Linnæus University
Sweden

Degree project

Compliance with corporate ICT security practices in work from home environment

Attitude changes in the move from office to home

Author: Rosen Todorov
Supervisor: Sarfraz Iqbal
Examiner: Anita Mirijamdotter /Päivi Jokela
Date: 2022-02-02
Course Code: 4IK50E, 15 credits
Subject: Information Systems
Level: Graduate
Department of Informatics

Abstract
The Covid-19 pandemic and the ensuing lockdowns that multiple countries put in place have forced companies to nearly instantly switch to an entirely remote work environment, irrelevant if they were prepared to or not. Such abrupt change in the work environment and the digital nature of modern work is bound to raise issues with employees, specifically in terms of security and compliance. Through the prism of Habit theory this thesis investigates exactly what the impact on employees has been and how in turn employee attitude has impacted company security compliance. Including multiple companies and countries allows to establish what have been the universal issues employees encountered. Limiting the scope to companies in the IT sector presumes the organizations covered by the research would have been more likely and prepared to move to remote work, although the results of the research indicate not all companies were ready for this. The unprecedented nature and abruptness of the lockdowns caused a mix of compliance issues for organizations, only some of which were addressed in the course of lockdown period and was mostly dependent on companies' readiness to move to a remote-work model. Furthermore, the findings suggest that compliance is highly dependent on self-efficacy and the ways companies can address this is by targeting specific employee habits.

Table of Contents

1. **Introduction**

This chapter establishes the background and trends in the area of remote and hybrid work, how these trends were forced to accelerate because of the pandemic, and what concerns the rapid shift has raised. The purpose of the research and specific research questions are supported by a preliminary review of the established body of research in the field, and the scope and limitations of the thesis are outlined.

1.1 Research Background

As economies have become more and more prosperous, companies in advanced countries develop towards knowledge and automation working model. This has allowed for the emergence of different possibilities either of remote working which can be as fully remote /telecommute, or as a part work from home, part work from office – the so-called Hybrid Workplace (Justice et al., 2019). While this has been a definite trend over recent years, companies have not made quick strides to move over to a remote office environment. Until the emergence of COVID-19, the number of remote workers in the EU remained stable at 5.4% for the preceding decade 2009-2019, although so-called hybrid workers have been increasing – from 5.2% to 9% over the same period (Milasi, Fernandez-Macias and Gonzalez-Vazquez, 2020). Case studies indicate this fits employee preferences since given the choice more than half of the employees would choose a hybrid model over being fully remote, citing ”loneliness” or ”social isolation” (Bloom et al., 2015).

The impact of the global pandemic and related health and safety measures countries implemented have led many companies to scramble and accelerate their move to a fully remote working environment, as preferable to halting operations. While this can be done in a way that brings benefits to the organization in terms of productivity and costs (Bloom et al., 2015), many companies lack the knowledge, experience, or long-term vision to execute the transformation under these forced conditions (Kane, 2019). Considering the impact on employees from this transformation does not provide a more optimistic view of the current ecosystem, as even before the move to a home office environment, employees presented signs of stress and fatigue from misuse or excessive use of IT systems (Tarafdar, Gupta and Turel, 2013).

These factors have led to the rise of the research field of Computer-Supported Cooperative Work (CSCW), which investigates the cultural and social aspects of technology integration in cooperative work – remote, hybrid, or co-located, synchronous or asynchronous (Schmidt, 2011). Separation across each of these facets of organizational structure allows for more narrow-focused changes to business transformations as well as gaining a better understanding of the factors affecting worker performance and satisfaction. Using this methodological framing, this thesis will explore the employee side of the digital transformation, more specifically the impact of the rapid and forced shift in work location and daily routines. It will show how the employee attitudes and perceptions of company culture have changed in the transition from office work to remote work, and the impact of these changes on the Information security and ICT practices of corporations.

The number of variables in this area of research makes definitive findings incredibly challenging. Some researchers have started to investigate the psychological or organizational factors that contribute to employee compliance with security practices. Others have evaluated the statistical weight of specific theoretical frameworks such as Normative, or Motivational theory. The differentiation in work location has also begun to come into view with research like” Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines” (Godlove, 2012). Most of these also do not differentiate by

the type of organization, or location adding to the number of variables that can impact the results of the research as well as the practical applications of the findings.

Above all, however, no one has faced such a rapid shift in the work environment. Compounded by the fact that the circumstances around the move to remote work have been forced on companies and not being voluntary means that organizations might not be at all prepared to facilitate this shift. This leaves a tremendous research gap on how company security practices adapt to such abrupt changes and how this in turn impacts employees and their compliance.

1.2 Research Purpose

This thesis serves to identify employee perspectives on how moving to a fully remote work environment has impacted their attitude toward Information security practices and compliance. This means the organizational approach and adaptation, as well as specific security practices, are covered only as far as they have a notable impact on employees and their attitude. Specific security practices and communication strategies are entirely viewed from the perspective of the employees responsible for implementing them, as nearly 30% of security vulnerabilities stem from "insider" threats rather than external attacks on company infrastructure (Willison and Siponen, 2009). The master's thesis is focused on the societal element of corporate and information security. The focus is on how employees view and adhere to established or changing guidelines in a work environment that is undergoing drastic changes with regards to work-life balance, commuting, social interactions, and other changes brought on by the move to remote work. Based on this focus, the research questions raised are:

RQ1: How has the move to remote work changed the way security practices are communicated?

RQ2: How has the move impacted employees and their attitude towards security compliance?

1.3 Knowledge Gap

A preliminary literature review in accordance, with best practice, allows to more fully frame the thesis and its research purpose and contribution (Levy and J. Ellis, 2006). Because of the nature of the topic, which includes work from home and information security, the results of the said review are quite varied. Information security is a relatively mature topic and while the field sees constant innovation and changing best practices, there are well-established principles. The literature on the topic includes not only recent studies in implementing and maintaining best practices but also books, corporate guidelines, and other publications with near enough 70 years of backlog.

These results provide a solid background to the topic but are only tangentially related as they mostly examine IS security or Information security in a theoretical / best practice framework and do not involve the human element. Several studies examine the individual contribution to security practices from the management standpoint, related best practices, and implementation frameworks such as" Managing the introduction of information security awareness programs in organizations" (Tsohou et al., 2015) and" Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture" (Hu et al., 2012).

The other fundamental pillar of this thesis is the employee attitude toward information security and its implementation. The established literature identifies a plethora of problems related to general IT implementation practices including "technostress", misuse of IT resources, or addiction to the use of technology (Tarafdar, Gupta, and Turel, 2013). Some of

these issues, especially related to information security practices are further explored, with research delving into the possibility to involve employees less in updating security systems and the effects of culture and habit on overall Information security. The limiting factor in all these is the lack of distinguishment between the office and home environment and the employee attitude change related to moving from one working paradigm to the other.

Only one research exists that evaluates employee attitudes toward information security in a home environment vs in an office environment that can be used as e stepping stone for this master thesis. The previous findings on the topic serve to identify key attitude elements in employees that affect their compliance with security practices such as social pressure and individual empowerment (Godlove, 2012). These elements will be included in the data gathering section of this thesis, but they provide only the groundwork for establishing how attitudes change when moving from the office to remote work.

1.4 Topic Justification

Historical trends indicate the move towards a fully remote or hybrid environment is still growing, with the pandemic-related lockdowns only forcing companies to act sooner rather than later. This has given additional opportunities for researchers to validate previous studies and explore emergent issues. Despite the trend towards work from home even before the lockdowns, previous research indicates that people would prefer at least some level of face-to-face interaction (Bloom et al., 2015). Recent research validated these findings and re-iterates employees' preferences in some form of a hybrid model (Bloom, 2020). These ongoing radical changes are putting stress on companies and workers, however, the actual effects of the changes are not quite understood.

The focus on changing attitudes of this thesis serves to add insight to the significant body of research that exists examining employee behavior and compliance-related factors. Studies on technostress factors (Tarafdar, Gupta and Turel, 2013), or the relationship between culture and compliance (Son, 2011,Vance, Siponen and Pahnila, 2012) serve to establish a theoretical framing on employee motivation, however, they do not consider the working environment as a contributing factor, or how changing it may affect security compliance.

Existing research specific to employee attitude related to information security in an office or a remote environment does exist, but both environments are treated as separate, so neither a hybrid setup is considered, nor how personal attitudes change when moving to a different environment (Godlove, 2012). As a whole, the previous body of research in the area provides multiple framing tools for how employees are impacted by the change in environments, but no research examines the actual impact. The dynamic changes back-and-forth brought on by the pandemic is highly likely to force companies to change their remote and face-to-face work practices even more times. This research serves to investigate how this will impact employee attitude and information security, and provide insight into how these impacts can be mitigated.

1.5 Scope and limitations

The framework of this thesis is based on evaluating employee sentiment and how the attitude to information security in particular has changed with the shift to fully remote work. Given these factors, the scope of the research is limited to people who are working in fields or jobs that allow for fully remote work. Participants of the study will not be limited to a specific company or country, but rather the goal is to collect as varied samples as possible. Additionally, since the main parameter is the **change of attitude** when moving to remote

work, a second limitation is that, because remote work was forced on by the pandemic additional emotional factors may influence individuals.

With these limitations in place, the profile for people who will be considered for interviews in the data gathering process of this research is limited to individual contributors, or small team leaders as people in middle and upper management or executive roles are likely to have significant deviations in behavior. Participants must be employees in IT or IT-related companies as these would both likely allow for a full move to remote, but also would have the security awareness to recognize the risks in such a shift. In terms of regionality, as most major corporations have multicultural offices in multiple countries the participants will not be geographically limited, however, a minimum of 2 participants per country would be considered to reduce the risk of the results being an abortion of the norm. In addition, with the limited scope of the research gender and age will not be taken into consideration but will still be gathered.

As the scope of the research is change from the rapid shift to remote because of the pandemic, best security practices and norms are not considered. The focus is on general practices, how the move affected each of the selected parameters (attitude, compliance and communication). How this affected employees and companies and if this information shows actionable findings that can help companies improve their environment, or can help researchers understand what impact the pandemic has had on employees.

2. Literature Review

The following chapter outlines the search parameters used for the literature review and groups the findings from the selected articles based on specific themes covered by the previous research in the fields of security compliance and employee attitudes toward security practices. These are supplemented by a review of the relevant theoretical framework used in previous research and the significance of this in identifying the research gap.

2.1 Search goals and parameters

As an essential element in framing the research topic, a literature review was carried out based on general methodology practices and IS-specific recommendations. Specifically, limitation of search parameters within specific relevant literature and backward search through related reference literature (Levy and Ellis, 2006). The search was carried out using Linnaeus University's search engine – OneSearch as it links to the most relevant databases and includes the "basket of eight" – the most highly ranked IS journals (table 1):

Journal	***Abbreviation***	***ISSN***
European Journal of Information Systems	EJIS	0960-085X
Information System Journal	ISJ	1350-1917
Information System Research	ISR	1047-7047
Journal of Association for Information Systems	JAIS	1536-9323
Journal of Information Technology	JIT	0268-3962
Journal of Management Information Systems	JMIS	0742-1222
Journal of Strategic Information Systems	JSIS	0963-8687
Management Information Systems Quarterly	MISQ	0276-7783

Table 1: Parameter search for basket of eight

Initial search parameters used were limited to basked of eight and keyword search:

"Corporate security compliance" AND ISSN (0960-085x OR 1350-1917 OR 1047-7047 OR 1536-9323 OR 0268-3962 OR 0742-1222 OR 0963-8687 OR 0276-7783). Accounting for only peer-reviewed articles in English published after 2010 results in 171 hits. These parameters serve for an initial exploratory search of the topic but do not account for attitude changes or the remote work element.

Secondary search parameters used were ("Work from home" OR "Remote work" OR "Hybrid work") AND "Security compliance", where OR/AND are Boolean operations. These parameters retrieve 32 results.

A tertiary search was based on attitude-related articles. Keywords used were" Employee attitude" AND" security compliance" resulting in 59 articles.

Since the original draft of this thesis some additional research on the topic, especially surrounding COVID, has been published. However because of functional changes to OneSearch and access to it, precise identification of those works is not possible at this stage.

2.2 Selection process

Based on the iterations of search parameters the combined results were >250 articles with varying levels of relevance to the thesis topic. Articles were selected based on title relevance to the research purpose as a majority of the results were only tangentially relevant. Selection relevance was double-checked based on the contents of the abstract in order to ensure source

literature provides foundational knowledge. In the case of" Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines" (Godlove, 2012) additional steps were taken to verify that the article does not have the same research goals as this master thesis and that the research gap identified is genuine. The findings of the literature review are divided based on a thematical analysis of the selected literature.

2.3 Psychological factors for employee attitude

IT integration in the workplace has been ongoing and ever-increasing. Any and all minor operations and activities are being automated or outsourced leaving employees with an ever-increasing set of applications or devices they need to use and monitor. Increases in technology use have induced companies to also introduce ever more stringent cyber security measures in order to mitigate the risks from hackers or other cybercriminals. As employees are the endpoint for any security framework and vulnerabilities remain ever-present there has been significant research focused on employee behavior (Safa and Von Solms, 2016) or even on motivational factors for employee compliance (Son, 2011).

Recent studies however look at the negative effects of this increase in technology and how the increase itself is causing a multitude of issues. The overwhelming number of applications and devices employees are required to interface with has led to increases in "technostress" (Hwang and Cha, 2018, Tarafdar, Gupta and Turel, 2013). The findings of these studies show staggering effects of increased technology integration going beyond stress or simple misuse. Companies experience negative consequences induced by the increased demand on individual contributors, who feel strained and unable to comply with all the requirements. The main contributing factors to the increase in "technostress" identified are: "techno-overload, techno-invasion, techno-insecurity, techno-complexity, and techno-uncertainty" (Hwang and Cha, 2018).

In the past companies have attempted to ensure compliance by changing their practices and tools to require more interaction. This leads to more stress and less compliance by employees leading to a feedback loop that can spiral out of control and have a severe negative impact both on companies and employees mental health. On the other hand, the constantly increasing set of IT solutions workers have had to interact with has also been shown to lead to IT addiction problems (Tarafdar, Gupta and Turel, 2013). As can be expected with addiction symptoms, despite the reported increase in stress many employees continue to seek out IT interactions by either using commuting, personal time, or vacation to answer work emails or search for work-related information (Tarafdar, Gupta and Turel, 2013).

As "technostress" is a common finding in the studies of psychological effects of IT on employees, the recommendations for resolving the root issue also share similarities. The more detailed view is to address specific statistically significant contributors that may not be IT-related such as organizational role or organizational commitment (Hwang and Cha, 2018). The general recommended approach for companies however is to restructure and reduce the need for interfacing with technology or at least inform their employees of the risks "One of our studies showed that a simple educational video on the risks of Internet overuse significantly increased the motivation of users to control and reduce Internet use. IT leaders should provide forums, such as brown-bag meetings, for employees to discuss and share their IT-related experience" (Tarafdar, Gupta and Turel, 2013).

While these studies do not examine the work from home aspects of "technostress" the nature of requiring remote connection to work would only exacerbate the symptoms. With employees spending on average 23 minutes per day on work-related emails outside of working hours and engaging in IT-related leisure activities (Facebook, YouTube) during

working hours in conventional work settings, a work from home environment that blurs the lines between personal time and working hours can only make the situation more complex (Tarafdar, Gupta and Turel, 2013).

2.4 Employee behavior and obstacles to compliance

As the focus of this master's thesis is employee attitude towards changes in the working environment, the contribution of corporate culture and social influences have a significant role. Previous research in these areas indicates that establishing a robust company culture related to security practices can have a significantly better contribution to ensuring data protection (Vance, Siponen and Pahnila, 2012). The drive for a drastic increase in remote work has been the pandemic measures governments and companies have been forced to take, leading to the reasonable assumption that many organizations have moved to such a model without being fully prepared to do so. These changes can increase productivity on a temporary basis for most companies, but also increase feelings of "isolation" and "loneliness" in employees (Bloom et al., 2015).

The remote environment leads to a decrease in social interactions and an increase in reliance on IT. As previously mentioned, the natural result of this would be an increase in "technostress". This is a significant contributing factor to issues with security practices. The obvious solution to this would be for companies and managers to attempt and reduce complexity and required involvement by end-users in order to improve security compliance. This however does not appear to be a straightforward solution as only reducing involvement does not seem to have a significant effect on security compliance (Pham et al., 2017). What researchers have discovered is that aside from the cultural elements that induce compliance out of habit (Vance, Siponen and Pahnila, 2012), the other most contributing factors are employee empowerment and contributions (Lee and Hwang, 2021).

Reducing technical involvement can also be conducive to improving Information security, but needs to be targeted at specific issues that contribute to non-compliance such as reducing employee involvement in required software updates to improve endpoint security (Tan, Goode and Richardson, 2020). Managing these implementations and organizational changes is a key part, as cultural and technological elements of IS are interconnected with the structural and operational activities of companies. The main elements for frameworks to help manage this are related to awareness and communication of the interconnected nature of any organizational change and its impact on security considerations (Tsohou et al., 2015).

2.5 Role of management and culture in security compliance

Corporate culture and norms have a defining role in how employees view their contribution to the company and how they treat their responsibility for information security. Remote workers show a remarkable understanding of the need for Information security even when not having to follow specific norms. This is enhanced when the company has clear communication regarding the individual responsibility of employees and a clear line of communication to resolve inquiries (Godlove, 2012). This again leads to the critical role managers play in information security. While decision-makers are less likely to be an end node for information security, they are instrumental in ensiling individual beliefs and organizational culture, which drive policy compliance (Hu et al., 2012).

This preventative approach to security policy shows promises over alternatives, as evidence shows that regardless of company involvement and scrutiny, employee-related data breaches continue to occur even if an accurate correlation cannot be drawn (Cuganesan, Steele and Hart, 2017). However, a clear correlation exists between compliance with security

policies and a management-established cultural habit for compliance (Vance, Siponen and Pahnila, 2012). These relations are examined across the office and remote work environments, however with the pandemic-induced changes, there is no research that indicates how the change has impacted employees, managers, and the company culture elements that contribute to policy compliance.

2.6 Theoretical framing

Having the correct theoretical framework is crucial in establishing the significance and the scope of the research question while also providing the tools to interpret the findings (Cai et al., 2019). In this sense, the theoretical framing is narrowly linked with the literature review in establishing the background information and linking it with the gathered data. Taking this into the consideration one must also examine the theoretical framing of the literature review articles in order to understand and apply their framing correctly to the research question.

Previous research in the area of compliance is heavily reliant on non-IT-related frameworks ranging from psychology, criminology, and health to education or organizational management (Kuppusamy et al., 2020). In their systematic study of frameworks used Kuppusamy et al. determine that the most often used frameworks with more than 50% of instances are:

- Theory of planned behavior (Theory of reasoned action) – 19%
  A psychological framework that postulates that actions are based on more or less well-formulated plans or established models of behavior (Icek Ajzen, 1985)

- Protection Motivation theory – 19%
  The theory is based on the fear of a particular event transpiring, the probability of it coming to be, and the severity of the negative effect (Rogers, 1975)

- General deterrence Theory – 9.7%
  The general approach is the difficulty with measuring deterrence and outlining steps for measuring specific effects of "preventative punishment" (Gibbs, 1975)

- Neutralization theory – 7.8%
  While the theory is focused on criminal activity amongst minors, the general theme is the importance of social environment and interaction for the integration of individuals at higher risk of committing crimes (in the IT sense this would be non-compliance) (Sykes and Matza, 1957)

This means that using a framework that is based on Theory of planned behavior or on Protection motivation theory will be most in line with previous scientific studies. Habit theory is a mix of elements from Motivation theory and Theory of planned behavior as well as Cooping theory (Wood and Quinn, 2004). The elements of motivation and planned behavior theory are the driving factors for long term decision making, these are organized around achieving specific or generic goals in the mid to long term and then formulating patterns of behavior (habits) that are conducive to the attainment of said goals (Wood and Quinn, 2004). The other half of Habit theory comes from the elements of Coping theory which describes habit behavior as "homeostasis" – a state in which individuals operate in a highly effective manner in their environment irrelevant of environmental factors, but changes from the normal patterns can cause severe issues in cognitive capabilities (Lazarus and Folkman, 1984). Changes in the environment are viewed as stress factors and the trigger for coping

mechanisms with the homeostatic environment being considered nominal even if it would be considered stressful by an external observer (Lazarus and Folkman, 1984).

The way these theories fit in the framework of Habit theory is explored in “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory” (Vance, Siponen and Pahnila, 2012). The framework is structured in long-term behavioral elements – Threat appraisals and reactionary elements – Coping appraisals (Vance, Siponen and Pahnila, 2012). Each of these is divided into sub-categories with threat appraisals consisting of evaluating vulnerability, perceived severity, and expected rewards and coping appraisals consisting of rewards Efficacy, self-efficacy and response cost. The research not only presents the working model of the Habit theory framework but also evaluates the impact of each of the elements on the intention to comply with IS security policy (Vance, Siponen and Pahnila, 2012). As the nature of this thesis and the number of participants makes any statistical evaluation dubious only the relative impact of the elements will be considered in the application of the framework to the findings of the thesis.

How this will be applied in practice is by deconstructing the three main factors that are behavioral influences in Theory of planned behavior and allocating them to the decision trigger factors in Habit theory.

Theory of planned behavior elements:

- Attitudes: The individual's positive or negative evaluation of compliance with ICT security practices. Positive attitudes towards compliance may result from beliefs about the benefits of security practices, such as protecting sensitive information or maintaining organizational reputation, while negative attitudes may result from beliefs about the inconvenience or inefficiency of complying with security measures.

- Subjective norms: The individual's perception of social norms or expectations related to compliance with ICT security practices. Subjective norms may be shaped by the opinions and expectations of significant others, such as supervisors, colleagues, or IT support personnel, regarding the importance of adhering to security practices.

- Perceived behavioral control: The individual's perception of the ease or difficulty of performing ICT security practices in the WFH environment. Perceived behavioral control may be influenced by factors such as the individual's self-efficacy, perceived barriers or challenges to compliance, and the availability of resources and technical infrastructure for implementing security measures.

Theoretical Framework: Based on the Habit Theory and the TPB, the following conceptual framework is proposed for examining compliance with corporate ICT security practices in the WFH environment:

Cue:

- External cues, such as security prompts or email notifications related to security measures
- Internal cues, such as the individual's perception of the importance of ICT security practices

Routine:

- Compliance behaviors, such as following password protocols, using virtual private networks (VPNs), or encrypting communications

Reward:

- Positive rewards, such as convenience, efficiency, and ease of work
- Negative rewards, such as fear of delays, inconvenience, and penalties for non-compliance

Moderating Factors:

- Individual characteristics, such as prior ICT security knowledge, experience, and awareness
- Organizational factors, such as security policies, enforcement mechanisms, and organizational culture
- Environmental factors, such as the availability of ICT security resources and technical infrastructure in the WFH environment

Attitudes:

- Beliefs about the benefits or drawbacks of compliance with ICT security practices

Subjective Norms:

- Perceptions of social norms or expectations related to compliance with ICT security practices

Perceived Behavioral Control:

- Perceptions of ease or difficulty in performing ICT security practices in the WFH environment

These can be represented in a matrix representing origin and likelihood of compliance. Each of these factors can be fulfilled or unfulfilled to some extent which will impact an individual's likelihood of compliance and one factor can lead to changes in others. For example: high level of IT security knowledge will highly increase compliance and lack of knowledge will be decrease compliance, but IT knowledge can be impacted and increased by organizational culture, by routine training and communication (Vance, Siponen and Pahnila, 2012).

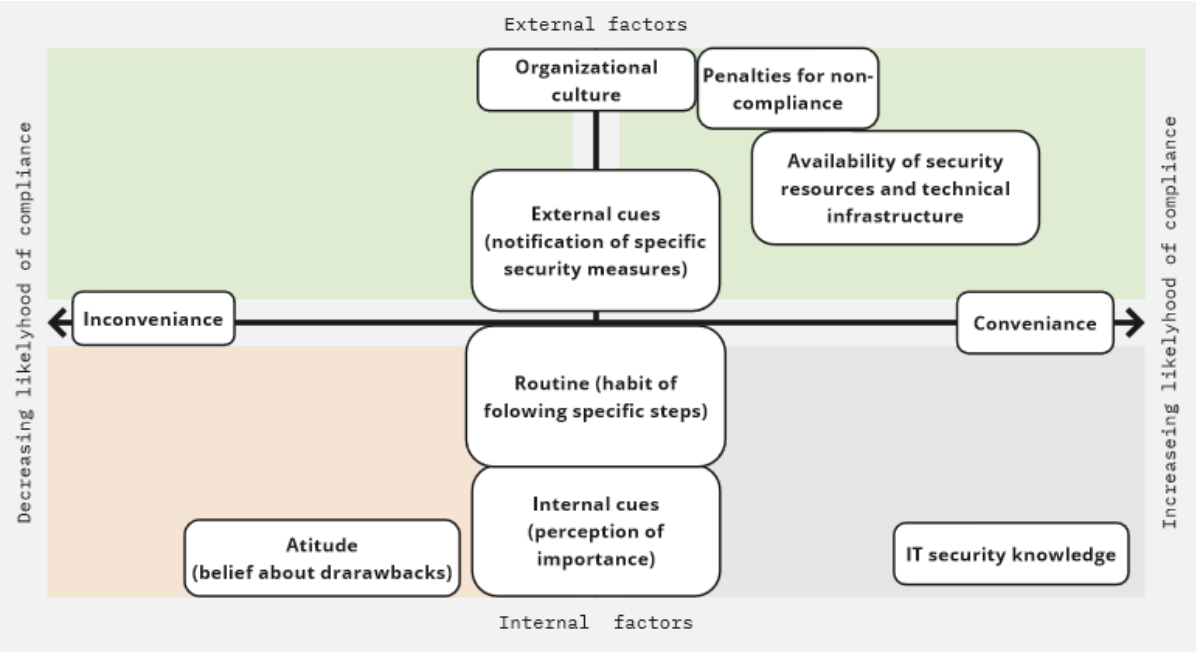

Figure 1: Impact of individual factors to compliance (based on Vance, Siponen and Pahnila, 2012, Godlove, 2012).

3. Methodology

This chapter covers the Information Systems (IS) theoretical methodology with the research-specific paradigms and methods that will be used. The data collection process is then covered by outlining how the information will be gathered, and analyzed and what are the ethical implications of this research.

3.1 Paradigm

IS methodology commonly relies on three paradigms: positivist, interpretivist, and critical realism, to understand the epistemology of the research (Creswell and Creswell, 2018). These are selected depending on the research needs. Quantitative methods and a positivist paradigm are commonly used together in research focused on explaining objective reality. The limitation of this approach can be the limited perspectives on underlying forces (Creswell and Creswell, 2018). The interpretivist paradigm is conducive to research focused on the subjective experiences of individuals and their perception of reality. Qualitative methods are most suited to this type of research. Unlike the subjective and objective approaches of these paradigms, the critical realism approach is tightly focused on people's ability to affect their reality. Instead of acknowledging the world as objective, or individuals' perceptions as subjective, it views the world through the lens of individual perception of objective reality and how people construct it through societal and cultural norms (Myers, 1997). With these limitations and uses for IS paradigms, the research focus on this thesis will be best served by applying an interpretivist view of IS, with a focus on participants' subjective views on how their environment has changed.

3.2 Research methods

Research paradigms establish the framework for a research approach, however, a paradigm is insufficient on its own to fully explore a research topic and needs to be supported by a legitimate research interest with its related research questions, data collection, and analysis methodologies (Creswell and Creswell, 2018). The investigation of employee attitude changes relies on participants' subjective perceptions of reality, therefore an interpretivist paradigm is best suited for this research.

As the nature of the study is to examine how employee attitude has changed when moving to a home environment observational approach is not applicable without significant imposition in participants' lives, which in itself may impact the validity. This means that while an ethnographic model would be best suited to fulfill the research requirements of the study and provide a consistent and objective results it is not applicable, because of the risk of invalidating the results (Schmidt, 2016). The limiting factor on participants – being knowledge workers who moved from office or hybrid environment to fully remote put constraints on the research that fit more closely to a qualitative case study (Martyn Denscombe, 2017). This can be further refined by noting the tight timeframe of the events and the single cross-country cause of the shift to remote work – the COVID19 pandemic. Such framing is necessary in order to provide a frame of reference for future research. While the focus of the thesis is the security compliance and attitudes the recency and universal reach of the pandemic is undoubtedly a major element of this research.

By expanding the participant pool beyond a single company or country, the research should be able to provide more generalized insight into employee attitudes. At the same time by taking elements of the case-study methods in structuring the interviews around a common historical framing (pandemic – move to home – changes in policies) the thesis should limit the

impact of researcher bias that is expected from using an interpretivist paradigm and an ethnographic approach (Creswell and Creswell, 2018).

3.3 Data collection

In ethnographic studies, a mix of observations, focus groups, and interviews are used to gain insight into participants' actions and decisions (Martyn Denscombe, 2017). Interviews are the preferred method for data collection for this study, because observation of remote workers will both be a huge imposition in personal space, as well as have a high likelihood of impacting the results. The selection criteria for participants are mostly determined by the purpose of the research, with secondary characteristics being convenience and availability. In order to verify the response validity of participants a semi-structured interview approach is best suited. A number of pre-determined questions will serve to verify that participants fit the research criteria as well as examine their attitudes in relation to categories framed by previous studies to establish a baseline.

To allow room for following up on individual topics with interviewees, the questions are not pre-determined or the same for all interviewees. However, in order to best serve the research paradigm and theoretical framing, the questions were formed around a pre-determined framework based on the lockdowns. The goal is to establish the homeostasis baseline for employee attitude in a work from office or hybrid environment that can then be used to analyze the impact of moving to a remote setup, the process of coping, and the impact of individual events on employee attitudes toward security. Some additional generic context data will be gathered from participants such as country, age, length of employment, or other environmental data that can be a factor in employee behavior. The interview general structure and some of the specific questions can be seen in Appendix 2. The structure was carried out with all participants while question order was varied depending on the interview flow.

Interviews were carried out over a 6-week period in order to ensure people have a similar experience and mindset to world events that may impact their mental state or their work practices. This includes covid policies across countries, announced vulnerabilities of software/platforms, and increased likelihood of cyber-attacks because of geopolitical events such as the Russian invasion of Ukraine. These events not only cause changes in the communication practices of some companies but create significant stress for some individuals based on where they live which made the short time frame for the interviews crucial.

Participants were spread across 3 European countries – Bulgaria, Germany, and Sweden, with a minimum of two participants from each country to account for the interviewee's experience to be too far from the "standard" for the respective country. Participants were selected from the author`s sphere of acquaintances with steps being taken to avoid close personal contacts that could impact the consistency of the data. Eight interviews were carried out in total, with participants covering a variety of roles that would allow for a differentiated perspective. The roles varied from technical consultants and IT transformation managers to team leads and shift planners. Some of the participants were individual contributors that are expected to work with more autonomy whereas others were in positions of authority that not only allow them visibility over the experience of multiple team members but also expect them to track employee's compliance or plan security practices communication. The overall split for roles can be segmented into administrative, operational, and conceptual roles going from least direct experience with IT to most direct experience with IT (conceptual roles being responsible to create infrastructure designs or systems).

	Country	*Role*
Participant 1	Bulgaria	Administrative – Processes specialist
Observer 1	Bulgaria	N/A – Spouse of Participant 1 (see data validity)
Participant 2	Germany	Conceptual – Technical consultant
Participant 3	Germany	Administrative – Team lead
Participant 4	Sweden	Operational – IT project coordination and implementation
Participant 5	Bulgaria	Administrative – workforce planning specialist
Participant 6	Sweden	Conceptual – Digital strategist
Participant 7	Bulgaria	Operational – IT support and deployment

Table 2: Interview participant list

3.4 Data validity

For the convenience of the participants, the interviews were carried out through online conferencing applications. In order to maximize the quality of the collected data, the participants and interviewer used cameras in order to be able to detect nonverbal cues. Audio and video recordings were not carried out in order to make the subjects feel at ease and improve the reliability of the responses (Al-Yateem, 2012). Instead, direct speech-to-text transcriptions were used to facilitate the interviews and ensure all relevant comments were recorded without impacting the quality of the interview. Each interview consisted of 3 sections:

- Greeting the participant and having a short discussion with them to gauge their behavioral baseline responses (where possible this was carried out both in the participant's native language Bulgarian/German and in English)

- Participants were then informed that transcription was started, and a few basic questions were asked to set them at ease and to verify any changes in behavior

- Near the end of the session, participants were informed that transcription was no longer being recorded, which was followed by a short discussion regarding their responses and or other people's experience in relation to the questions such as family members or friends. The change to more informal discussion allowed for people to feel more at ease and discuss some corrections that they would give to their responses

Additionally, the spouse of one of the subjects was present at one of the interviews and a separate discussion was carried out to verify the observable differences in the subjects' responses. Since the only way to investigate this topic un-intrusively is to question people about their experiences directly this interview structure allows compensating for some of the deficiencies of such an approach (Bogaard, Colwell and Crans, 2019). This allows for weighing other participants' behavior and responses to what would be observable reality. This also allows accounting for other deficiencies in the data collection which is nonetheless necessitated by the nature of the research. These drawbacks include the possible unreliability of individuals' self-assessment (Yu, 2013), or the vagueness of responses based on personal experience (Philipps and Mrowczynski, 2019)

This was one of the first interviews to be carried out so that any potential issues would be factored into the questions, follow-ups, and general structure of the other interviews. The responses of the interview can be separated into verbal (verbatim in the transcript) and nonverbal data (body language, hesitation in response, filler words, etc.). Reading through the transcript of the verbal data would indicate a high level of compliance and awareness of

corporate security practices. The nonverbal cues – hesitation, non-comital or quiet responses indicated points of interest that could then be followed upon. When verifying the reliability of the interview with the observer only minor variations were encountered. The raised concerns from the non-verbal points of interest were elaborated as either uncertainty about whether a specific action would constitute a breach of security practices or a knowing breach that is of minor significance. The examples presented were:

- Not knowing if this constitutes a breach of data security policies – asking a spouse to help with a technical issue on the corporate laptop that encountered an error that made it impossible to rely on a remote IT team to resolve it.
- Minor infractions – sometimes not locking the laptop at home when leaving it, or showing internal company documents to their spouse, which would not be considered privileged information

Nonverbal cues from other participants, where present, were all in the same categories, so responses from them are considered to be in the same failure of compliance categories. This is corroborated by the few participants in positions of authority and visibility over multiple remote workers. These individuals reported that technical issues, in particular, were present amongst multiple people in the first few days or weeks after the lockdowns and the corporation's focus was on getting their environment to be capable of supporting remote work thus leaving the potential issue unaddressed.

3.5 Data Analysis

In ICT-related research, the common analytical models rely on forming themes from the data with either the 3 Cs approach (Lichtman, 2013) or the 6 steps thematic approach (Braun and Clarke, 2006). While both of these are differentiated, the general premise is the same – codifying data to gather in themes/concepts and then refining those until a unified concept can be presented (fig 4.).

3 Cs	**3 Cs (step-by-step)**	**6-step Thematic analysis**
Codes	Initial coding (summary of responses)	Become familiar with the data
	Revisiting initial coding	Generate initial codes
Categories	Developing initial categories	Search for themes
	Modifying categories	Review themes
	Revisiting categories and sub-categories	Define themes
Concepts	Moving from categories to concepts	Write-up

Table 3: Analysis methodologies (Braun and Clarke, 2006, Lichtman 2013)

Of the two methods Thematic analysis is the more suitable for this research as 3C's method could be more easily influenced by the codified categories in the theoretical framework. Thematic analysis would also allow to compare and contrast individual elements based on country, occupation or familiarity with security practices.

3.6 Ethical considerations

Data collection for this research involves interviewing employees regarding their view on data practices and communication of said practices, as well as their self-perception on adhering to these security policies. As such the interviewees can be subject to scrutiny should the information divulged reach their employers. Ensuring the anonymity and privacy of the employees is paramount in order to protect them from any possible negative consequences, thus also ensuring the reliability of their answers. To achieve this a non-disclosure agreement was offered to participants, that neither side would discuss the interview and related questions and answers outside of the parameters of this research (Kaiser, 2009). The consent form for this can be found in the Appendix. Additionally, participants were given the option to withdraw their consent at any point and request their data and answers not be used for the purposes of this research. In the pursuit of participant anonymity direct quotations have been used as little as possible. This is necessitated by the use of participants roles and locations. Since these elements offer a structured contribution to the findings of the thesis, additional quotations contributed to a specific role or location could be considered as violating the NDA and rising participant privacy.

4. Empirical findings

This chapter outlines the findings of the conducted interviews grouped in a thematic analysis framework. This describes the timeline of the lockdowns and the general organization approach to moving to remote work and how it affected employees. Tendencies and themes are grouped wherever possible but outlier cases are also highlighted to allow for understanding the background of those scenarios and evaluation on their general application.

4.1 Codifying and categorizing the data

The following chapter outlines some of the initial codes and related quotes that serve to identify themes.

The first step in codifying the data was to pull responses from different roles to similar questions mostly based on the timeline of lockdowns:

Before the pandemic:

“We have a lot of edit identifications through phone ... every website or whatsoever our applications …for everything I need to identify”

“We have our typical trainings maybe every month or every two months”

“We deploy and use 2-factor authentication and VPN connection to VM’s, nothing huge”

“Not for general use, only when connecting to customer environments to be more cautious”

“We had our laptops from the company, and smartphones and we needed to use VPN”

“We only had smartphones to contact customer” “we got outlook so sometimes the VPN would cause issues with the credentials”

After the pandemic:

“We had a specific training for this as well. What we need to do when we are at home.”

Q: *Do you follow these instructions?*
“Not all of them”, “I cannot say that I'm strictly following all of this”

“You might need to tunnel in if you need something specific from the intranet, but a lot of the time it’s not necessary”

“I think that's because I'm as we as a consultancy company are used to working remotely doesn't matter if we work at home or at our customer sites. There are already mechanisms in place to increase our security”

Revisiting the codes and viewing through the lens of the role type revealed significant discrepancies in how individuals approach information security with the above-mentioned

findings being noticeably different between administrative, operational, and conceptual employees. Each level indicates more familiarity with security practices and risks from before the pandemic:

“We get standard security practices you know. We get training emails every 3 months or so and we do phishing campaigns.”

“In (interviewee’s country) we don’t have that many employees so it is not very relevant, but in (Other EU country), we had 10-15 people failing the tests, It should be less than 3%.”

“Passwords with rules for regular changing” “Active Directory accounts” and “something called ITHS card with 6-digit code to extend certifications across the entire public domain”

Overall, the data was still more timeline-based, and looking through that prism is more relevant for the theoretical framework of Habit Theory therefore that is the approach taken. The employee security awareness is a relevant theme but pre-established habits look to have more impact than actual role or country.

4.2 Grouping themes based on the experienced timeline and its impact on employee habits

4.2.1 Pre-pandemic environment

Detailed below are the employee experiences and habits before the pandemic as well as their view on security practices and communication.

The first and immediately observable pattern to emerge from the gathered data is the similarities in participants’ experience with lockdowns, move to remote work, adjustment, and return to the office. While people in different countries and roles experienced these events at different times because of the timing of local regulations, the timeline of these experiences has been universal for all participants. In order to evaluate how the lockdowns and the move to an entirely remote environment affected individual compliance and attitude, a baseline of the pre-pandemic environment has to be established. Participants were asked questions in that area to establish what they consider “normal”, and how they see their employer’s requirements compared to the average for their country in terms of security, remote work practices, and communication. Additionally, questions about their role are relevant to this section, to establish parallels between participants as well as country and general practices. To evaluate the factors on remote work eligibility data was gathered from people in IT roles or in IT-related companies (such as IT services or supply chain for IT). The roles that the participants occupied run the range from administrative – shift planning and process management, through operational – system administration and support, to conceptual – solution design and technical consultancy. From the data it would appear that country, gender or role have little influence on whether an individual was able to work remotely pre-pandemic or not. This seems to be mostly related to the company and its preferences.

Most participants reported that they had the option of hybrid work before the pandemic, usually in a 40%-60% or 60%-40% split. The outliers in this regard are – participant 4, in an IT operational role who was required to be fully on site although the description of responsibilities did not seem to necessitate this and participant 2, in an IT conceptual role who

almost never needed to be on-site, but would instead work from a client site. These are noteworthy as they represent the extreme scenarios prior to the pandemic. In the period of lockdowns, participant 2 encountered no issues in the move to remote, while participant 4 had significant security-related issues that prevented normal day-to-day operations.

Before the pandemic hit most participants reported having to participate in yearly security awareness trainings. These are described as being standard video materials and/or slides with learning check sections that require the employee to answer 3-5 multiple-choice questions. The general length of these trainings would be around 15 to 30 minutes and information contained within would be the absolute minimum for security compliance – lock work station when away, if you have the availability to work remote pay attention to what connection you are using, do not leave your device unattended if in a public place, change the password frequently, etc. Additionally, most employees would get a mock phishing campaign or other emails related to information security on an infrequent basis to serve as a reminder.

Physical security for most employees was based on requiring ID to access the office and reminders to watch for "tailgating" (walking in behind someone who authorized their entry without using your authorization card). Participants who were working on customer-specific projects would be expected to follow additional security arrangements depending on the customer requirements. The most common of these arrangements would be to not be allowed to use or even have your personal mobile while at work. This is then enforced by the employer in different ways either using surveillance in the office and reporting individuals that used their mobile or by requiring employees to go through a turnstile that would be used to detect electronic devices. In both scenarios, the interviewees reported that some employees were still managing to take their mobile with them resulting in an estimated once-per-month breach of guidelines. These breaches would result in a warning to the employee with the risk of termination.

In terms of log-in credentials, use of software, and other tools most individuals encountered no issues. Password change protocols were standard across all companies with slight variations on how often it would need to be changed. Two-factor authentication was required by only some of the employers and was implemented in different ways. Individuals with more flexibility on work location or device had two-factor authentication while some others had physical authentication hardware bound to their corporate laptops. Using VPN's was highly encouraged and for some companies required in order to use any of the production tools employees needed to access especially when connecting from outside of the corporate office.

Attitude towards security practices is heavily dependent on how intrusive individuals found them in their personal lives. When it comes to trainings, phishing campaigns, and password changes most individuals viewed these as normal. Although conceptual IT workers reported that they found these slightly redundant, as their experience and recent research they have read indicates that specific password requirements and change intervals only lead to people writing down their passwords in unsecured locations or using the same password with only minor variations over and over again thereby invalidating the usefulness of the mandatory changes. Meanwhile, intrusive requirements such as the ban of mobiles in the workplace caused significant disgruntlement of employees and often non-compliance. In these scenarios the reported employee issues were:

- going against the habit of always being connected
- creating stress because you would be unreachable in case of emergency (one participant was expecting a baby and could not accept being unreachable at any point of time)

- the reasoning behind the policy and reasoning for compliance not being explained by the employer

In these scenarios, compliance can be viewed both through the lens of habit and motivational theory as a significant contributor towards non-compliance, but can also be viewed from the facet of stress theory where events in an individual's life could instantly create serious risks for compliance as viewed by the company.

4.2.2 Lockdowns and move to remote work

The following section covers the initial employee experiences with lockdowns, the challenges they faced and how they view their company's response to the change in work environment.

For the different countries and cities, the lockdowns where people had to move to a remote environment happened at different time frames with up to several months' differentiation. Levels of lockdowns were also different across countries with some individuals experiencing strict closures for at least a several-week period and some only public health guidelines and recommendations. Irrelevant of when or where exactly the individuals were located all companies elected or were forced to go to a fully remote workforce in an extremely short notice (people were usually told one or two days before that they will need to work from home). Organizations and individuals were operating in conditions of significant personal stress and uncertainty. All participants reported at the time organizational focus was primarily on personal health and safety as well as compliance with hastily passed government regulations with secondary concerns being the ability to actually conduct operations in a distributed manner. With all employees working from home the questions and concerns of security were not present immediately on the move to work from home, and the initial topics around security were usually raised by employees facing issues interfacing with some of their organization's systems.

Despite the similarities in how lockdowns were communicated and conducted across organizations and countries employees had significant differences in experience with the move to remote work. For employees in organizations that allowed remote work prior to the lockdowns, the transition was fairly smooth. In the initial days some faced issues with connectivity, authentication, and utilizing teleconferencing tools (Zoom, MS Teams, etc). These issues seem to have been universal but also not systemic as no two accounts relayed any specific issue, but rather individual instances of issues. These were, for example, connecting to a specific internal document or tool or conducting larger-scale team meetings entirely virtually.

This is the point at which some participants infringed on corporate guidelines when asking their spouses to help troubleshoot a technical issue. The participants in leadership roles, and IT operational roles indicated that the companies were at least somewhat aware of this, but no one reported the company raising immediate objections to this (some companies provided guidelines for such scenarios in the following months). Almost all of the interviewees reported they encountered some issues in the transition to remote work, other than changing habits and adjusting to the environment. Some of these events can be viewed as systematic as they happened to multiple individuals while others were entirely specific to the participant and their role.

Participants in IT operational roles reported an increase in workload at the beginning of the lockdowns. This was mostly related to helping individuals with troubleshooting authentication or technical problems. On top of this systematic issue, one of the participants

was in a fully office-based role which added issues to the move to remote. The organization was entirely unprepared to facilitate remote work which resulted in significant issues in the beginning few days – not possible to access systems remotely and no authentication available whatsoever. The particular organization is a hospital system that handles patient data; hence data privacy was a significant issue. Remote connectivity was possible after the first week of remote work and full access to all the tools to the point where remote workflow could be equated to the in-office operations took six to eight weeks. During this timeframe, no changes to security policy were made or communicated and the organization did not compromise on its security practices.

The second systematic scenario in the move to remote is related to participants who work on customer projects, more specifically those who before the lockdown were not allowed to have their mobile devices with them in the workplace. These individuals reported that even before the lockdowns when home office work was possible it was highly regulated and monitored, usually requiring specific reasoning to be authorized. Once lockdowns went into effect, the move to entirely remote work the companies amended the login policies to require two-factor authentication at all times to verify the users. While this was required for most of the other participants as well it is noteworthy here as these individuals were both required to use their phones for two-factor authentication and not allowed to have their phones with them at their work desks. This caused some discontent enhanced by the fact that the company had unclear communication on the guidelines and this was further exacerbated in the return to the office and two-factor authentication guidelines that were communicated at that point.

Providing a slight insight into the organizational view of the transition, one of the participants was responsible for deploying a national-level website for facilitating educational activities as part of a government agency. In this scenario, the participant was the one responsible for creating and configuring the security policies for the remote environment, with all of the activities related to the website (concept, programming, and deployment) having to be executed in a 48-hour timeframe. When discussing the project requirements, the organization communicated the following prioritization:

- Deployment deadline - website and required functionalities need to be available by 8AM Monday
- Security and privacy – concerns were discussed but were secondary to the functionality
- Costs – when incurred about the budget for the tasks the organization dismissed the topic as irrelevant as the only focus should be on delivering the functionality in time

4.2.3 Working from home

The so-called "new normal". This chapter shows how employee behavior changed and what participants observed as new routines and habits started to settle after the shock of the change in environment wore off.

After the initial challenges of moving to an entirely remote workforce, most participants reported that it took them about a month to get comfortable with their new daily routine. Almost all people reported having later starts to the day, with interruptions throughout related to household tasks and family members. This in turn resulted in most of them being unable to separate work time and personal time. When following up on this most participants reported

that after several months, they had to make a conscious effort to "disconnect" from work after their workday was concluded thus allowing them to separate work and personal life.

In the interim, most participants reported that they observed similar trends among their colleagues. The process of this blending and separation of work and personal life was observed in several different stages. The first few weeks after lockdowns people would join conference calls fully dressed in their office clothes, position themselves somewhere with a neutral background (blank wall usually), and would communicate in a very professional manner. After about a month, participants observed that people were mostly joining calls in their home clothes, in different locations of their house, and often with family members moving in the background. Some participants even noted that family members noticing that they were in the frame might approach "to say hello to people in the call" or even participate in some small talk. After several months most people reported noticing an increase of conference calls where other people would not have their camera turned on, or if so, they would use the blurred background (or other background) functionality with discussions being mostly professional and work-related but without the "stiff professionalism" of the first few weeks of lockdowns.

This blending of personal and professional environments was not limited to conference calls. When asked most participants admitted they have had increased discussions about their work with their spouse or live-in partner. Some participants claimed that while work-related conversations were increased, they were mostly related to discussing when specific meetings would take place so that they would not be disturbed, or if they had a deadline or high workload that they needed to manage so that they can balance housekeeping responsibilities with their partner.

On the other hand, some participants admitted having increased discussions at home for specific work-related topics. Initially participants denied these discussions covering sensitive topics or anything that would be considered privileged information, but body language indicated those responses were unreliable. Before following up on this gradient of information security was discussed with participants. Most interviewees reported having a tiered information security policy with three of five tiers of information security policy:

Figure 2: Information classification (left-to-right from less to more protected information)

Not all organizations had all of the same distinctions but the general distinctions were mostly present, with publicly available information being anything in the company that does not discuss customer specifics, financial results or is not otherwise marked as privileged information. Internal and private communication would either be labeled as such or would be related to customer, team or financial items that must not be shared outside of the company. Confidential information would always be clearly labeled and its sharing and distribution would be covered by contractual clauses with employees. Secret or "strictly confidential" information was only encountered in participants working with/for government entities where the information distribution would be restricted by law.

Following up with participants on those outlined distinctions and their adherence, at least half of the participants agreed they often shared internal information with their partners or friends with the volume increasing since the move to remote work. Some participants agreed that they occasionally discuss private information with their spouses such as specific processes or projects. This was mostly in a function of "bouncing ideas off someone" where they reported the information shared would be considered privileged information but

considered the context and manner of information sharing not a risk to the company information security.

Secret information was available to only a few participants in relation to patient information or student record databases and these individuals were concise and clear that this was not discussed with anyone external and would even have limited internal discussions. Body language and non-verbal cues do not indicate inconsistencies in those statements.

Confidential information was most noteworthy, as there were exceptions to the rule. Most participants would not share this type of information and reported that distribution and discussion of this type of information in the company itself were limited. The two exceptions of this were the individuals working on customer projects. As part of their contracts, these employees had signed non-disclosure agreements that prohibited them from discussing who the end customer of their company is, what they do in their day-to-day work or any work-related topics with anyone outside of the company. Both participants who were in this type of scenario worked for different companies and different end customers but had similar clauses in their contracts to cover this type of information. Similarly, both participants shared that they have discussed information that is covered under these clauses with their family or friends, and depending on their exact work function might share this type of information on a daily/weekly basis.

For authentication, document, and device security all individuals reported that after the intimal scramble companies established a fixed policy and made efforts to clearly communicate the policy – for all companies this would be to use two-factor authentications, and most also required the use of a corporate VPN. Most organizations took additional steps to communicate the risks from unsecured connections and to conduct more frequent phishing campaigns to make sure employees are vigilant. One of the participants in an IT operational role disclosed responsibility for carrying out such campaigns and the organizational view on the matter. With the increased normalization of home office work and the work-life balance blending work and personal time, the company wanted to ensure employees are vigilant and established an ongoing phishing campaign with individuals being selected at random on a weekly basis to receive mock emails, and each employee receiving a minimum of one fake email per quarter. Comparative to the pre-lockdown campaign there was an increase in people not catching the phishing attempt and clicking on links in the email, with those most noticeable in the initial months of lockdowns followed by a return to the normal trend.

4.2.4 Return to office

Employees view on some company's efforts to return to office work as well as the frustrations and gaps in communication that this raised for some employees

---

At the moment of performing the research for this thesis, some participants reported that their organizations have begun to change policy and request for individuals to return to some sort of hybrid work. Most participants reported organizations are looking to bring people back in a 40% office to 60% home split, including employees who had limited or no availability for work from home prior to the pandemic. This is being carried out gradually with no huge changes in security or access. Some participants commented that they would require an adjusting period and expressed worries about possibly forgetting to lock their computer when moving away from their desk, or leaving their device unsecured and unattended. With the limited nature of the return policy no one has reported any actual issues or significant changes in terms of data security.

The individuals that reported they have to use two-factor authentication but are also not allowed to use their mobiles in their workspace confirmed that in the return to the office this has remained the company policy. This has caused significant annoyance to themselves and their colleagues as it appears to them that the security policy is inconsistent and the requirement appears arbitrary. Noteworthy is that these are the same companies that have the highest levels of noncompliance when it comes to sharing confidential information.

4.2.5 Global events affecting security

When inquired about specific global events outside of the pandemic and lockdowns that could affect security, responses varied on several parameters. The line of questioning related to hardware and software-specific vulnerabilities were focused on the December 2021 announcement of the JAVA log4j library vulnerability. Since JAVA applications are widespread and the specific library was a very common tool. Additional vulnerabilities discussed were the Intel processor cash vulnerabilities announced at the start of the year which affected specific combinations of processors and firmware. As can be expected responses and awareness were heavily dependent on the participant's role:

Administrative and support	IT operational	IT conceptual
Administrative and support functions were not aware of any vulnerabilities	Participants in these roles were aware of the news of major vulnerabilities but only needed to act if their organization determined it was affected by the issues and received guidelines on how to proceed	Individuals in these roles were fully aware of vulnerabilities as they happened, checked systems, and created update and distribution plans to mitigate risk

In terms of communication of such vulnerabilities the sources were also different based on the roles. Administrative functions did not receive any communication and because of their limited IT knowledge it is unclear whether they would have been impacted directly. The nature of the vulnerability makes that unlikely. IT operational roles received limited communication only if they needed to deploy changes to their environments. Conceptual roles received the information from the news/personal research before it was introduced to their organization with Participant 2 only noting that the environment, they currently work on is not impacted. Participant 6 reviewed potentially impacted systems and created information packages for their organization.

The other line of questioning related to global events was the Russian invasion of Ukraine since Russia is widely accepted to be one of the major originators of state sponsored hacking activities. In this scenario all functions were aware of the event and were to some extent aware of the increased risk to their online environment. People across most organizations received mails reiterating the importance of following security practices and being watchful for phishing attempts. The people in people leadership roles received additional notifications and were required to participate in frequent meetings to discuss the increased risk and ensure their teams are aware.

4.3 Relating empirical findings to the elements of the theoretical framework

Cue:
People focused on prompts such as emails or direct communication from managers, but compliance was not consistently affected. Participants reported disregard for compliance when the cues became too obtrusive.

Routine:
Participants whose companies were more prepared to move to a hybrid or remote model were less severely impacted by the move but reported the same adjustment period.

Reward:
Positive rewards seem to have had significantly higher impact on compliance across all participants, specifically ease of use. Negative rewards vary between security involvement levels – mostly dependent on whether the employee would be directly involved in any consequences from a security breach.

Moderating Factors:
The most significant moderating factor across all participants is job role and how directly the role is linked to technology and security.

Attitudes:
Attitude change has mostly been based on the pandemic's impact on a person's routine. Overall compliance and security have been more of an afterthought for some companies and with the drastic change – impacted employees more severely.

Subjective Norms:
Through the interviewed individuals' subjective norms have been tightly linked to a person's role so moderating factors is more heavily considered when analyzing the data

Perceived Behavioral Control:
Behavioral control is dependent on the routine, reward and subjective norms of the participants which makes it mostly varied even between instances of the same participant.

5. Discussion

This chapter contains the inferences that can be made from the data gathered when viewed through the established theoretical framing of Habit theory (Motivational and Coping Theory) as well as the specific instances that are framed by Normative theory. The discussion is divided based on the research questions. How communication regarding security changed, what was the impact and changes in compliance and how did this in turn affected employee attitude.

5.1 RQ1 - Changes in the communication of security practices

All participants, when directly asked if they have observed any changes in communication, claimed that they have observed no changes. Aside from the scramble and confusion in the immediate aftermath of the move to work from home companies have retained consistent messaging related to data security and communication consisting of periodic virtual trainings (usually annually or bi-annually) with some form of phishing campaigns or communication. People in leadership roles reported receiving regular communication in relation to global vulnerability or threat events where these could affect their team but those were related to the specific events and not work from home specifically.

This, however, along with other participant comments related to specifics around phishing campaigns, authentication procedures and other security policies indicate that organizational communication regarding security was much more frequent than participants were consciously aware of. On top of this, the participants that were in roles responsible for executing phishing campaigns or deploying new features to their organization observed that with the move to remote organizations were aware of the possibility of increased vulnerability and increased frequency of phishing campaigns as well as communicating security reminders when deploying new tools or features. This is consistent with existing theoretical modeling and can be expected to result in increase in compliance (Safa and Von Solms, 2016).

This organizational adaptation allowed organizations to continuously re-iterate the security policies and monitor at least somewhat the compliance in a format that was non-intrusive to the employees, again in adherence to existing theory that aims to reduce factors that can prompt non-compliance (Hwang and Cha, 2018). From the lens of Motivational theory, this is seemingly incredibly prudent by organizations as regular and non-intrusive communication strives to retain the security habits of the employees and relies on self-efficacy. The higher volume of communication that people leaders reported can also be attributed to Motivational theory best practice as the second-highest contributor to compliance is threat awareness. Cascading the information in this manner allows for the team leads to communicate the information directly to employees ensuring awareness. The remaining participants in the study did not communicate receiving any such information indicating not all organizations have adopted existing research and as standard practice and some factors that would significantly impact compliance were not properly communicated to all employees (Godlove, 2012).

This lack of threat communication was also observable in the initial weeks of lockdowns. Based on the accounts of some employee's, organizations were aware that a rapid shift to remote work can create vulnerabilities in their systems, or had to deploy new systems to accommodate the new work paradigm, but valued continuation of operations over security (although there is no direct evidence security was actually compromised). The role of corporate culture and organization, especially the attitude toward working from home before it was mandated by governments clearly had a significant role, especially in the first weeks of

the lockdowns where these types of companies had to restructure their entire cultural and operational model (Hu et al., 2012). The one organization that does not adhere to this trend was a hospital where patient data security is governed by law. While no direct data from the organization is available it is evident that the operation of the IT team was not deemed to impact the operation of the facility and trying to shorten the few weeks of difficult transition did not merit slackening of security standards.

The fact that this was not directly communicated to the employees directly did cause discontent, although in this particular scenario, employees could reason out the cause of the issues, and frustration was mitigated by understanding the root cause, and understanding that it is a short-term issue that is being addressed. Longer-term frustration was faced by employees in client-assigned roles where the requirements for authentication and mobile access were changing with no clarity on reasoning. These organizations moved to two-factor authentication while up to that point strictly enforcing a policy of no mobile phones allowed at the workstation. Individuals in these roles were also baffled by the fact that two-factor authentication was conducted not through specific apps but through a browser on the phone and viewed this as a vulnerability as the personal phones were not monitored or controlled by the organization. The same individuals also reported frequent changes (although usually minor) that would happen on an almost weekly basis that would need to be communicated in a team meeting. Aside from the two-factor authentication, these changes were frequently related to using and authenticating to specific production apps or no longer requiring them, causing frustrations amongst the employees of the constant changes and constant requirements for authentication as each app would require separate login credentials.

The lack of clear communication and frequent minor changes are clear contributors to the non-compliance to security compliance of these employees. The gathered data indicates frequent infractions to the requirement to not have the mobile phone when at the workstation since the return to the office. This is undoubtedly influenced by the fact that two-factor authentication and why the security policies are established in a manner that does not allow the employees to evaluate the risks of security breaches. Additionally, having worked from home and have had their mobiles always available as well as required created a specific "homeostasis" expectation in these employees (Tarafdar, Gupta and Turel, 2013). Compiled with the abundant scientific evidence of separation anxiety when people don't have access to their phones, this breach of policy is hardly surprising. The participants in these roles reported that these were still open topics as the return to office happened relatively soon, but a clear misunderstanding of the compliance contributors from these organizations is observable.

5.2 RQ2 – Changes in compliance and attitude in the move to remote work

5.3 Habit theory modeling of the data

Applying the findings of the interviews to the habit theory model and how each category has been impacted by the pandemic two elements need to be identified. Examining each category, and its relative impact on attitude and compliance allows to also explain the differences in perceived change in communication versus actual changes in communication. Where applicable differences between habit theory and protection motivation theory have been highlighted.

5.3.1 Threat appraisals

Vulnerability – Companies identified the increased risk to security in the move to remote work. This was addressed with an increased frequency of communication and monitoring as

well as changes in security practices the scope of these actions being linked to how prepared the given company was to move to a remote work setup. Considering this has a modest impact on employee's intention to comply it is understandable why many participants did not notice any changes.

Perceived severity – For companies that already offered hybrid working models the lockdowns were not related to any increases in risk. The response of the companies that were not prepared for the move depended on whether they perceived the risk of security breach outweighed the risk of stopping operations. This resulted in a mixed impact on employees along those lines with some employees not noticing many changes at the beginning of lockdowns, some not noticing changes but being aware of the increased risk with information security, and some not being able to do their job at a 100% for several weeks while their organization balanced the risks of operation and security. Considering this is one of the primary drivers to compliance it is also understandable why the employees that were impacted shared increased frustrations.

Rewards – Employees switched some of their communication about work-related topics from colleagues to family members. This was not perceived as having changes with vulnerability and severity was a consideration in terms of limiting some of the information shared. These types of discussions fill in the role of regular office communication. While this is a negative contributor to compliance and clearly is at odds with policies, it is unclear if/what risks are related to this type of communication. From the interviews, it seems organizations were aware at least to some level of this scenario but without specific research on organizations, it is unclear just how aware they were or why no communication on this was shared with employees. More recent research indicates that imposing penalties (negative rewards) for non-compliance can have an effect on compliance, although with diminishing returns and with no guarantee of compliance (Trinkle et al., 2021).

5.3.2 Coping appraisals

Response efficacy – Differentiation along response parameters is again linked with how prepared an organization was to move to remote work. The companies that did not have established practices around authentication procedures or limited phone usage especially faced issues. Employees were irate about the constant changes in policies, mostly for not understanding the relevance of many of the changes and how they contribute to security.

Self-efficacy – While this is the primary contributing factor to compliance it also does not seem to have had any impact on employee attitude. All participants reported that the security practices they were expected to follow were "normal" even if they did not understand them or found them excessive at times.

Response cost – Less prepared companies forced more frequent changes in policy. The increased volume caused issues with compliance and impacted the attitude of employees in these organizations as they reported sometimes not being sure what the late changes were. Based on the modeling this is a minor detractor to compliance. Based on emotional reaction during the interviews, this was one of the higher contribution factors to employee dissatisfaction and negative experience around security compliance.

These findings are mostly consistent with recent research in compliance especially with regards to response and self-efficacy. Response cost on the other side is at odds with resent

research which claims it has little to no effect on compliance (Mou et al., 2022). This likely stems from the difference in frameworks used as response cost viewed from Habit theory standpoint differs from response cost in the context of Protection motivation theory. This serves mostly to underline the lack of unified theoretical framing in the research field of security compliance.

6. Conclusion

This section contains the summary of discussed theory as well as shortened and explicit statements as answers to the posed research questions. The limitations of the research design, future research opportunities, and scientific contributions are also outlined below.

6.1 Conclusions

While this research does not offer insight into the organizational approach to secure communication and changing policies, it establishes that there is a clear link between company communication and attitude toward security in the event of dramatic changes in the working environment. Additionally, it is evident that companies whose communication and monitoring practices target specific contributing elements in Habit theory can expect better results in adherence to security practices and no impact on employee attitude. The lack of an organizational point of view however does not allow to determine if this tailoring of the messaging and monitoring is deliberate or coincidental. What has been able to be determined is the clear answers to the research questions posed:

RQ1: How has the move to remote work changed the way security practices are communicated?

While most participants especially in companies already offering the opportunity for remote work did not notice any changes, evidence shows that companies increased the frequency of communicating security information – mostly in the form of reminders and/or changes in policy, as well as increasing the monitoring of compliance via phishing campaigns. Recent research in this field shows conflicting data about deterrent and response efficacy depending on methodology used. This leaves some uncertainty in the tangible results and suggests that a more robust study in the area is necessary.

RQ2: How has the move impacted employees and their attitude towards security adherence?

The impact on employees has been heavily dependent on two primary factors. How prepared the organization was to transition to remote work and how aware employees were of the technical and other factors relating to information security. Employees in organizations that had non- or limited home-office capability before the pandemic all faced frustrations with changes in security. Of those employees, the ones in more IT-related roles had sufficient information to at least somewhat moderate those frustrations which were then eventually addressed by the organization.

6.2 Contribution

Considering the trends of the past 10-15 years for increased flexibility when it comes to the workplace it is surprising how unprepared and inflexible some companies have been to switch to remote work. The pandemic and the ensuing lockdowns left little choice to companies and that being – to choose continued operations remotely or closing/limiting their business. Faced with these options a few companies did chose to limit their business or at least continue operating without compromising security in any way which did cause significant issues with the workflow and employee satisfaction. These were exceptions rather than the rule as most organizations even if not prepared opted to continue in an entirely remote manner with varying degrees of initial success. How smooth the transition was mostly depended on how

prepared or familiar organizations were with a remote or hybrid model. Some employees even barely noticed a difference in their security, communication or day-to-day activities.

This research gives valuable insight for companies to understand not only what issues employees are raising in regard to compliance, but also what changes in communication can be carried out to increase compliance without having an impact on employee attitude and increasing "technostress". This correlation between company communication and employee attitudes can be further examined in detail and leveraged in order to increase compliance without impacting employees. Workers are the vector for security breaches in more than 1/3rd of cases, this research clearly shows that minimal organizational adjustments or clarity in policy and communication can relieve significant pressure from employees. The fact that this is also not related to any major investments in technology or services should make it a primary goal for companies that plan to continue operating in some sort of hybrid or remote model.

The abrupt nature of the shift and the examination through the lens of Habit Theory indicates both the durability of the framework as well as the inflexibility related to habits that can crop up in a fast-changing environment. It is evident that companies with a good understanding of the importance of habit theory and already established remote practice could easily and safely switch to remote work without having to halt their operations for security concerns. It is also evident that the enduring nature of employee habits caused an increase in divulging sensitive internal information.

6.3 Limitations and future research

The narrow topic of this research along with some of the circumstantial findings indicates significant future prospects in the area. Additionally, the inconsistent or outright conflicting findings of recent research indicated that there is significant room for foundational research in this area. Most significant gap is a consistent theoretical framework to information security compliance. There is also room for additional research in company structure and security compliance policy. Primary amongst these is the possibility for organizational changes and adaptations. Rather than looking at the impact and attitude of employees examining in detail the response and system put in place by organizations can provide the full picture of the impact the pandemic has had on companies and their approach to security. Also, relevant but only covered in a limited fashion is the correlation between individuals working on customer projects and their systematic non-compliance with secure information. This was out of scope for this research as there was no indication that attitudes or compliance changed with lockdowns or work from home, but the systemic nature of the issues presents a possible future avenue for research.

The nature of the research design and the reliance on individual self-reporting paired with face-to-face interviews also raises some questions regarding the reliability of the findings. Additional steps were taken to enhance the quality of the gathered data and ensure the validity of the research, but potential quantitative follow-up on this research taking into account the specific factor that has impacted employees the most can evaluate the most impactful factors to employees. Overall, the research provides valuable insight for organizations in areas in which they can focus to improve both their security and employee experience, as well as raise awareness of security issues that companies have been systematically unable to address.

References

Al-Yateem, N. (2012). The effect of interview recording on quality of data obtained: a methodological reflection. *Nurse Researcher*, [online] 19(4), pp.31–35. doi:10.7748/nr2012.07.19.4.31.c9222.

Bloom, N. (2020). *How working from home works out*. [online] Stanford Institute for Economic Policy Research (SIEPR). Available at: https://siepr.stanford.edu/publications/policy-brief/how-working-home-works-out [Accessed 4 Feb. 2022].

Bloom, N., Liang, J., Roberts, J. and Ying, Z.J. (2015). Does Working from Home Work? Evidence from a Chinese Experiment. *The Quarterly Journal of Economics*, [online] 130(1), pp.165–218. doi:10.1093/qje/qju032.

Bogaard, G., Colwell, K. and Crans, S. (2019). Using the Reality Interview improves the accuracy of the Criteria-Based Content Analysis and Reality Monitoring. *Applied Cognitive Psychology*, [online] 33(6), pp.1018–1031. doi:10.1002/acp.3537.

Braun, V. and Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, [online] 3(2), pp.77–101. doi:10.1191/1478088706qp063oa.

Creswell, J.W. and Creswell, J.D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, California: Sage Publications, Inc.

Cuganesan, S., Steele, C. and Hart, A. (2017). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology*, [online] 37(1), pp.50–65. doi:10.1080/0144929x.2017.1397193.

Gibbs, J.P. (1975). *Crime, punishment and deterrence*. New York Elsevier.

Godlove, T. (2012). Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines. *Information Security Journal: A Global Perspective*, [online] 21(4), pp.216–229. doi:10.1080/19393555.2012.668747.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational

Culture*. *Decision Sciences*, [online] 43(4), pp.615–660. doi:10.1111/j.1540-5915.2012.00361.x.

Hwang, I. and Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, [online] 81, pp.282–293. doi:10.1016/j.chb.2017.12.022.

Icek Ajzen (1985). *From intentions to actions : a theory of planned behavior*. S.L.: S.N.

Justice, S.B., Bang, A., Lundgren, H., Marsick, V.J., Poell, R.F. and Yorks, L. (2019). Operationalizing reflection in experience-based workplace learning: a hybrid approach. *Human Resource Development International*, [online] 23(1), pp.66–87. doi:10.1080/13678868.2019.1621250.

Kaiser, K. (2009). Protecting Respondent Confidentiality in Qualitative Research. *Qualitative Health Research*, 19(11), pp.1632–1641. doi:https://doi.org/10.1177/1049732309350879.

Kane, G. (2019). The Technology Fallacy. *Research-Technology Management*, [online] 62(6), pp.44–49. doi:10.1080/08956308.2019.1661079.

Kuppusamy, P., Samy, G.N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. and Perumal, S. (2020). Systematic Literature Review of Information Security Compliance Behaviour Theories. *Journal of Physics: Conference Series*, 1551, p.012005. doi:10.1088/1742-6596/1551/1/012005.

Lee, W.J. and Hwang, I. (2021). Sustainable Information Security Behavior Management: An Empirical Approach for the Causes of Employees' Voice Behavior. *Sustainability*, [online] 13(11), p.6077. doi:10.3390/su13116077.

Levy, Y. and J. Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline*, [online] 9, pp.181–212. doi:10.28945/479.

Lichtman, M. (2013). *Qualitative research in education : a user's guide*. Los Angeles ; London: Sage Publications.

Martyn Denscombe (2017). *The Good Research Guide for small-scale Social Research Projects*. 6th ed. London Open University Press.

Milasi, S., Fernandez-Macias, E. and Gonzalez-Vazquez, I. (2020). *Telework in the EU before and after the COVID-19: where we were, where we head to*. [online] *EC.Europa.EU*. European Comission Siance and knowladge service. Available at: https://ec.europa.eu/jrc/sites/default/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf [Accessed 3 Feb. 2022].

Myers, M.D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, [online] 21(2), p.241. doi:10.2307/249422.

Pham, H.C., Pham, D.D., Brennan, L. and Richardson, J. (2017). Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, [online] 21. doi:10.3127/ajis.v21i0.1321.

Philipps, A. and Mrowczynski, R. (2019). Getting more out of interviews. Understanding interviewees' accounts in relation to their frames of orientation. *Qualitative Research*, [online] 21(1), p.146879411986754. doi:10.1177/1468794119867548 p 59-75.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), pp.93–114. doi:10.1080/00223980.1975.9915803.

Safa, N.S. and Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, [online] 57, pp.442–451. doi:10.1016/j.chb.2015.12.037.

Schmidt, K. (2011). *Cooperative Work and Coordinative Practices*. London: Springer.

Schmidt, K. (2016). Computer-Supported Cooperative Work (CSCW). *The International Encyclopedia of Communication Theory and Philosophy*, [online] pp.1–4. doi:10.1002/9781118766804.wbiect144.

Siponen, M., Pahnila, S. and Mahmood, M.A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, [online] 43(2), pp.64–71. doi:10.1109/MC.2010.35.

Sohrabi Safa, N., Von Solms, R. and Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, [online] 56, pp.70–82. doi:10.1016/j.cose.2015.10.006.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, [online] 48(7), pp.296–302. doi:10.1016/j.im.2011.07.002.

Sykes, G.M. and Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, 22(6), pp.664–670. doi:10.2307/2089195.

Talib, S., Clarke, N.L. and Furnell, S.M. (2010). *An Analysis of Information Security Awareness within Home and Work Environments*. [online] IEEE Xplore. doi:10.1109/ARES.2010.27.

Tan, M.K.S., Goode, S. and Richardson, A. (2020). Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security. *Behaviour & Information Technology*, [online] pp.1–30. doi:10.1080/0144929x.2020.1734087.

Tarafdar, M., Gupta, A. and Turel, O. (2013). The dark side of information technology use. *Information Systems Journal*, [online] 23(3), pp.269–275. doi:10.1111/isj.12015.

Trinkle, B.S., Warkentin, M., Malimage, K. and Raddatz, N. (2021). High-Risk Deviant Decisions: Does Neutralization Still Play a Role? *Journal of the Association for Information Systems*, [online] 22(3), pp.797–826. doi:https://doi.org/10.17705/1jais.00680.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, [online] 24(1), pp.38–58. doi:10.1057/ejis.2013.27.

Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, [online] 49(3-4), pp.190–198. doi:10.1016/j.im.2012.04.002.

Willison, R. and Siponen, M. (2009). Overcoming the insider. *Communications of the ACM*, 52(9), p.133. doi:10.1145/1562164.1562198.

Wood, W. and Quinn, J.M. (2004). Habits and the Structure of Motivation in Everyday Life. *Social Motivation*, [online] pp.55–70. doi:10.1017/cbo9780511735066.006.

Yazdanmehr, A. and Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, [online] 92, pp.36–46. doi:10.1016/j.dss.2016.09.009.

Yu, C.-H. (2013). *Reliability of self-report data Do the subjects tell the truth?* [online] Available at: https://www.creative-wisdom.com/teaching/480/Reliability%20of%20self-report%20data.pdf [Accessed 23 Apr. 2022].

Appendix: Consent form

This informed consent form is for participants who we are invited to take part in the master thesis research, titled "**Compliance with corporate ICT security practices in work from home environment**".

I am Rosen Todorov, working on my master thesis for Linnaeus University. I am doing research on people's experience with information security in the move to remote work. I am going to give you information and invite you to be part of this research. Before you decide, you can talk to anyone you feel comfortable with about the research. If you chose to participate you are free to withdraw your consent at any time in which case the information you shared will be discarded and not used for the research.

The goal of this research is to investigate employees' attitude toward information security and compliance when moving from an in office to a home office environment so that companies can tailor their decision making and better prevent risks from information security gaps.

Your involvement will be limited to a 1-to-1 interview session. The discussion will be recorded and transcribed. The information shared in this interview will be only available to myself and my scientific supervisor to verify the quality and validity of the research. The information gathered will not be shared with 3rd parties. Information will be stored on a local drive to minimize the risks of it being accessed by an unauthorized entity.

The interview will be carried out through Zoom (or another video-conference app) and will take approximately 1 hour to be completed. The questions in the interview are not pre-written so the format will flow more like a discussion but there are pre-selected focus areas that will be covered. These involve the security policies of the company you work at – apps, practices, processes, etc. As well as how these policies are communicated and the impact on yourself.

You can request a copy of the data gathered from the interview and you can request to receive a copy of the final publication. If for any reason you feel you want to withdraw your consent you can. If you feel that your information is being misused or that I am not respecting your wishes to withdraw consent you may contact my scientific supervisor directly at "sarfraz.iqbal@lnu.se" or contact the university Administration.

Rosen Todorov

Signature _____

I have read the foregoing information, or it has been read to me. I have had the opportunity to ask questions about it and any questions I have been asked have been answered to my satisfaction. I consent voluntarily to be a participant in this study

Print Name of Participant_____

Signature of Participant _____
Date _____
Day/month/year

Appendix: Interview structure and questions

Small talk and introductions

Share a security anecdote before initiating recording to gauge how the participant responds while not being "on the record"

Environment context questions:

- Age
- Country
- General employment practices in the country and if the company differs from those. Length of service in the company and a description of the company (sector/rough structure/role within the company)
- Did you have the option to work from home before Covid – how often/connectivity/security-related questions

Questions to establish homeostasis:

What was your average day/week before moving to work from home?

- What kind of security systems did you have to engage within the office? (Physical/IT/proxy/two factor authentication or other) – how did engaging with these make you feel (was it smooth, was it frustrating, etc.)
  Here examples would be discussed to get a full picture
- How often was security communicated or discussed?
- Do you remember any examples?
- In the event of security discussions who were the interested parties (employees/managers/directors etc)

Did you use to discuss your work with your family/friends/roommate and to what extent?

- Sharing information, documents etc

Questions to evaluate stress from change of environment:

How did your average day change when you moved from home?

- In the beginning
- Did you get use to the new environment – how long did it take you
- After you adjusted

Have you noticed changes in security discussions?
Discuss examples: logging in, leaving laptop open, sharing sensitive information with Family/roommate/friends

Stress event questions:

- Did you change environments while working from home (room/house/city/country)?
- Were there times when you were working from home when you had to go back to the office?
- Log4j or other vulnerability events – were you aware of these, how were they communicated, and how do they impact you?

- Masking regulations/lockdowns/war in UA – Questions about related and unrelated to security events to gauge differentiation in responses

Small talk and closure

Stop recording and have a post-interview debrief in case the participants have comments on something they previously said “off the record”

Lnu.se

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/fakulteten-for-teknik