage of the widespread use SMS messages when attempting to defraud users into revealing sensitive information. Smishing is typically dangerous as SMS messages have a higher opening rate than i.e., emails and phones, unlike emails, typically lack good filters to stop the message from being received (Corrons, 2023).

Scareware

Scareware is either a mixture of malware and social engineering or pure social engineering where the victim is scared into downloading malware or coerced into carrying out acts such as transferring money or sharing sensitive data such as user credentials under duress. Scareware often infects websites and then uses pop-ups with warnings and threats such as false antivirus pop-ups designed to cause panic (Buxton, 2022).

2.4.2 Malware Attacks

Malware is a malicious, intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems. Common types of malware are viruses, worms, trojans, spyware, adware and ransomware (Cisco, 2023a).

Viruses

Viruses are disguised as files and execute malicious code on an infected device once the file is executed by the unsuspecting victim. Viruses typically spread through downloads, email attachments or by plugging in infected external hardware to a device (Latto, 2022).

Worms

Worms are similar to viruses with the exception that they can execute and have a self-replication mechanism that allows it to replicate and spread on their own. As soon as a worm gains a foothold in a host machine, it can spread throughout a network without any external aid or actions (Belcic, 2020).

Trojans

Trojans are malicious files that appear to be legitimate files often packaged and delivered inside legitimate software. Many trojans download additional malware after having been installed. (Belcic, 2021).

Adware

Adware is malware that quite simply forcefully pushes unwanted commercial ads onto the end user, often through the browser (Latto, 2020). While adware technically is not harmful to the end user, it does have the likely effect of causing irritation to the user and create browser latency.

Ransomware

Ransomware is a type of malware that blocks access to files and computer systems through encryption while demanding a ransom payment in exchange for returning access to the user (Latto and Seguin, 2023).

Spyware

Spyware is a malware that sits quietly in the background collecting data on the unsuspecting victim. Once the spyware has been installed on the device it is used for operations such as logging the keystrokes carried out on the keyboard, otherwise referred to as keylogging, recording audio, voice or conducting screen captures and collecting the browser history of the device (Seguin, 2023).

2.4.3 Password Attacks

Passwords are the most implemented security control there is and serve as the first line of defense. Password attacks are attacks designed to bypass this defense and illicitly gain access using user credentials. The most common password attacks are brute force attacks and dictionary attacks. 81 percent of hacking-related breaches are due to weak or stolen passwords (Flynn, 2023).

Brute Force

Brute force attacks are typically carried out with the help of a password hacking tool (i.e., John the Ripper, oclHashcat, LOphtCrack) to find the correct key sequence by trying all possible character and symbol combinations within a specified character length. Modern computers can crack an eight-character alphanumeric password or ID in just a few hours (Molinaro, 2021) using a brute-force attack.

Dictionary

Dictionary attacks are, as the name suggests, password attacks that utilize a dictionary containing commonly used passwords. Dictionary attacks are often used as a first-stage attacks as they are significantly faster to carry out than brute force. If the dictionary attack fails, the password-cracking tool will often move over to a brute-force attack. Because many people use regular words as their passwords due to them being easier to remember, many passwords are vulnerable to dictionary attacks (Molinaro, 2021).

Credential Stuffing

A credential stuffing attack is when an attack has previously gained the user credentials from one source and sets out to see if the same credentials have been used for a different website, device, or service (Molinaro, 2021).

Password Spraying

Password spraying attacks is a type of brute force attack where the attacker already has access to a list of usernames and seeks out to attempt to log in using different default passwords. By continuously shifting between different accounts, password spraying attacks avoid normal lockout mechanisms in place to protect from normal brute force attacks. Password spraying attacks are considered particularly dangerous as a large portion of users fail to replace their default password.

2.4.4 Denial of Service Attacks

Denial of Service attacks are attacks designed to overwhelm a target or service, typically with illegitimate traffic, to stop legitimate users from using the service.

DDoS

Denial of service (DoS) attacks are typically distributed (DDoS) across multiple sources to make it more difficult to stop the attack once it has begun. Most DDoS attacks are conducted via botnets which are groups of devices, often infected through some type of malware, that lay dormant until called upon by a command-and-control server (CnC) to attack a target. Different types of DoS/DDoS are Application layer attacks, Protocol attacks and Volumetric attacks (Belcic, 2021).

Application Layer Attack

Application layer attacks refer to the application layer of the 7-layered OSI model where the application layer represents the top layer. Application layer attacks are designed to generate large volumes of application traffic, such as HTTP requests, that will inevitably exhaust the victims' resources.

Protocol Attacks

Protocol attacks are attacks that take advantage of the mechanics in the communication protocol, such as flooding the victim with SYN packets used to synchronize communication between sender and recipient in a TCP connection, or by sending malformed or oversized ICMP echo request messages also known as Ping of Death (PoD).

Volumetric Attacks

Volumetric attacks are as the name suggests an attempt to overwhelm the system by simply sending volumes of traffic that the target is unable to process.

2.4.5 Injection Attacks

Injection Attacks are a group of cyberattacks where something is injected into the target to illicitly gain access to a device or obtain information that can be used in future attacks. There are many different types of injection attacks, such as HTTP header injection attacks or email injection attacks, but the two most well-known injection attacks are SQL injection attacks and cross-site scripting attacks. The OWASP Foundation, which works to improve the security of software, released its top 10 exploit list in 2021 and ranked injection attacks as number three (OWASP, 2021).

SQL Injection

SQL injection attacks are used to inject SQL code into an SQL database to view or modify the database that can contain highly sensitive information such as user credentials, account numbers or other private information. SQL Injections typically target web databases and can occur via user input, cookie modification, server variables or automated hacking tools such as SQLMAP (Belcic, 2020).

Cross-site Scripting

Cross-site scripting often referred to as XSS is used to inject malicious scripts into trusted websites which are then executed on users visiting the website. XSS allows threat agents to maximize their gains while minimizing their efforts as each individual does not have to be attacked individually but each individual that visits the site is automatically made vulnerable. There are three basic categories of XSS attacks; reflected, stored and DOM-based (Belcic, 2020).

2.4.6 DNS Tunneling Attacks

DNS tunneling attacks exploit the DNS protocol to tunnel malware and other data through the DNS protocol to bypass potential security controls as DNS queries are often allowed through most firewalls or other security controls (Palo Alto Networks, no date).

2.5 Common Security Controls

Just as it is important to discuss common threats that employees working from home are confronted with, discuss the common security controls that employees can reasonably be expected to have at their disposal in their private IT infrastructure when working in a WFH setting.

2.5.1 Firewalls

A firewall is a security control that monitors incoming and outgoing traffic on a network and matches these against a set of rules that determines what traffic is and is not allowed on a network or device (Freda, 2023).

Hardware Firewall

Hardware firewalls are physical devices typically located on the network edges to help filter traffic going into the network and block unwanted traffic. Hardware firewalls can typically be found in the homes of most people today as a feature of their consumer-grade home routers.

Software Firewall

Software firewalls come, as the name suggests, in the form of software. Where hardware firewalls are typically designed to protect an entire network from unwanted traffic entering it in the first place, software firewalls are typically designed to protect specific endpoints, such as PCs, from attacks. Most computers today come with software firewalls such as the Windows Defender firewall that comes preinstalled with all Windows operation system installations since Windows XP SP2 in 2004.

2.5.2 Antivirus Software

Antivirus, or Antivirus protection software, is a program designed to prevent, detect, and help remove threats from endpoints (Cisco, 2023b). Similar to software firewalls, some form of antivirus software often comes preinstalled on most end devices today. 85 percent of American adults use some kind of antivirus software in 2022 (Turner et al., 2023).

2.5.3 Virtual Private Network

A Virtual Private Network, or a VPN, is an encrypted connection connecting devices or networks to another network over the internet while keeping the connection private. The connection is encrypted to ensure that sensitive data that is passed between the device and the network is kept safe from eavesdropping (Cisco, 2023c).

2.5.4 Multi-Factor Authentication (MFA)

Multi-factor authentication, or MFA, uses multiple sources of validation before granting access to users (Cisco, 2023d). Commonly used types of MFA are SMS codes or authenticator. MFA is used as an extra layer in case user credentials are leaked or a password attack is launched against the user. Eighty-seven percent of employees at companies with over 10,000 employees are required to use MFA (Flynn, 2023) with Smartphones at 73 percent being considered by far the most convenient method for MFA.

2.5.5 Email Filters

An email filter is a filter that analyzes incoming emails to identify spam or phishing emails and stop these from reaching the user. Most email services today employ some type of email filter.

3 Methodology

This chapter discusses the research methodology employed in the thesis work. Concretely, the chapter details the research approach, data collection methods and data analysis.

3.1 Research Approach

The research aim of this thesis work is to identify and solve problems and challenges associated with adopting a WFH model. To achieve this, several factors that are difficult to quantify (i.e., socio-technical factors) are investigated, which meant that qualitative as research methodology was deemed most suitable to achieve the stated research goal and questions of the thesis and therefore employed in the work. The research philosophy employed is interpretivist which allows the researcher to analyze different perspectives and experiences to understand and explain human and social realities (Al Balushi, 2016).

Data collection in the thesis is conducted through two different methods, Systematic Literature Review (SLR) and semi-structured interviews, to form a complete picture of the challenges and opportunities identified by both in academia and the professional sphere. Both SLR and semi-structured interviews collect qualitative data that is well-suited to help answer the research objective and questions outlined in the paper. As both data collection methods are qualitative, thematic analysis was selected as an appropriate data analysis method. Saunders et al. (2019) suggest that the work can either employs inductive or deductive reasoning as research approach when collecting and analyzing the data. Inductive reasoning means that theories are generated by the research and deductive reasoning allows the researcher to begin the research with a preconceived theory. As the work relies on two data collection methods, SLR and semi-structured interviews, a mixture of both inductive and deductive reasoning was selected to increase the depth of data analysis (Dawadi, 2020). The SLR was conducted to provide a theoretical foundation, where the research produced themes and theories inductively which was then used to draft and carry out the interview guide used by the semi-structured interviews (deductive).

3.2 Systematic Literature Review

This section details all the parameters under which the SLR was conducted. An SLR is an established method of conducting research and several frameworks have already been developed to facilitate the process of conducting the SLR. For this work, the eight-step framework created by Okoli (2015) was selected and modified to fit the parameters of the paper. The “draft a review protocol” step,

for instance, was deemed unnecessary as the paper only has one researcher and was therefore disregarded.

3.2.1 Identify the Purpose

An SLR is often a good way to gauge the prevailing sentiments that exists on a given topic within the research community and can aid the author in discovering the body of work and forming an understanding of what aspects of a problem have already been pursued to its limits and what areas require further research. The COVID-19 Pandemic and the resulting increase in WFH constitutes one of the largest shifts within the professional sphere in modern times resulting in many written papers on the topic. Only by delving into the prior academic work can the research goal and research questions of such a large topic be adequately answered.

3.2.2 SLR Delimitations

An SLR can be conducted with a broad or narrow inclusion process. A broad also referred to as a traditional approach, SLR is conducted with a wide inclusion criteria when collecting data. This is done to present a complete and accurate image of the body of work that exists within the field. In contrast to the traditional approach, the critical evaluation aims to only include studies that meet a predetermined threshold of quality to make the SLR more concise and poignant. While both methods have merit, the critical evaluation approach was deemed as the most suitable for the scope of this thesis.

The shift towards WFH is one of the most radical changes that society has made in the professional sphere since the industrial revolution and affects a wide variety of different research fields. As this thesis seeks to answer questions with information security, cybersecurity, financial and psychological implications, the body of work would simply be too large to create something of quality without the ability to scale down the body of work to include only the most relevant articles.

While the aim is to scale down the body of work to a more manageable size, it is imperative that the inclusion criteria does not become overly critical and result in over-exclusion (Meline, 2006). For this reason, great care has been taken when creating the inclusion and exclusion criteria for the SLR along with crafting the keywords used in the search strings when conducting the searching for literature to be included.

3.2.3 Practical Screen

When using a critical evaluation approach in conducting an SLR, a set of predetermined criteria is applied when searching for relevant material to be reviewed (Meline, 2006). For the SLR results to be possible to validate by other,

subsequent researchers, it is important to ensure that the criteria that were used in the SLR are well defined and that each step of the SLR process is described in some detail (Okoli, 2015). For these reasons, an overview of the inclusion and exclusion criteria can be viewed in Table 1 and the selected predetermined criteria are presented and motivated below.

Language

The language employed in the article by the authors must be either Swedish or English due to this being the languages known to the author of this paper.

Publication

The paper must have undergone a peer-reviewing process prior to being published. The reasoning for this is that peer reviewing provides a degree of quality control that can be used to scale down what would otherwise be a vast body of work given the width of the topic being researched. Webster and Watson (2002) suggest that major contributions are likely to be found in journals but that conference proceedings with a reputation for quality could also be examined and included in the SLR. Levy and Ellis (2006) point out that, although conference papers are a valuable scientific venue for the exchange of ideas, the overall rigor of conference proceedings is generally lower than those found in leading journals. For these reasons, journals and conference proceedings are selected as the primary publication sources to be included in the SLR. The deviation of this norm is if a paper was discovered during backwards or forwards referencing which Webster and Watson (2002) suggests can be a helpful tool in finding articles that were published prior to or after the publication that is being reviewed. Additionally, conference proceedings will be given extra consideration for quality when appraised for quality.

Timespan

The paper must have been published within a predetermined timespan that stretches from 2000 through to 2023 with extra weight being added to articles written during or after the COVID-19 pandemic in 2019 that started the serious shift towards Work from home that is prevalent today.

Technology advances rapidly and papers written on the Work from home phenomenon before the year 2000, while quite possibly valuable to answering the research questions and the goal of the research, will be detailing a technical situation that is vastly different to the one seen today. Available security control measures and the threat landscape are ever-evolving things that compete with one another which means that major changes are always happening. Additionally, the technology that is used to achieve Work from home along with other factors such as internet access and access to portable end devices have changed radically towards facilitating a WFH model.

Predetermined Keywords

The thesis aims to investigate the cybersecurity and information security complications faced by employees and organizations when following a WFH model. These cybersecurity and information security complications faced by employees and organizations in a WFH model also have a socio-technical dimension that is accounted for in the predetermined keywords used to search the literature.

As WFH is described through the use of various different terms (i.e., Teleworking, Remote Working, Work from Home, WFH and more.), this is also reflected by the keywords that include a combination of multiple terms used to describe the same WFH phenomenon.

While aspects such as productivity, cost and financial impacts are of interest for the review, as appropriate security measures are reasonably compared to the value of what is being protected, this is a sub aspect that will be noted during the SLR and not a directly matched key concept as this would simply make the work too large and is an aspect better answered by the semi-structured interviews conducted directly with companies.

The keywords used are grouped into two distinct categories: Work from Home terms and Security terms. All keywords used can be viewed below.

- Work from Home terms: Work from Home, Telework, Remote Work
- Security terms: Cybersecurity, Cyber Security, Information Security, Socio-technical, Security Culture

Original finding

The paper must be an original finding and not already screened in a previous search conducted using different keywords or in a different database to avoid the same paper being presented multiple times. This is increasingly important in this SLR as the topic rapidly has expanded its importance in the research and professional environment with no one established keyword to describe the WFH phenomenon leading to the keywords used to describe WFH often being used interchangeably. Additionally, as multiple databases are being used to search, there is a risk that a paper is present in multiple databases.

Database

The paper must be found within the database provided by IEEE Xplore, Web of Science, Scopus, or ACM Digital Library. These databases were carefully selected to cover the multiple aspects and fields of research that are being considered in this paper about the Work from Home paradigm with an obvious lean towards the fields of IT, Information Security and Cybersecurity. While there are multiple databases outside the selection that could have added value to the SLR should they have been included, time constraints meant that their inclusion

would have led to a decrease in the quality of the secondary data collection method employed in the paper (semi-structured interviews), diminished the quality of the SLR or both.

Relevance to Research Questions

The paper should serve to answer the research goal and questions set up in the paper. By reading the abstract of the paper it is possible to filter out papers that are not applicable to the scope of the SLR or the questions the paper attempts to answer.

Inclusion Criteria	Exclusion Criteria
The language employed by the authors of the paper is Swedish or English	The language employed in the paper is not in Swedish or English.
The paper is peer reviewed or found in a peer-reviewed paper through backwards referencing.	The paper is not peer reviewed or found in a peer-reviewed paper through backwards referencing.
The paper is published in a journal or conference proceeding	The paper is not published in a journal or conference proceeding
The paper is accessible to the researcher free of charge.	The paper charges money for access
The paper was published within the predetermined timespan 2000-2023	The paper is not published within the predetermined timespan of 2000-2023
The paper contains a keyword from the Work from Home terms group (“Work from Home”, “Telework”, “Remote Work”) combined with a keyword from the security terms group (“Cybersecurity”, “Cyber security”, “Information Security”, “Socio-technical”, “Security Culture”)	The paper does not contain a keyword from the Work from Home terms group (“Work from Home”, “Telework”, “Remote Work”) or the paper contains a keyword from the Work from Home keyword category but not a keyword from the security terms group (“Cybersecurity”, “Cyber security”, “Information Security”, “Socio-technical”, “Security Culture”)
The paper has not previously been screened when conducting a search with different keywords or in a different database.	The paper has been previously screened when conducting a search with different keywords or in a different database.

The paper was published in IEEE Xplore, Web of Science, Scopus or ACM Digital Library.	The paper is not published in IEEE Xplore, Web of Science, Scopus or ACM Digital Library.
-	The paper abstract is not relevant to the research topic.
-	The paper abstract does not help to answer any of the stated research questions.

Table 1. Inclusion and Exclusion Criteria

3.2.4 Search the Literature

The search was conducted with the previously mentioned inclusion and exclusion criteria in mind. The search was first conducted in IEEE Xplore and then repeated in Web of Science, Scopus, and ACM Digital Library subsequently. An overview of the search results can be viewed below in Table 2.

Keyword used in the Search	Database searched	Number of Results	Number of Articles meeting the predefined criteria
"Work from Home" AND Keyword from Security terms group ("Cybersecurity", "Cyber security" "Information Security", "Socio-technical", "Security Culture") i.e., "Work from Home" AND "Cybersecurity"	IEEE Xplore	1004	18
	Web of Science	671	5
	Scopus	85	2
	ACM Digital Library	320	3
"Telework" AND Keyword from Security terms group	IEEE Xplore	16	3
	Web of Science	7	1
	Scopus	30	3

("Cybersecurity", "Cyber security", "Information Security", "Socio-technical", "Security Culture") i.e., "Telework" AND "Security Culture"	ACM Digital Library	100	3
"Remote Work" AND Keyword from Security terms group ("Cybersecurity", "Cyber security", "Information Security", "Socio-technical", "Security Culture") i.e., "Remote Work" AND "CyberSec"	IEEE Xplore	1321	7
	Web of Science	3988	4
	Scopus	97	1
	ACM Digital Library	269	1

Table 2. Security Keywords

As mentioned previously, backwards, and forwards searching can be a valuable tool to cover literature that has been missed in the search due to the selection of databases, time period or keyword selection. Due to the already large number of articles extracted, only backwards searching was utilized in the SLR that yielded seven particularly interesting pieces of literature. The results of the backwards search can be viewed below in table 3.

Paper Title	Retrieved from Paper
"The Security Awareness Paradox: A Case Study"	"A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic"
"Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond"	"A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic"

“Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic”	“A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic”
“Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity”	“A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic”
“Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic”	“Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses”
“A muti-level influence model of COVID-19 themed cybercrime”	“Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses”
“Securing the home worker”	“Home working and cyber security – an outbreak of unpreparedness?”

Table 3. Backwards Search Results

3.2.5 Extract the Data

During the data extraction process outlined in the selected framework proposed by Okoli (2015), information applicable to the research question is extracted. The articles were examined for their relevance in solving the research questions presented in the thesis and then further examined against the inclusion and exclusion criteria outlined in the screening process.

During the data extraction process the paper abstract was first read and if it served to answer any of the research questions or further the research goal, the paper was extracted for quality appraisal. During this step a total of 29 articles were identified as relevant to the research topic and passed on to the quality appraisal step for full paper analysis.

3.2.6 Appraise the Quality

While there is no correct way of appraising the quality of the selected papers (Okoli, 2015), Bandara et al., (2015) suggest a number of questions could be asked to help appraise the quality of the article. Specifically, the following questions viewed below were selected as particularly suited in the context of this paper.

1. “How does this paper relate to the scope and goals of my literature review?”

2. “Does the paper contribute to answering the stated research questions of this paper?”
3. “Are the conclusions and claims of the paper backed up logically or empirically?”

Should the paper pass all the questions stated above, the paper will be considered to have passed the quality appraisal. Should the paper, however, not pass either of the questions stated above then the paper is deemed to have failed the quality appraisal and is subsequently discarded and not passed on to the Synthesis phase.

After having analyzed all the extracted papers in depth and matched them against the three questions stated above, an additional 10 articles were discarded from the SLR bringing the total number of research papers to be reviewed in the SLR down from 29 to 19. The articles that made their way to the synthesis phase can be viewed below in table 4.

Article Number	Article Name	Reference
1	“A Dynamic Theory of Security Free-Riding by Firms in the WFH Age”	Pal et al., 2022.
2	“A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack”	Alwashali et al., 2021.
3	“Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses”	Pritom et al., 2020.
4	“Cybersecurity Challenges during Pandemic in Smart Cities”	Himdi et al., 2021.
5	“An Analysis of Information Security Awareness within Home and Work Environments”	Talib et al., 2010
6	“Security vs. Flexibility: Striking a Balance in the Pandemic Era”	Soni et al., 2020

7	“A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic”	Andreasson et al., 2020
8	“The Security Awareness Paradox: A Case Study”	Tariq et al., 2014
9	“On cyberslacking: Workplace status and personal Internet use at work”	Garrett, R. K., and Danziger, J. N., 2008
10	“Home working and cyber security – an outbreak of unpreparedness?”	Furnell, S. and Shah, J. N., 2020
11	“Organizational and team culture as antecedents of protection motivation among IT employees”	Sharma, S. and Aparicio, E. 2022.
12	“Securing the home worker”	Furnell, S., 2006
13	“A multi-level influence model of COVID-19 themed cybercrime”	Naidoo, R., 2020
14	“Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic”	Khan et al., 2020
15	“Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity”	Ahmad, T., 2020
16	“Cyber security in the age of COVID-19: A	Lallie et al., 2020

	timeline and analysis of cyber-crime and cyber-attacks during the pan-demic"	
17	"Some Cyber Security Hygienic Protocols For Teleworkers In Covid-Pandemic Period And Beyond"	Abukari, A., M., and Bankas, E., K., 2020
18	"Working from home during COVID-19 crisis: a cyber security culture assessment survey"	Georgiadou et al., 2021
19	"Securing your remote workforce against new phishing attacks"	Sarginson, N., 2020

Table 4. Article Overview

3.2.7 Synthesizing Phase

When the papers have been screened, selected, and scored, it is necessary to aggregate the papers to paint a complete and coherent picture of the collected literature (Okoli, 2015). As all the reviewed studies are qualitative, they can be aggregated into groups to present a better overview of the emerging themes to come out of the SLR.

Watson and Webster (2002) suggest that synthesis is best done by creating a concept matrix or thematic analysis to showcase which concepts are covered by the papers that have been reviewed during the SLR. The synthesis yielded the following distinct concepts; Security Culture, Information Security, Cybersecurity and Cyberattacks.

3.3 Semi-structured Interviews

This section details all parameters and considerations surrounding the semi-structured interviews.

3.3.1 Creating the Interview Guide

Semi-structured interviews often entail having an interview guide that is meant to provide structure and focus to the natural flow of conversation with each interview and contain questions that can help to further and answer the research questions and goal (Adeoye-Olatude, O. and Olenik, N., 2020).

Successfully crafting an interview guide requires background knowledge of what questions are pertinent to ask and what topics are worth investigating beforehand, making it important to already have some prior knowledge of the body of work that has been produced on the research topic. This is the primary reasoning behind paring the SLR with Semi-structured interviews and conducting the SLR prior to the semi-structured interviews so that the SLR findings could serve as inspiration when crafting the interview guide.

Semi-structured interviews should be open ended to invite conversations with the interviewees and the interview guide or the questions created for it should not be followed strictly (Kalio et al., 2016). While many questions created for the interview guide were yes or no questions contrary to how semi-structured interview questions are generally constructed, this was done due to time constraints and the many topics that the interview questions covered. All participant were encouraged to expand on their answers after giving an initial yes or no answer in order to explore the topic surrounding question fully.

3.3.2 Recruitment

Once adequate background information has been obtained and the interview guide has been constructed, recruitment phase could be initiated. WFH is a research topic that affects a wide range of different companies across different sectors that may all have widely different experiences with the phenomenon, it was important for the interviews to include perspectives from representatives of companies working in very different sectors that may face very different challenges.

Additionally, the aim with the interviews was to collect data on topics not just limited to cybersecurity and information security topics. Due to this reason, it was important that the interviewee/company representative was well versed in topics that were not exclusive to the information security and cybersecurity efforts of the company but also had a good overview on company operations and could discuss topics such as company support infrastructure, what equipment is/was made available to employees, impacts brought on by the shift to working from home had on company productivity, finances and more.

The request went out to multiple companies through email and positive responses came back within a few days from four different companies. All interviews were carried out with senior employees within their respective organizations. Two out of four interviews were carried out as one on one interviews, one interview was conducted with a duo of two employees, and one of the interviews was conducted with a team of three employees. Overview information on the interviewed parties has been provided below and can be viewed in table 5.

Identifier	Company Sector	Size of Organization	Interviewee Professional title
Company 1	Administrative Authority	Large	HR Generalist
Company 2	Technology Sector	Large	Chief Security Officer
Company 3	Finance Sector	Large	Head of Communications, Assistant Head of Communication Manager, Communications Expert
Company 4	Technology Sector	Medium	Chief Financial Officer, Head of Communications Manager

Table 5. Interview Overview

3.3.3 Interview execution

The interviews were carried out remotely using online communication medium. The communication medium Zoom was suggested to all interview candidates but the choice was ultimately left to the interview candidate to decide. In all but one interview Zoom was used. In the one case Zoom was not used, Skype for Business was used as the alternative media.

Prior to the Interviews, all participants were sent the interview guide containing the questions and details outlining the pseudonymization scheme, interview purpose, publishing details and interview questions. At the start of each interview, the participant or participants were asked if they had been able to read through the interview guide and if they had understood and consented to being interviewed under the terms outlined in the anonymization scheme and if they consented to having their voices recorded for the sake of note keeping on behalf of the researcher. Once consent had been explicitly given by all participants, voice recording was enabled and the interview commenced.

After each interview was concluded, all answers were transcribed from audio to text and the sound recordings were destroyed as per the conditions stipulated by the interview guide and agreement between researcher and respondents.

3.4 Data Analysis

Data Analysis was conducted using thematic analysis. Inductive reasoning was employed when conducting the SLR to avoid biases as themes emerged from the text. When creating the interview guide, the themes that had already emerged from the SLR were used as the foundation and inspiration for the guide. By using thematic analysis, findings can be divided and synthesized within sub-categories, or themes, of heterogeneous papers (Reis et al., 2007) which suits the data collection methods employed by the paper well.

Dawadi (2020) outlines a six phase process that the work undergoes when conduct a thematic analysis; Familiarization with the data, Generating the initial codes, Searching for themes, Reviewing Themes, Defining and Naming Themes and Writing the Report.

3.4.1 Familiarization with the data

Familiarization with the data entails just what the name suggests, familiarization with the collected data to figure out what type and number of themes may emerge through the data. Concretely, during this stage, what the author did was to carefully analyze the literature that was collected for the SLR and wrote short summaries to serve as notes where and key concepts were identified and the general points of the article were recorded.

3.4.2 Generating initial codes

During the second phase, the data is revisited again and codes emerged from the text. Codes that were created for this paper were codes such as Phishing, Ransomware, Security Awareness, Multi-Factor Authentication, Email Filters, Employee Education, Policy Documents and Phishing to name but just a few.

3.4.3 Searching for themes

Phase three captures and combines clusters of codes that were formed during phase two into overarching themes. As nearly all codes that emerged during phase two have a natural place within the fields of information security or cybersecurity, despite Dawadi (2020) suggesting that this phase is the hardest, it was not that difficult to piece the themes together. An overview of the emerging themes can be viewed below.

- Cybersecurity and Attacks, Information Security, and Security Awareness and Security culture.

3.4.4 Reviewing Themes

The intention with phase four is to combine all the themes previously created to refine initially grouped themes and to fine tune the information groupings further. As previously stated, the codes that emerged and created themes have a

natural place in the fields of information security and cybersecurity making it easy to group them into very fine-tuned definition groups.

3.4.5 Defining and Naming Themes

Similar to Phase Four, this Phase is skipped as there are already premade naming schemes for the different themes that emerged from the codes making it unnecessary to come up with definitions and names.

3.4.6 Writing the report

The last and final step of the process outlined by Dawadi (2020) is to write the report using the themes created during the thematic analysis. This was also done.

3.5 Research Validity and Reliability

Ensuring rigor of qualitative research is important to assure the validity and reliability of the results and is commonly accomplished through a demonstration of trustworthiness in the results (Adeoye-Olatude and Olenik, 2020). The best way to achieve trustworthiness is through open transparency, detailing clearly every step that has been taken to achieve a result and making it possible for people who follow to reproduce the study with similar results and thereby validating the paper. For this reason, the researcher has attempted to the best of his ability to detail and outline how each step of the data collection process was carried out.

Semi-structured interviews can suffer from low validity due to the flexible nature of the format with open ended questions that can lead to inconsistencies amongst the answers. Additionally, when conducting semi-structured interviews, there is a high risk that the researchers' biases can affect the result which is why this work relied on the SLR to shape the interview guide for the semi-structured interviews to avoid any inherent biases going into the interviews. Finally, the validity of a research study involving humans can be viewed by how well the results among the study participants represent findings among similar individuals outside the study (Patino and Ferreira, 2018). This is an issue that has been carefully considered when recruiting respondents and understanding what group of respondents the data is sourced from and how the results may have been affected by the selection. The work does, for instance, make a conscious effort to not only interview cybersecurity and/or information security professionals to avoid collecting data that could present a skewed image painted by a very specific group of professionals but rather seeks to include roles with a more general view on the organization and a big picture understanding of the many factors that are affected by the shift to a WFH model.

3.6 Ethical Considerations

Levy and Ellis (2006) suggests that ethics is of great importance when conducting research and is necessary to maintain the credibility of the entire research field. When referencing and including the work of other people, great care must be taken to not take the source material out of context or make intentional misstatements about what the source material says.

The European Code of Conduct for Research Integrity (allea, 2017) outlined four guiding principles when conducting research;

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis, and the use of resources.
- Honesty in developing, undertaking, reviewing, reporting, and communicating research in a transparent, fair, full, and unbiased way.
- Respect for colleagues, research participants, society, ecosystems, cultural heritage, and the environment
- Accountability for the research from idea to publication, for its management and organization, for training, supervision and mentoring, and for its wider impacts.

The four guiding principles outlined in the European Code of Conduct for Research Integrity were amended in 2023 (allea, 2023) to also include the principles of independence and impartiality when conducting research.

Researchers must pay careful attention to how perspectives of authors and research participants of original studies are represented in the work to ensure that missing perspectives are conveyed and made visible in the text (Suri, 2019).

3.6.1 Ethical Considerations SLR

While systematic literature reviews rely on publicly available documents as evidence and do not collect or present any personal, sensitive, or confidential information, respect and professional courtesy must be extended to all literature collected and analyzed when forming an overview of the existent body of work associated with the research topic (allea, 2023).

Additionally, Suri (2019) suggests that systematic reviewers must consider how their own contextual positioning may be influencing the compilation of the review and to take care to minimize unacknowledged biases. Identifying disconfirming cases and exploring rival connections can serve to enhance the quality of the literature review.

3.6.2 Ethical Considerations Semi-structured Interviews

This paper seeks to identify problems and challenges that companies and employees are confronted with when implementing a Work from Home model.

Unlike an SLR, semi-structured interviews create original data from real companies and people that could potentially be harmful to the participants of the interviews should it be used in the wrong way.

While the questions designed for the paper were crafted with great care not to reveal potentially harmful information, it is difficult to find a balance between receiving the answers needed to produce an interesting result and protecting the participants. When faced with such challenges, it is always better to proceed with care and add as many layers of protection to the participants as possible to ensure that their participation does not lead to unforeseen repercussions. For this purpose, a pseudonymization scheme has been selected as the best way to add an additional layer of security for the companies and people that participated in the interviews without having to significantly degrade the quality of the interviews.

Pseudonymization Scheme

As an added layer of protection Pseudonymization was applied to protect the identity of the participants and the companies they represent. The pseudonymization scheme was carried out as follows:

- Participants names are withheld and in place of their name, their work title is provided i.e., Chief Security Officer.
- Company names are withheld and in place of their name, the sector that they operate along with an approximation of the size of the company is given i.e., A large company within the finance industry.

Additionally, all answers given during the interview was inspected by the researcher after the interviews had been carried out with pseudonymization in mind to ensure that no answers were given that could lead to the identification of the participant or the company they represent. This could be, for example, the name of a company program or directive shared publicly that could be used to tie the interview to a specific company. If any answers were given that could lead to the identification of the participant or the company they represent, the information was redacted.

Informed Consent

All interview questions were sent to the participants in advance of the interview to give the participants the opportunity to read through the questions and give them time to decide if there were any questions that they may not for whatever reason want to answer and ensure that the participant was not “put on the spot”. If any questions were identified as too sensitive to answer, the participant was given the right to refuse to comment.

As the interviews were audio recorded and stored temporarily until the answers had been put into writing, all participants were informed of this and were asked to give explicit consent to being recorded under this premise. The participants were informed in advance of the interviews being held regarding the pseudonymization process and were asked to give explicit consent to the pseudonymization scheme.

4 Results

This chapter presents a concept matrix created using thematic analysis and presents the results from the SLR and semi-structured interviews using the themes that have emerged during the work.

4.1 Emerging Themes

Following the Thematic Analysis guide outlined by Dawadi (2020) and the concept matrix proposed by Webster and Watson (2002), a concept matrix containing the different emerging themes found in the SLR has been created.

The themes identified when reviewing the papers included in the SLR, the following themes emerged: Information Security, Cybersecurity and attacks, and Security Awareness. To clarify which codes belong to which concept, more information is given below and an overview of the themes and papers connected to them can be viewed in the Concept Matrix in table 6.

	Concept Matrix Themes		
Paper nr.	Information Security	Cybersecurity and attacks	Security Awareness
1			X
2		X	
3		X	
4			X
5	X		X
6	X	X	X
7	X		
8	X		X
9	X		
10		X	X
11	X		
12		X	X
13	X	X	
14		X	

15		X	X
16		X	
17	X	X	X
18		X	X
19	X	X	

Table 6. Concept Matrix

4.1.1 Information Security Theme

The information security theme collects and covers all topics that has to do with organizational security aspects of the WFH model or protection of data assets. Different steering documents, such as policy documents, guidelines and procedures, and all strategic work pertaining to data assets are collected under the information security theme.

While it could be argued that security awareness falls under the theme of information security, due to it being featured so prominently in the reviewed articles it was broken out and placed into its own theme to highlight its importance.

4.1.2 Cybersecurity and Attacks Theme

The cybersecurity theme collects all security controls that are tied to physical devices or software. VPNs, firewalls, antivirus programs, email filters and more are all collected under this theme.

As Cybersecurity is closely related to cyberattacks, and because it makes sense to discuss security controls and attacks together, codes that involve different types of cyberattacks are included under this theme as well. Ransomware, Trojans, Viruses, Phishing, Zero-day attacks, Password attacks and Social engineering attacks are but a few examples of things that have been gathered under this theme.

4.1.3 Security Awareness and Culture Theme

The security awareness and culture theme was placed as its own theme due to its prominent featuring in the papers reviewed for the SLR. The security awareness and culture theme cover codes such as employee security awareness, corporate security culture, and training programs aimed to raise security awareness or improve corporate security culture.

4.2 Write the Literature Review

The final step of the guide created by Okoli (2015) suggests that the final step should be to highlight any novel findings found during the SLR and a summary

should be provided on these. Each emergent theme identified during the SLR is therefore summarized below with all its key takeaways.

4.2.1 Information Security

The Human factor is frequently being pointed to as the weakest link in the security chain. Garrett and Danziger (2008) pointed to how employees frequently break governing documents and use company resources in a way that breaks both acceptable use policies and security best practices. This problem is only further enhanced when employees move away from the secured traditional IT infrastructure of the company, where they are protected by security professionals and serious security control measures and where security steering documents regulate behavior, into their private homes. Pal et al., (2022) found that employees are increasingly using their work devices for personal tasks with, for instance, 36 percent of respondents using their work device to watch online streaming services.

Security steering documents can be useful in enhancing cybersecurity against cyberattacks to influence employees in working from home to follow security best practices (Abukari and Bankas, 2020; Ahmad, 2020; Sharma and Aparicio, 2022; Talib et al., 2010). Abukari and Bankas (2020) propose the establishment of a policies for WFH employees that considers and addresses the following key components: punitive measures, social engineering measures, preventative measures, desk policy, caller IDs, monitoring, social media, auditing and compliance, and personnel behavior.

Sharma and Aparicio (2022) suggest that organizational culture has potentially huge implications on information security compliance. Similarly to Tariq et al., (2014), Sharma and Aparicio claim that team culture could guide and improve information security behavior by making employees invested in the security work of the company and avoiding the vicious cycle that Tariq et al., (2014) discussed where people who are viewed as a security risk to the organizations cybersecurity and information security work is excluded from all security work and by doing so only perpetuate the employee remaining uneducated on cybersecurity and information security topics and a risk to the organization.

The shift from working out of the office to working out of the home has also made it increasingly difficult for companies to secure information assets as they are being stored in what is often insecure IT infrastructures. Soni et al., (2020) highlighted this issue when they made the claim that implementing and managing information security prior to shifting to the WFH model was to be considered relatively easy as all the critical data and applications belonging to the organization were being stored inside the corporate IT infrastructure that was protected by professionals and backed up by the, often significant, security apparatus of the organization. The WFH shift and the decentralization of the

storage of information has made it increasingly difficult to protect information and achieve the core principles (Confidentiality, Integrity, and Availability) of the CIA triad.

The COVID-19 pandemic exposed many disaster recovery plans and business continuity plans to be inadequate (Naidoo, 2020) and in need of major revisions to include the eventuality of future cyberwars or pandemics.

Additionally, the COVID-19 pandemic has exposed significant shortages in cybersecurity employees/experts (Soni et al., 2020, Andreasson et al., 2020). Andreasson et al., (2020) revealed when investigating Swedish administrative authorities with 174 respondents that 48 percent only had one staff member with cybersecurity as one of his/her work tasks.

4.2.2 Cybersecurity and Attacks

The WFH shift has created a situation where valuable data is being stored in the relatively insecure IT infrastructures of the employees which has turned the employees into attractive targets for cyberattacks.

Some of the challenges that organizations face now are specific to the WFH model. Abukari and Bankas (2020) highlighted the poor configuration of IT devices in employee homes in general, and the poorly configured network devices in particular, as a particularly pressing security matter. Insecure routers and networks in employee homes can be used to gain unauthorized access to the employee network which, in turn, can be used to compromise the corporate IT infrastructure due to the connection that now exists between home networks and corporate networks.

Social engineering attacks, such as phishing attacks, has increased in popularity significantly with the shift towards WFH and is being frequently identified as the biggest problem facing employees in a WFH model (Pritom et al., 2020; Alwashali et al., 2021; Sarginson, 2020; Georgiadou et al., 2021; Abukari and Bankas, 2020; Lallie et al., 2020; Ahmad, 2020; Khan et al., 2020; Naidoo, 2020). Lallie et al., (2020) and Naidoo, (2020) both found that there is a correlation between media and government announcements and cyberattacks where cybercriminals take advantage of the momentum, uncertainty and attention created by large societal events to craft elaborate social engineering, typically phishing, campaigns. Pritom et al., (2020) highlighted five different classes of COVID-19 inspired attacks (malicious websites, malicious emails, malicious mobile apps, malicious messaging, and misinformation) that were created by attackers during the height of the pandemic to take advantage of the uncertain climate, all of which were social engineering attacks. Khan et al., (2020) created a list of attacks very similar to the one by Pritom et al., (2020) with the only exception being that Khan et al. also highlighting Ransomware attacks and Smishing attacks.

While phishing attacks have been identified as the predominant attack used by cybercriminals (Lallie et al., 2020; Naidoo, 2020), WFH employees are still at risk of a multitude of other attacks such as brute force attacks, ransomware attacks, and DDoS attacks to name but a few (Lallie et al., 2020; Pritom et al., 2020; Alwashali et al., 2021). Lallie et al., (2020) points out that, while phishing attacks are the most common attacks, they are frequently used to transition into other attacks. A common example of this phenomenon are phishing attacks that transition password attacks once they have managed to get a hold of user credentials. Furthermore, is also common for attacks to be multifaceted, such as employing DDoS attacks to draw attention away from attempts to gain access through password attacks.

While not an attack, Khan et al., (2020) highlighted the 'attack' on privacy that has occurred by the big tech companies that have increased their data collection significantly since the pandemic as more aspects of the work environment is being digitized through the shift to a WFH model which increases data generation and the collection of it.

As mitigation suggestions to the many attacks associated with the WFH model, Multifactor Authentication (MFA) together with Password managers arise as the most prominently argued for security control (Ahmad, 2020; Soni et al., 2020; Furnell and Shah, 2020; Sarginson, 2020; Alwashali et al., 2021) due to their respective simplicity to use. When attempting to implement security controls for people with limited technical expertise, it is important to select a security control that will not have a negative impact on user experience though cumbersome configurations or slowing down processes. If a security control is perceived to be a hinderance, users will simply sidestep the control (Furnell, S. and Shah, J. N., 2020), especially when residing in such a free and liberated environment as their own homes. Shah (2006) highlighted the usability of security features themselves remaining a lingering problem as their interfaces are often poorly designed, with confusing functionality, and an overuse of technical terminology that discourages the users from implementing it.

When protecting the communications, VPN connections are identified by several sources as an important security control in establishing the connection between the private IT infrastructure to the corporate IT infrastructure (Sarginson, 2020; Abukari and Bankas, 2020; Ahmad, 2020; Georgiadou et al., 2022). VPN connections are highly recommended as it provides security to the data in transit. Soni et al., (2020) suggested that critical data should be categorized and only be made accessible via VPN provided by the organization to ensure that it remains segregated from data that is downloadable on a personal device.

Another element to establishing good cybersecurity to consider is the configuration aspect. Alwashali et al., (2021) suggests that device hardening is an

important part of achieving security in the home IT environment. Endpoints should block inbound communications unless there is an explicit need to allow the connection and Remote Desktop Protocol should be allowed only if MFA is enabled on the device as it is often used to carry out attacks. Abukari and Bankas, (2020) suggests that devices in the homes are typically poorly configured when compared to the work environment devices, which indicates that there may be difficulties in achieving a good security configuration on devices. Abukari and Bankas were particularly worried about the configuration of the network devices. A properly configured network devices and security controls such as firewalls can be used to raise the network security of home networks significantly (Abukari and Bankas, 2020; Furnell, 2006). Furnell (2006) found that out of 238 respondents, 44 percent had not configured their firewalls appropriately.

4.2.3 Security Awareness and Culture

In the work from home model, employees are connected to their workplace through their private IT infrastructure. In such a situation, it is imperative that companies support their employees in protecting themselves against attacks as this will in turn protect the organization from attackers using employee IT infrastructures as a backdoor into the corporate IT infrastructure (Himdi et al., 2021; Abukari and Bankas, 2020). Different employees will spend different amounts of time with different experience and know-how in setting up and protecting their private infrastructures (Pal et al., 2022) and will require varying degrees of help and support when attempting to achieve an acceptable level of security. Furnell (2006) suggested that a 'Computer Driving License' where a baseline level of competence would be required before allowing the user onto the internet. Shah further noted that currently there is no checks and balances that stops someone from connecting a device riddled with malware to a network or the internet.

Tariq et al., (2014) highlight a common problem with Security Awareness training and Security Culture being that employees who are untrained and uninformed of information security and cybersecurity risks are treated as a risk by the people responsible for conducting the security work at the company. This makes it impossible for the employees who are deemed to be a risk to improve their understanding and raising their security awareness and because their security awareness is low this creates an endless loop of negativity.

Training is shown to have a significant impact on improving user security behavior; not only are users more likely to identify threats, they are also more likely to follow security best practices. Users who had received security awareness training were 27 percent more likely to use strong passwords than people who had never received training (Talib et al., 2010). Abukari and Bankas (2020)

suggested that training protocols that focus on addressing the significant risk that social engineering attacks pose towards WFH employees should be pursued by companies. They highlight the importance of the ability of the employees to identify phishing emails, websites, and fake news as an important step to achieving security and pointed to the need for this information to be continuously refreshed to ensure that employees are always alert and up to date on the most recent developments on the threat landscape.

4.3 Results from semi-structured Interviews

This section contains the results of the semi-structured interviews. As previously stated, all participants were pseudonymized as follows: The representative of company 1 works as a HR generalist in a large administrative authority and is identified in the text simply as “Company 1”. The representative of the second company works as a chief security officer for a large company within the Technology sector and is identified in the text as “Company 2”. Company 3 was represented by a group of three people made up of one head of communications, an assistant communications manager and a communications expert who work within the finance industry. They are all collectively identified in the text as “Company 3”. The two representative of the fourth company works as chief financial officer and as head of communications manager respectively at a medium sized company within the technology sector and are collectively identified in the text as “Company 4”.

4.3.1 Work From Home

The interviewees were asked to provide some introductory background information about the WFH situation at their respective companies. The participants were asked Whether they allowed WFH, when they started allowing it (pre or post COVID-19), whether their WFH model is full-time, part time or something else and what tools they used for internal communication within their respective companies. All companies had instituted WFH when COVID-19 hit. In Companies 2, 3 and 4 the WFH privilege was extended to all employees while Company 1 instituted WFH for all employees that could fulfill their work tasks remotely and rotated the ones who had responsibilities that could not be completed remotely in and out of the office. In all interviewed companies, WFH was full-time remote with necessary office attendance for specific work-related events. All companies used some kind of corporate VPN when connecting to company resources. In Company 1, Skype for Business was used for internal communications together with email and work phone. In Companies 2, 3 Microsoft teams and WhatsApp were used for internal communications. Company 4 only used Microsoft teams for communications. Company 2 clarified their policy for internal communications as below.

"If it is business related things that need to be communicated confidentially, we have been asked to use Microsoft Teams" (Company 2)

4.3.2 Information Security

The respondents were asked about questions pertaining to the aspects of information security and the steering documents in place at their respective companies. All participants had steering documents in place to help guide employees in how to work securely when working from home but not all interviewed companies had these documents in place before the pandemic started. Company 1 had to amend existing documents and create new ones to address the new working conditions brought on by the shift. Company 4 did not have a complete set of security steering documents prior to the COVID-19 and had to hire in an outside consultant to help revise old documents and create new ones to account for the shift.

"As bad as it might sound, We never finished creating all our security documents in the first place. We started making them but I don't know why we never found the time to finish them. When the pandemic hit, with so many things going on at the same time, we simply felt overwhelmed and decided to bring in a consultant from the outside to help us update our security documents" (Company 4).

The companies differed widely on which steering documents were in place too. The differences can be illustrated by looking at each respective company stance on the topic of working from other physical spaces that were not the employee homes. In Companies 1 and 4 this action was strictly prohibited by company policy. In Company 3 this behavior was allowed in certain areas that had been cleared by the company in advance (i.e., Libraries). The response of Company 2 was that they did not have an "Work from Home" policy but rather a "Work from Anywhere" policy that allowed them to work from whatever physical space they wanted to so long as they had completed the company security education program that was mandatory for all new hires and had to be refreshed periodically by all employees.

"Actually, We do not have a "Work from Home" policy, but rather a "Work from Anywhere" policy that allows us to decide where we work. The only condition we have to fulfill is a periodic online security education program that we have to complete that makes us aware of security threats that exist while working from public spaces - like being careful of what network you connect to." (Company 2).

All interviewed companies communicated out and informed their employees of rules and regulations with some frequency although all companies admitted that

the frequency had decreased somewhat since the severity of the pandemic had subsided.

4.3.3 Security Awareness and Culture

On topics the topics of security awareness and security culture it was found that all companies had some form of employee training scheme in place but they varied in frequency. Companies 1 and 4 stated that they had a training scheme to educate employees on security practices when working from home and that they did give refresher courses. Company 4 stated that refresher courses were given on demand but that all employees had to finish it once every year. Company 1 stated that they gave refresher courses but did not want to call it periodic per say. Company 2 had the security program mentioned earlier that had to be finished as a part of new hires and had to be refreshed roughly once every six months. Company 3 had an annual security education program designed as a game that came with prices for the employees that scored the highest but participation was not mandatory. Only Company 3 could remember all the content of their training programs in detail as one of the interviewees had just finished the program recently. All participants claimed that their education programs contained information on common cyberattacks such as learning to distinguish between a phishing email and non-phishing email and know what a social engineering attack was.

All training schemes in all companies were directed towards all employees but the training scheme at Company 3 was optional as they wanted employees to participate on their own free will rather than being forced into it.

"We have tried to make the training program fun instead of forcing people to do it because we don't want people to just click through all the questions to finish it as fast as possible. We decided to score the process and give the high score a small reward like a paid lunch or something" (Company 3)

On the question of whether employees not directly working with cybersecurity and information security topics are involved in the security efforts to protect company data and assets or not, Companies 1, 2 and 4 said yes, through safe practice, but Company 1 made it clear that they have employees that work with security issues and that this work is separate from the rest. When asked to assess to what degree does employees contribute to the security work Company 1 answered medium and Companies 2 and 4 answered high. Company 3 said that non-IT employees are not really involved in the security work other than perhaps flagging suspicious emails and reading cybersecurity news that are sent out to all employees periodically. When asked to quantify involvement for non-IT employees in security work they answered "low".

4.3.4 Cybersecurity

Surprisingly, when asked if having employees working from home constituted an increased security risk for the organization none of the participants felt that it meant an increased risk. Company 1 said that it probably meant an increased risk in the beginning because of all the chaos caused by the pandemic but that they had government directives to prioritize cybersecurity and information security and that they are much more secure today than before. Company 3 said that they did not think employees working from home meant an increased risk but did agree with the example of employees storing company documents on personal devices as a little worrying. Companies 2 and 4 thought it was more secure to have employees working from home. When asked to elaborate on the reasoning for their answer Company 4 stated that the shift to WFH had forced them to bring in a outside security specialist to help them which had improved the security of the company and Company 2 replied that people had been bringing work home unofficially long before the pandemic and that the change that had occurred from then to now was that everyone was much more educated on how to practice security when working from home.

Work from Home is not something new, people have been bringing work with them home for years, unofficially. At least now it is official. What is different now is that now we have procedures in place for when we fall behind and have to work from home and everyone is much more trained in cybersecurity today than before the pandemic. Yes, I actually think it is safer now than it was before. (Company 2).

On the question of whether the respondents had experienced an increase in cyberattacks directed at their respective organizations after switching to a WFH model or not, companies 1, 2 and 4 replied no. Company 3 said that they received a little more COVID-19 related phishing emails during the pandemic but that this phenomenon had died off more than a year ago.

4.3.5 Support Infrastructure

All respondents provide IT support to their employees working at home. For communication with the IT department Company 1 uses the same tools that they use for internal communication; Skype for Business, work phones and emails. Company 4 uses work phones. Company 2 uses WhatsApp to communicate with their IT department and Company 3 has their own internal system specific for IT support tickets. When asked about the responsiveness of the IT department and whether or not it was instantaneous or not all Companies initially said yes but after a brief paus and a reassurance that the interviews were anonymous Companies 2, 3 and 4 admitted that the IT support can be very slow at times and that even smaller issues can lead to hours or even days of lost

productivity. Company 1 was satisfied with their IT department and stated that the IT department was very competent and quick to service their employees.

"Wait, this is anonymous right? Well, I guess I can tell the truth then. Our IT department is really slow and if your work laptop stops working at home you might as well go watch TV for the rest of the day" (Company 3)

Company 1 supply their employees with laptop, work phone, multifactor authentication card reader and during the height of the pandemic Company 1 offered their employees the ability to bring home an office chair. Company 2, 3 and 4 provide their employees with a work laptop.

4.3.6 Impacts on Productivity

On the topic of productivity, all respondents said that they believed that, in general terms, productivity had increased within their respective companies. Only Company 1 had measured their productivity increase but did not have the results on hand. Company 1 did, however, point out that some employees had expressed their desire to work out of the office over working from home.

4.3.7 Impacts on Financial Factors

When asked about the financial bottom line none of the respondents initially thought they had made any positive gains but once the topic of reduced office space was brought up both Company 1 and Company 2 said that they had significantly reduced their office space and that they have without a doubt saved a lot of money. Company 2 stated that, while they had not closed any office space in [redacted], they had scaled down the office space internationally. Company 3 noted that the only reason that they had not saved any money on office space, was due to the fact that they had just recently moved into their office building prior to the start of the pandemic and were tied by a rather long lease. If not for the lease, they were confident that they would have saved a significant amount of money as well. Company 4 were in a similar situation to Company 3 with just having moved into their new office and invested in office equipment.

"Actually, now that you mention office space, we have definitely made significant financial savings. We used to have two offices in [redacted] *and closed down one when we shifted towards working from home"* (Company 1).

5 Discussion

This chapter analyze the findings and highlights novel findings discovered and to make suggestions for how the WFH model can be improved upon from cybersecurity and information security perspectives. Additionally, the ethical and societal aspects associated with the findings is discussed.

5.1 Previous Research

The shift to a WFH model that often occurred as a result of the COVID-19 pandemic has had a large impact on information security and cybersecurity work. Information that used to be stored in an infrastructure protected by advanced security appliances that had been configured by security professionals is in a WFH model increasingly being stored on employee devices and on the employee networks. This decentralization of sensitive information and data created a significant challenge for organizations during the pandemic to achieve the same level of security they had prior to the shift. To address these new challenges, an increased need for security awareness and employee training was held up as the way forward which is clearly indicated by security awareness and culture being featured in over half (10 out of 19) of the reviewed papers that were included in the SLR and emerging as its own theme during the thematic analysis.

The results of the semi-structured interview, too, indicate that companies identified security awareness and culture as one of the more serious aspects of WFH needing to be addressed with some urgency with all companies interviewed having instituted not only first-time training courses for their employees, but also provided them with access to refresher courses. The improved work surrounding security awareness and culture in the companies led one of the interviewed companies draw the conclusion that, not only had instituting the WFH model not put the company at a greater risk, but thanks to the enhanced security work, the overall security of the company had increased as employees had brought their work home prior to the company shifting to a WFH model and that now thanks to the awareness training they were much better prepared and alert.

When the WFH shift occurred, many threat actors took advantage of the uncertain times and the anxiety that existed around the pandemic. The pandemic was leveraged and used to craft specific COVID-19 themed social engineering attacks as noted by both Lallie et al., (2020) and Naidoo (2020). These increased attempts to leverage social engineering attacks occurred in at a time period when employees and organizations were just in the starting phase of implementing the WFH model and were particularly vulnerable. The human factor has long been considered the weakest link in the cybersecurity and information security fields, but perhaps this is no longer the case. Tariq et al., (2014) noted the paradox that occurs due to security professionals viewing employees as the weakest

link which, in turn, leads to these employees being excluded from the security efforts of the company and serves to perpetuate the lack of knowledge among employees and creates a negative loop. Shifting to a WFH model makes it much harder for security professionals to exclude employees from the security efforts and force companies to invest more resources in providing their employees with the tools necessary to, at the very least, recognize some common security threats and attacks that they are faced with today.

This reinvigorated importance to invest in employees is more important now than ever before. According to the articles reviewed in the SLR, out of all the attacks being leveraged against WFH employees today, social engineering attacks in general, and phishing attacks in particular, are by far the most prominent which is clearly indicated by the fact that nine out of the nineteen articles included in the SLR discussing and highlighting the risks associated with phishing attacks specifically.

While security controls such as Multi-Factor Authentication (MFA) are cheap, easy to use and can be used to protect against phishing attacks, The best mitigation to phishing attacks is to quite simply train employees to recognize and distinguish between an attempted phishing attack and a legitimate message, website, or phone call. If the MFA were to be left alone to protect against phishing attacks, it is not impossible that attackers will attempt to use social engineering to bypass the MFA protection as well. Additionally, losing credentials to a phishing attack may still be a problem even if the MFA appliance protected one account or device as users are prone to recycle user credentials and use the same credentials in multiple places. That is not to say that MFA appliances do not fulfill a purpose by providing an extra layer of protection to user credentials.

Together with Password managers, MFA was one of the most recognized security control in the SLR. When implementing security controls, the usability factor needs to be carefully considered as users have a tendency to sidestep controls that are overly complicated or time consuming to implement or maintain. MFA and password managers require little to no maintenance from the employee once set up and is easily used when needed. Shah highlighted this problem with usability of security features all the way back in 2006. Shah claimed that security features tend to have interfaces that are poorly designed with confusing functionality and that use overly technical terminology that only serves to discourage users from using it. The semi-structured interviews indicate that companies still have some work to do on this front with two out of three respondents not providing or mandating the use of MFA. Considering the fact that MFA can be implemented using a phone or by relatively cheap devices, this problem could be remedied fairly easily.

One of the problems highlighted with employees shifting from working out of the office to working in a WFH model is how the equipment has been configured. Alwashali et al. (2021) suggested that device hardening is an important part of achieving security and pointed to the need to block remote desk protocol if MFA was not enabled. This sentiment was echoed by Abukari and Bankas (2020) who were particularly concerned with the configuration of network devices. Most home routers today contain firewall features and can, with proper configuration, be used as an important security control in protecting the home network from the outside. Furnell (2006) found that 238 respondents, or 44 percent, did not have appropriate firewall configurations. With that said, questions arise on who should carry the responsibility to configure the home network. While home network devices are constructed to be easier to configure than enterprise network devices, they still require significant knowledge that may be unrealistic to expect for the employee to possess. Considering the issues regarding bad configurations mentioned above, it could be more reasonable to utilize the significant resources that the company has access to. Especially when considering the potential financial cost savings and the increased security achieved. When considering the underlying incentives, companies purchasing home routers that come preconfigured with security best practices or sending out security personnel to help employees configure the home network may not be entirely unrealistic.

The research findings indicates that IT support as it relates to work from home is a possible area for significant future improvement. Only Abukari and Bankas (2020) indirectly discuss IT support when discussing desktop sharing and how it can facilitate remote problem solving for IT departments in an WFH model. Alwashali et al., (2021) only considered remote access from a security perspective when they suggested that device hardening is conducted in such a manner that Remote Desktop Protocol is explicitly blocked unless MFA is enabled to protect against ransomware attacks. The semi-structured interviews echoed similar problems with lack of IT support with three out of four admitting that seeking help from their respective IT departments was associated with significant loss of productivity.

When implementing security controls and conducting security work, it is always important to consider the costs of the security controls relative to the value of what they protect. Both information security and cybersecurity are aspects that are reasonably considered as business drivers that allow companies to take greater risks. The shift towards the WFH model is often associated with increased employee productivity, decreased costs and access to an international talent pool that makes it easier to recruit skilled labor or push down labor costs. Two out of the four respondents stated that their companies had made significant savings by moving to a WFH model due to the ability to reduce the amount

of rented office space. Furthermore, the two respondents who had not reduced office space claimed that the reason behind this was due to having invested in the office space not long before the pandemic hit and WFH became the new norm. When asked if they thought the company would have acted differently if the situation had been different, both claimed that their companies would have more than likely reduced office space to reduce costs. Office space is a significant expense, and because most office space is rented this cost is also continuous. If one were to consider the costs associated with the security controls that would be required to achieve an acceptable level of risk in a WFH model and compare these to the cost savings achieved by not having to rent office space or rent less office space the result is undoubtably in favor of the WFH model.

Considering the legal elements associated with the WFH model, the results does not give any indication in either way on the topics of GDPR or NIS2. It does, however, paint a picture of non-compliance with the work environment act. Out of the respondents interviewed, only one company provided their employees with office equipment to bring home and supported their employees in creating their home offices. Considering that the work environment act states that it is the responsibility of the employer to fulfill certain prerequisite criteria on work environment parameters such as lighting, air quality, and sound levels to avoid employee illness and accidents. The lack of support in providing the necessary equipment to create a home office suggests that compliance here may be lacking. Furthermore, no company interviewed actually sent someone out to their employees to investigate whether they were compliant with the work environment act or not.

5.2 Ethical and Societal Aspects

Researchers are always responsible for protecting and handling participant data. The need to collect data for the thesis was carefully assessed and only data with the explicit purpose to further the research goal was collected during the semi-structured interviews. Great care was taken during all phases of making this paper to avoid unnecessary data collection or the collection of sensitive data that could be used in ways other than the intentions stated in the research goal.

As the thesis focuses on security matters, any data provided by respondents could potentially be considered sensitive. For this reason, the author has gone to great lengths in providing respondents with as many layers of protection as possible and sought out to remove data that could be connected to a particular individual or organization by employing a rigorous pseudonymization scheme. Additionally, the author has sought explicit consent from all participants before including their responses in the thesis.

Finally, great care has been taken during all phases of making this paper to avoid inherent biases and allowing the information uncovered during the data collection for the paper stand on its own merit. An example of this is how the thematic coding that produced the emergent themes from the SLR was used to inspire and shape the Interview guide later used during the semi-structured interviews.

5.2.1 Societal Aspects

Work from home has the potential to reshape the world to the better. The ability to remove the need to commute to and from a physical workspace has enormous implications for the environment in a time when the planet is in a precarious situation with rising temperatures due to global warming and air pollution reaching dangerous levels in certain large cities.

Cutting out the commute would also aid in preserving limited natural resources (i.e., oil) allowing them to be put to better use. Additionally, less commuting makes it possible for governments to cut cost significantly as they no longer must spend as much resources on things like road maintenance.

Work from home also open for greater flexibility in where people choose to live which could become increasingly important in a future where living space in large cities are limited and air quality levels are questionable at best.

Out of the 16 UN Sustainable Development Goals, Work from Home could be used to address several, but the two Sustainable Development Goals that are most affected by the shift are, perhaps, Goal 4 and 11;

Sustainable Development Goal 4, “Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all”, could be facilitated significantly from Work from Home becoming the new norm. Not only does a Work from Home climate facilitate investments towards communication infrastructure that could be used for online learning, but it also gives employees better control over how they spend their hours making it easier to work and study.

Sustainable Development Goal 11, “Sustainable cities and communities” is perhaps the one which Work from Home hits on the head the most. Less need for commute to and from work will, as stated above, significantly affect pollution levels to the better, reduce the consumption of non-renewable resources and give people more freedom in deciding where to live and giving them the opportunity to move away from crowded cities to areas where housing is more plentiful.

6 Conclusion

The thesis sought out to identify the problems and challenges found in Swedish companies working in a WFH environment when attempting to enhance the state of cybersecurity and information security from both employer and employee perspectives. To achieve the research goal the following RQ:s were asked; What problems do users and companies face when attempting to improve the security of their respective IT infrastructures in a WFH model, what do users and companies currently do to mitigate or eliminate the problems they are faced with in a WFH model, and what can be done to further enhance the security state of employees and employers employing a WFH model going forward?

On the question of what problems users and companies face when attempting to improve the security of their respective IT infrastructures in a WFH model, the thesis found that phishing attacks have become the preferred method of attackers to target employees in the WFH model. Employees are frequently considered to be a weak link in security work and with the shift that comes with the WFH model from a secure corporate IT infrastructure to an insecure private IT infrastructure along with the decentralization of valuable information and data have become attractive targets for particularly social engineering attacks such as various forms of phishing attacks. The lack of security in the private IT infrastructure was identified in the thesis as missing vital security controls in place such as MFA, the lack of adequate configuration of devices and network equipment in the home networks, the lack of security steering documents pertaining to the new work situation, inadequacies in IT support provided to employees, and the lack of security awareness amongst employees.

To address the challenges highlighted above and to answer the question of what employees and companies currently do to mitigate or eliminate the problems associated with the WFH model, security training was highlighted as a prominent response to raise security awareness and improving the security culture at the company with all respondents having introduced rather extensive forms of education schemes targeting all employees of the company that not only were used to provide employees with initial training but also include refresher courses to ensure that security awareness remained high throughout the company. Every company interviewed in the semi-structured interviews indicated some optimism towards the future of WFH due to the significant advances that had been made in each respective company on the front of education, security awareness and security culture. Additionally, all companies had instituted some technical measures to secure company communications and data in transit with regards to the WFH situation. All respondent companies had identified certain communication protocols, i.e., Microsoft teams, as suitable to be used for internal communication. Additionally, all respondent companies had implemented VPN

solutions for their employees when connecting to the company IT infrastructure and resources from home.

On the question of what can be done to further enhance the security state of employees and employers moving forward, the thesis highlighted the need to address the inadequacies in device and equipment configuration in the home IT infrastructure and the improvement of IT support offered to employees working from home. Additionally, some rudimentary, and easy to implement security controls, such as MFA, should be made available to employees.

Because neither cybersecurity nor information security exists within a vacuum, and investments into security controls should be done so with the value of what they are protecting in mind, the financial aspects of the WFH model were pursued. The thesis found clear indications that, at least for larger companies, the WFH model can be associated with significant cost savings through the reduction of office space. This is true even after having considering the cost of the security appliances promoted in the SLR as necessary to achieve a high level of security due to the significant differences in costs. Indications are also given that the WFH model can be associated with higher work performance, job satisfaction rates and productivity but that this is entirely dependent on employers respecting the employee boundaries between the private and professional domains and do not use their improved access to employees to encroach on leisure time or introduce additional stress and an unreasonable workload.

Furthermore, work environment is thought to be an important aspect that correlates to the productivity level of employees working from home. The thesis suggested that there may be some room for improvement in this area. Out of the respondents interviewed, only one company had provided their employees with any office equipment to bring with them home and no company had actively investigated the work environment of their employees. Improving employee work environment is not only important to improve productivity rates, but is also regulated in the work environment act which states clearly that it is the responsibility of the employer to fulfill the prerequisite criteria on work environment parameters such as lighting, air quality and sound levels to avoid employee illness and accidents. As it currently stands, company compliance of the work environment act when working in a WFH model may be at risk.

6.1 Future work

While WFH is hardly a new concept, the large and recent shift has created a situation where there currently exists no established terminology that can be used to describe the phenomenon. Finding the right terminology would be a good first step to help explain what type of work from home that is being employed. This need for a clearer terminology is evident when looking at the results from

the SLR, where terms such as “Telework”, “Work from home”, “Remote work” are sometimes used interchangeably. Even the interviews showed signs of the terminology not being clear and different words were used to describe the same thing and the same words were used to describe different things. Creating a clear terminology surrounding the WFH phenomenon could help facilitate future research within the field, especially for the purpose of conducting future SLRs that must search the literature using specific keywords.

Furthermore, this thesis only scratched the surface of financial factors such as work performance impact, employee morale, cost saving measures from employer/employee perspectives. Much more work could be conducted on this front, especially as more companies move over to a WFH model and model remaining in use across a longer time period which could make it easier to find reliable data on which financial impacts on the company that can be attributed to making the change and instituting a WFH model.

It is important to note the limitations of the interviews here and point out that the all respondents work in either large or medium sized companies. The financial equation is likely to change for smaller companies due to how the cost reductions and increases associated with the WFH model scale and how initial costs for implementing and making support infrastructure available to a larger group of people will have similar costs as it would have if it was made available to only a small group. A server, for instance, servicing 10 people will typically cost the same as a server servicing 100 people in both maintenance and initial deployment. The correlation between costs associated with office space and number of employees is much more linear, where the costs are measured in per square meter rented, and where more employees require more square meters to work.

The semi-structured interviews conducted in this thesis proved to be a valuable tool when making approximations of the financial impacts of shifting to a WFH model but is not the in-depth analysis that would be required to draw an empirical conclusion on the impact of the shift on the company financial bottom lines. It would be interesting to see case studies that take a deeper dive into the company finances of companies employing the WFH model to see the financial impacts, especially at a company that provides its employees with adequate security appliances and office equipment to set up their home office environment.

References

Abukari, A. M., and Bankas, E. K. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific & Engineering Research*. 11(4). 1401-1407.

Adeoye-Olatude, O. A., and Olenik, N. L. (2020). Research and scholarly methods: Semi-structured interviews. *Journal of the American Collage of Clinical Pharmacy*. 4(10). 1358-1367.

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal*.

Al Balushi, K. (2016). The Use of Online Semi-Structured Interviews in Interpretive Research. *International Journal of Science and Research (IJSR)*. 7(4). 726-732.

Allea. (2017). The European Code of Conduct for Research Integrity REVISED EDITION. Available at: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf. [Online; Accessed: 3 Sep 2023].

Allea. (2023). EUROPEAN CODE OF CONDUCT FOR RESEARCH INTEGRITY – REVISED EDITION 2023. Available at: https://allea.org/wp-content/uploads/2023/08/Feedback-to-Stakeholders-on-2023-ECoC-Revision-1.pdf. [Online; Accessed: 3 Sep 2023].

Alwashali, A. A. M. A., Rahman, N. A. A., and Ismail, N. (2021). A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack. *International Conference on Developments in eSystems Engineering (DeSE)*. 92-96.

Andreasson, A., Artman, H., Brynielsson, J., and Frankie, U. (2020). A Census of Swedish Government Administration Authority Employee Communications on Cybersecurity duing the COVID-19 Pandemic. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).* 727-733.

Arbetsmiljöverket. (2023). Arbetsmiljön när du arbetar hemifrån. Available at: https://www.av.se/halsa-och-sakerhet/sjukdomar-smitta-och-mikrobiologiska-risker/smittrisker-i-arbetsmiljon/coronaviruset/arbetsmiljon-vid-hemarbete/. [Online; Accessed: 15 May 2023].

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., and Beekhuyzen, J. (2015). Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support. *Communications of the Association for Information Systems, 37*(8). 154-204.

Barrero, J. M., Bloom, N., David, S. J. (2021). WHY WORKING FROM HOME WILL STICK.

Belcic, I. (2020). What is a Computer Worm? Avast. Available at: https://www.avast.com/c-computer-worm. [Online; Accessed: 28 Jun 2023].

Belcic, I. (2020). What Is Cross-Site Scripting (XSS)? Avast. Available at: https://www.avast.com/c-xss. [Online; Accessed: 28 Jun 2023].

Belcic, I. (2021). What is a Distributed Denial of Service (DDoS) Attack and How Does It Work? Avast. Available at: https://www.avast.com/c-ddos. [Online; Accessed: 28 Jun 2023].

Belcic, I. (2021). What is Trojan Malware? The Ultimate Guide. Avast. Available at: https://www.avast.com/c-trojan. [Online; Accessed: 28 Jun 2023].

Belcic, I. (2020). What Is SQL Injection and How Does It Work? Avast. Available at: https://www.avast.com/c-sql-injection. [Online; Accessed: 28 Jun 2023].

Bloom, N., Liang, J., Roberts, J and Ying, Z. J. (2012) Does Working From Home Work? Evidence From a Chinese Experiment. *The Quarterly Journal of Economics*. 130(1).

Bloom, N. (2020). How working from home works out. *Institute for Economic Policy Research (SIERP)*. Stanford. 1-8.

Bodnar, D. (2022). Social Engineering and How to Prevent It. Avast. Available at: https://www.avast.com/c-social-engineering. [Online; Accessed: 28 Jun 2023].

Bodnar, D. (2022). What is Pharming and How to Protect Against It. Avast. Available at: https://www.avast.com/c-pharming [Online; Accessed: 28 Jun 2023].

Borkovich, D. J., and Skovira, R. J. (2020). Working from Home: Cybersecurity in the Age of COVID-19. *Issues in Information Systems*. 21(4). 234-246.

Buxton, O. (2022). What is Scareware? Detection, Prevention, and Removal. Avast. Available at: https://www.avast.com/c-scareware [Online; Accessed: 28 Jun 2023].

Carpenter, P. (2020). Remote workers more at risk for social engineered deception and cyberattack. Security. Available at: https://www.securitymagazine.com/articles/93935-remote-workers-more-at-risk-for-social-engineered-deception-and-cyberattack. [Online; Accessed: 30 Aug 2023].

Cisco. (2023a). What is Malware? Cisco. Available at: https://www.cisco.com/site/us/en/products/security/what-is-malware.html. [Online; Accessed: 8 May 2023].

Cisco. (2023b). What Is Antivirus Protection? Cisco. Available at: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-antivirus-protection.html [Online; Accessed: 8 May 2023].

Cisco. (2023c). What Is a Virtual Private Network (VPN)? Cisco. Available at: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html [Online; Accessed: 8 May 2023].

Cisco. (2023d). What is Multi-Factor Authentication (MFA)? Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~how-mfa-works. [Online; Accessed: 8 May 2023].

Cisco (2010). Cisco SAFE for Small Enterprise Networks. Cisco. Available at: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/safesmallentnetworks.html. [Online; Accessed: 8 May 2023].

Corrons, L. (2023). Smishing: The elephant in the room. Avast. Available at: https://blog.avast.com/smishing-elephant-in-the-room. [Online; Accessed: 28 Jun 2023].

Dawadi, S. (2020). Thematic Analysis Approach: Step by Step Guide for ELT Research Practitioners. *Journal of NELTA*. 25(2). 62-71.

Dhillon, G. and Backhouse, J. (2000). Technical Opinion: Information system security management in the new millennium. *Communications of the ACM*. 43(7). 125-128.

Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*. 16(3). 293-314.

Egan, G. (2020). 2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike. Proofpoint. Available at: https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical. [Online; Accessed: 28 Jun 2023].

Eurofound. (2020). Living, working and COVID-19. Available at: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20059en.pdf. [Online; Accessed: 20 May 2023].

European Parliament and Council of the European Union. (2016). General Data Protection Regulation. Regulation (EU) 2016/679 of The European Parliament and the Council of 27 April 2016 on the protection of the natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. 1-88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Online; Accessed: 30 Aug 2023].

FBI. (2020). FBI IC3 Cyber Report. Available at: https://www.fbi.gov/investigate/cyber3/ic3. [Online; Accessed: 20 May 2023].

Freda, A. (2023). Avast. What is a firewall? Avast. Available at: https://www.avast.com/c-what-is-a-firewall. [Online; Accessed: 28 Jun 2023].

Furnell, S. (2006). Securing the home worker. *Network Security*. 2006(11). 6-12.

Furnell, S. and Shah, J. N. (2020). Home working and cyber security – an outbreak in unpreparedness?. *Computer Fraud & Security*. 2020(8). 6-12.

Garrett, R. K., and Danziger, J. N. On cyberslacking: Workplace status and personal Internet use at work. *Cyberpsychology & Behavior*. 11(3). 287-292.

Ghimiray, D. (2022). What Is an Evil Twin Attack and How Does It Work? Avast. Available at: https://www.avast.com/c-evil-twin-attack. [Online; Accessed: 28 Jun 2023].

Georgiadou, A., Mouzakitis, S., and Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*. 35. 486-505.

Grassi, P. A., Garcia, M. E., and Fenton, J. L. (2017). Digital Identity Guidelines. *NIST Special Publication 800-63-3*. 54.

Groothuis, B., Maydell, E., Kaili, E. and Mariani, T. (2021). The NIS2 Directive A high common level of cybersecurity in the EU. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. [Online; Accessed: 30 Aug 2023].

Hackney, A., Yung, M., Somasundram, K. G., Nowrouzi-Kia, B., Oakman, J. and Yazdani, A. (2022). Working in the digital economy: A systematic review of the impact of work from home arrangements on personal and organizational performance and productivity. *PLOS ONE*. 1-25.

Himdi, T., Ishaque, M., and Ahmed, J. (2021). Cybersecurity Challenges during Pandemic in Smart Cities. *International Conference on Computing for Sustainable Global Development*. 445-449.

International Organization for Standardization ISO. (2018). ISO/IEC 27000:2018(en) Information technology – Security techniques – Information security management systems – Overview and vocabulary. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. [Online; Accessed: 30 Aug 2023].

International Organization for Standardization ISO-2. (2020). ISO/IEC 27100:2020(en) Information technology – Cybersecurity – Overview and concepts. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en. [Online; Accessed: 30 Aug 2023].

Kalio, H., Pietilä, A-M., Johnson, M. and Kangasniemi, M. (2016). Systematic methodological review: developing a framework for qualitative semi-structured interview guide. *Journal of Advanced Nursing*. 72(12). 2954-2965.

Khan, N. A., Brohi, S. N., and Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.

Kritzinger, E., and von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*. 29(8). 840-847.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., and Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*. 105(2021). 1-15.

Latto, N. (2020). What is adware? Avast. Available at: https://www.avast.com/c-adware. [Online; Accessed: 28 Jun 2023].

Latto, N. (2022). What is a Computer Virus and How Does It Work? Avast. Available at: https://www.avast.com/c-computer-virus. [Online; Accessed: 28 Jun 2023].

Levy, Y. and Ellis, T. (2006). A Systems Approach to Conducting an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline, 9*(1). 3-31.

Lundgren, B. and Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*. 25. 419-441.

Macej, G. (2022). What is vishing and how do I protect myself against it? Avast. Available at: https://blog.avast.com/stay-protected-vishing-scams. [Online; Accessed: 28 Jun 2023].

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

Meline, T. (2006). Selecting Studies for Systematic Review: Inclusion and Exclusion Criteria. *Contemporary Issues in Communication Science and Disorders*. 33(2006). 21-27.

Molinaro, D. (2021). Avast. The Top 8 Password-Cracking Techniques Used by Hackers. Available online: https://www.avast.com/c-password-cracking-techniques. [Online; Accessed: 28 Jun 2023].

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*. 29(3). 1-16.

Nieles, M., Dempsey, K., and Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. *Computer Security Division Information Technology Laboratory*. p. 81.

NIS2. (2022). The NIS 2 Directive, Final Text. Available at: https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html [Online; Accessed: 26 Aug 2023].

O'Brien, S. (2020). Premiere Global Services, Inc. Global Telework Survey. Available at: https://www.pgi.com/blog/2015/06/pgi-global-telework-survey/. [Online; Accessed: 20 Mar 2023].

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*. 37(43). 879-910.

OWASP Foundation. (2021). *OWASP Top 10:2021*. Available at: https://owasp.org/Top10/ [Online; Accessed: 20 Mar 2023].

Pal, R., Sequera, R. X., Zhu, L., and She, Y. (2022). A Dynamic Theory of Security Free-Riding by Firms in the WFH Age. *2022 Winter Simulation Conference (WSC)*. 484-495.

Palo Alto Networks. (no date). What is DNS Tunneling? Palo Alto Networks. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-dns-tunneling. [Online; Accessed: 28 Jun 2023].

Patanjali, S., and Bhatta, N., M., K. (2022). Work from Home During the Pandemic: The Impact of Organizational Factors on the Productivity of Employees in the IT Industry. *Vision-The Journal of Business Perspectives*.

Patino, C. M., and Ferreira, J. C. (2018). Internal and external validity: can you apply research study results to your patients? *Jornal Brasileiro de Pneumologia*.

Pritom, M. M. A., and Xu, S. (2021). Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses. *IEEE International Conference on Intelligence and Security Informatics (ISI)*. 1-6.

R, P. (2018). What's a watering hole attack? Spiceworks. Available at: https://community.spiceworks.com/topic/2146395-what-s-a-watering-hole-attack. [Online; Accessed: 28 Jun 2023].

Reis, S., Hermoni, D., Van-Raalte, R., Dahan, R., and Borkan, J. M. (2007). Aggregation of qualitative studies – From theory to practice: Patient priorities and family/medicine/general practice evaluations. *Patient Education and Counseling*. 65(2). 214-222.

Sarginson, N. (2020). Securing your remote workforce against new phishing attacks. *Computer Fraud & Security*. 2020(9). 9-12.

Saunders, M., Lewis, P., and Thornhill, A. (2019). Research Methods for Business Students Chapter 4: Understanding research philosophy and approaches to theory development. 8(4). 128-171.

Sharma, S. and Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security 120 (2022)*.

Seguin, P. and Latto, N. (2023). The Essential Guide to Ransomware. Avast. Available at: https://www.avast.com/c-what-is-ransomware. [Online; Accessed: 28 Jun 2023].

Seguin, P. (2023). What Is Spyware, Who Can Be Attacked, and How Can You Prevent It? Avast. Available at: https://www.avast.com/c-spyware. [Online; Accessed: 28 Jun 2023].

Smite, D., Brede Moe, N., Hildrum, J., Gonzalez-Huerta, J. and Mendez, D. (2023). Work-from-home is here to stay: Call for flexibility in post-pandemic work policies. *The Journal of Systems & Software*. 195 (2023).

Statista. (2023). Annual net effective cost for prime office space in selected markets worldwide in 4th quarter 2021 and 3rd quarter 2022. Available at: https://www.statista.com/statistics/973436/office-markets-annual-cost-per-sq-f-global/. [Online; Accessed: 10 Jul 2023].

Staub, D. W., and Welke, R. J. (1998). Coping with System Risks: Security Planning Models for Management Decision Making. *MIS Quarterly*. 22(4). 441-469.

Soni, V., Kukreja, D. and Sharma, D. K. (2020). Security vs. Flexibility: Striking a Balance in the Pandemic Era. *IEEE Conference on Advanced Networks and Telecommunications Systems (ANTS)*. 1-5.

Suri, H. (2019). Ethical Considerations of Conducting Systematic Reviews in Educational Research. *Systematic Reviews in Educational Research*, 41-54.

Talib, S., Clarke, N. and Furnell, M. S. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *International Conference on Availability, Reliability and Security*. 196-203.

Tariq, M. A., Brynielsson, J., Artman, H. (2014). The Security Awareness Paradox: A Case Study. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*. 704-711.

Turner, G., Vigdeman, A., Birnstengel, C., Cruz, B., and Adkins, M. (2023). 2023 Antivirus Market Annual Report. Security.org. Available at: https://www.security.org/antivirus/antivirus-consumer-report-annual/. [Online; Accessed: 10 Jul 2023].

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

Warburton, D. (2020). 2020 Phishing and Fraud Report. F5 Labs. Available at: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report. [Online; Accessed: 28 Jun 2023].

Webster, J. and Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*. *26*(2). xiii-xxiii.

World Health Organisation. (2023). Statement on the fifteenth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. WHO. Available at: https://www.who.int/news/item/05-05-2023-statement-on-the-fifteenth-meeting-of-the-international-health-regulations-

(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic. [Online; Accessed: 10 May 2023].

Åhlfeldt, R-M., Spagnoletti, P., and Sindre, G. (2007). Improving the Information Security Model by using TFI. *IFIP International Information Security Conference*. 73-84.

Appendix A - Interview Guide

Introduction

These interviews are carried out as a part of the second year master's thesis for the program titled "Privacy, Information Security and Cyber Security" at the university of Skövde (more information about the program can be viewed here: https://www.his.se/en/education/informatics/privacy-information-and-cyber-security-masters-programme-iicma/).

Goal with the Interviews

The goal of the interviews is to gain insight into how the shift towards Work from Home (WFH) that often occurred in companies and organizations as a direct result of the COVID-19 pandemic has impacted businesses and organizations on the ground. The answers of the interviews will be contrasted to the prior academic body of work conducted on the impacts of Work from Home on factors such as Finances, Productivity, Information Security and Cyber Security to draw a conclusion on whether Work from Home is a sustainable method of working moving into the future and whether or not there are large discrepancies between companies practicing Work from Home in some capacity to academic thoughts on the matter.

Anonymization, Format and Consent

All participants in the interviews will only be known to the interviewer and will be fully anonymized in the written text for ethical reasons and to safeguard the individuals and organizations that participate in the investigation. In place of the name of the participant, the work title of the individual will be used and in place of the name of the organization an approximation of the size of the organization will be given along with the approximate sector that the organization operate within. An example of how anonymization in the written text is done is given below;

CISO in a medium sized company within the finance industry

The interviews will be conducted verbally either in person or through preferential communication medium (i.e., Skype, Zoom, Discord). The interviews will be recorded to capture the full conversation and to avoid misrepresentation of the answers given during the interview when transferred over into text. All participants must consent to the format before the interview is conducted.

Publishing

The final paper will be published upon completion through the university in Digitala Vetenskapliga Arkivet (DiVA).

Interview Questions

Work from Home

- Q1 - Do you currently allow Work from Home in some capacity at the company?
    - *If Yes:*
        - When did you start allowing Work from Home? Was it before or after the COVID-19 outbreak?
        - Is the Work from Home privilege extended to all employees, most employees or only a select few?
        - How does Work from Home look like at the company? (Full-time remote work, Part-time telework or Full-time remote work with necessary office attendance for specific work related events?)
        - What tools do you use to connect the employee working from home to company resources (i.e., Corporate VPN)?
        - What tools do you use for internal communication within the company with employees working from home (i.e., email or Zoom)?
    - *If No:*
        - Did you previously allow Work from Home?
            - *If Yes:*
                - Why did you transition back to a Work from Office paradigm?

        - Are there any plans to re-institute Work from Home in the future?
    - *If No:*
        - Was it ever a topic of discussion at the company and why did you ultimately decide against it?
        - Are there currently any plans in the company to revisit the topic in the future?

Security Culture

- Q2 - Do you have steering documents such as guidelines, procedures or policies (i.e., acceptable use policy) in place to help guide employees in how to work securely when working from home?
    - *If Yes:*
        - What security steering documents do you have in place that are relevant to employees working from home?
        - Were these documents in place before the COVID-19 outbreak or did you have to amend existing documents/create new documents to address the new employee working conditions?
        - Are the contents of these steering documents communicated out to the employees, and if so, roughly how frequently?
    - *If No:*
        - Are you currently working on creating steering documents for employees working from home?
- Q3 - Do you have any employee training scheme in place to educate employees on security practices while working from home?
    - *If yes:*
        - What topics (i.e., Phishing) do the training cover?
        - Are the training schemes directed towards all employees or only employees in particular positions?
        - Are these first time courses or do you also give periodic refresher courses?
    - *If No:*
        - Do you have any plans to institute any training scheme for employees in the future?

Q4 - Would you say that employees not directly working with Cyber- and Information Security topics at the company are involved in the security efforts to protect company data and assets?

- *If Yes:*
    - Could you assess to what degree (High, Medium, Low)?
- *If No:*
    - Why not?

Information- and Cybersecurity

- Q4 - Do you feel that having employees working from home constitutes an increased security risk for the organization?
    - *If Yes*:
        - What factor(s) would you point to as of particularly high risk (i.e. employees storing company documents on personal devices or working in an insecure IT environment)?
    - *If No*:
        - Why not?
- Q5 - Did you experience an increase in cyberattacks directed at your organization and its employees after having switched to a work from home model?

- *If Yes*:
  - Has the nature of the attacks changed (i.e. more direct targeting of individuals)?
  - What would you say is the most common form of attacks you are currently witnessing?
  - Has the increased volume in attacks resulted in a reinvigorated effort in security matters (i.e. increased spending for security appliances) at the company?
  - Is the number of attacks continually rising or has the increases plateaued or decreased after a certain point?
  - Are there any particular security controls that you've implemented that you would like to point out as particularly impactful in your security work?
- Q6 – How do you see the threat landscape for employees working from home evolving in the future (Better/Worse)?

Support Infrastructure

- Q7 - Do you offer any technical support (IT support) to your employees when working from home through phone, internal messaging tools or by any other means that would not necessitate them coming into the office.
  - *If Yes:*
    - What tools do you use to communicate with the support department (i.e. phone, instant messaging)?
    - If you were to rate the responsiveness of your IT support; Is the support instant, near instant or does employees generally have to wait an extended period to be helped?
  - *If No:*
    - Are you currently working on creating means by which employees can receive support in their homes?
      - *If No*:
        - Why not?
- Q8 - Do you provide your employees with any IT equipment (i.e., work laptops) to bring home and use while working?
  - *If Yes:*
    - What IT equipment do you provide your employees with?
  - *If No:*
    - Why not?
- Q9 - Do you provide your employees with any office equipment (i.e., chairs, lamps and desks) to bring home and use while working?
  - *If Yes:*
    - What office equipment do you provide your employees with?
  - *If No:*
    - Why not?
- Q10 - Do you provide your employees with any security equipment (i.e., card readers, home routers, firewalls)?
  - *If Yes*:
    - What security equipment do you provide?
  - *If No:*
    - Why not?

Impact on Productivity

- Q11 - Have you felt any impacts on productivity at the company that can be associated with working from home (i.e. increased work performance, higher work motivation)?
  - If Yes:

        - What are they?
        - Were the general impacts on productivity overall negative or positive to the organization?
        - Have you measured the impacts on productivity, and if so how?

Impacts on Financial factors

- Q12 - Has the shift towards Work from Home impacted the financial bottom line of the company (i.e. lower utility bills, cost savings through reduced office space, increased spending on equipment)?
    - *If Yes:*
        - Have these impacts been positive or negative?
        - If you were to estimate the impacts on the company finances, how impactful would you say that they have been (Low, Medium, High)?
    - *If No*:
        - Do you have any future plans on implementing any cost saving measures or investing in any equipment that can be directly tied to the shift towards work from home?

Final thoughts

- Q13 – Are there any topics connected to Work from Home that have not been raised during the interview that you would like to raise?
    - *If Yes:*
        - What are they?
    - *If No*:
        - Thank you for the time and effort you have spent in having participated in this interview.