University of Westminster

Westminster Business School

MSc Digital Business

Research Project

Raising Cybersecurity Awareness in Small and Medium-sized Businesses in Norway

Martine Siggerud

August 2022

Word count: 12 233

Acknowledgement

This research project marks the final product of my master's degree in Digital Business at Westminster Business School. The project could not have been done without help from the people around me. First, I wish to express my gratitude to the nine respondents and their contributions to this research. Without your insightful participation, this project would not have existed.

I want to thank all my professors on this course and would especially like to extend my gratitude to my course leader and supervisor, Fefie Dotsika. Your insightful comments and recommendations have been helpful and valuable throughout writing my project.

Finally, I would like to thank my family and friends for their support and encouragement this year, especially my flatmate Rebekka. This year would not have been the same without you.

This year has gone by so fast, and I am thankful for all the knowledge and experience I have gained.

Martine Siggerud

London, 29.08.2022

Abstract

The rapid digitalisation and the Covid-19 pandemic have drastically increased the number of cyberattacks in Norway. One increasingly targeted group are small and medium-sized businesses because they are an easier target due to a lack of resources, and cybercriminals see them as a path to larger organisations. The most prominent cyber threat is phishing and ransomware attacks because they target the business's weakest link, the employees. Many cybersecurity breaches are due to employees' lack of knowledge and awareness. Employees are the first defence but also the weakest link and the biggest threat to cyberattacks. Previous research focuses on implementing various training programs to raise cybersecurity awareness in SMBs. However, as critical cybersecurity has become over the last few years, many SMB managers do not see themselves as a likely target. Therefore, they cannot justify the extent of resources to use.

This research aimed to understand how managers can raise cybersecurity awareness in SMBs in Norway. This research provides seven recommendations for SMB managers to raise awareness based on reviewed literature and a qualitative study. First, managers need to put cybersecurity on the agenda, build a security culture based on openness, and lead by example. Furthermore, they should consider implementing an engaging training programme in the context of the work for the employees and implement third-party services. Last, they must communicate, understand, and inform about the threats.

List of Contents

List of Tables

List of Figures

1.0 Introduction

1.1 Background

Norway is one of the leading digital nations in the world (Regjeringen, 2019). Society relies on digital technologies in critical functions, and more and more services are online. The Norwegian government explicitly points out in the national cybersecurity strategy that the nation has become increasingly vulnerable to cyber threats (ibid.). The Norwegian National Security Authority (NSM) states that more Norwegian businesses see cybersecurity as necessary; however, there is still a lack of action to protect their assets. Moreover, they say that digital risk should be on the agenda for management to increase awareness (NSM, 2021). Numbers from the Digital Economy and Society Index (2022) state that 77 per cent of small and medium-sized businesses (SMBs) in Norway have adopted digital technologies. The rapid digitalisation and the COVID-19 pandemic that forced everyone to become digital overnight have drastically increased the number of cyberattacks (Georgescu, 2021; Pollini et al., 2021; NSM, 2021).

Cybersecurity threats have increased for organisations of all sizes; however, SMBs are increasingly targeted because of a lack of resources to protect, and limit cyber exposure (Bada and Nurse, 2019; PWC, 2021). Moreover, many SMBs deliver services to larger organisations, making them a path to bigger organisations for cybercriminals (PWC, 2021; Benz and Chatterjee, 2020). Even though the number of cyberattacks have increased, many SMB managers do not see themselves as a target for cybercrime; they do not see the risk and therefore cannot justify the expense of resources to use on cybersecurity (Benz and Chatterjee, 2020). When the management does not believe it will happen to them, this sends signals to the bottom line. For reference, this research refers to Gartner's definition of SMBs as businesses with up to 999 employees (Gartner, 2022).

A significant proportion of cyberattacks are caused by employees' lack of knowledge and awareness (Alshaikh, 2020; Lahcen et al., 2020). Therefore, only relying on technology-based solutions is not enough to reduce the risk of cyberattacks (Bulgurcu et al., 2010). A common mistake is that cybersecurity only concerns the IT department (PWC, 2021); however, cybersecurity is everyone's responsibility. One needs a holistic approach, not only technical solutions, to stand against cyberattacks (Pollini et al., 2021). Employees are the first line of defence and should be a part of the solution, not the problem (Li et al., 2019; Pollini et al., 2020). One of the most prominent cyberattack techniques today is phishing. In phishing, cybercriminals infect links or attachments in emails with malicious malware to encrypt file systems and demand ransomware (Qabajeh et al., 2018; Georgescu, 2021; Budke and Enko, 2020).

One severe cyberattack in the history of Norway is the attack on Norsk Hydro (Microsoft, 2019). Even though Norsk Hydro is a big organisation, it is worth mentioning because they were completely open about the situation when they found out they were attacked. Three months before the hackers announced the attack and demanded ransom, an employee unknowingly opened an infected email from what seemed like a trusted source, which allowed the attackers to invade their IT infrastructure and plant the virus (ibid.). The result of an employee opening an infected email resulted in the company losing millions of dollars (ibid.). This incident is only one of many examples of cyberattacks happening through phishing in Norway in recent years, showing how critical it is for employees to have knowledge and awareness of cybersecurity.

Previous research on cybersecurity awareness in SMBs focuses on implementing different training programs (Arachchilage et al., 2016; van Haastrecht et al., 2021; Ghafir et al., 2018; Bada and Nurse, 2019). Everything from mobile game applications to seminars and courses. However, employees who do not work with IT security tend to forget the acquired knowledge after; thus, it does not suit the aspect of their work. Therefore, the managers' role in raising awareness is crucial. Raising cybersecurity awareness in day-to-day life is vital to reducing attacks. Managers must provide enough information about cybersecurity so that employees understand the severity.

1.2 Research Question, Aim, and Objectives

Based on the literature and managers' experience, this research aims to explore how managers can raise cybersecurity awareness in small and medium-sized businesses in Norway and provide further recommendations for managers in SMBs to raise awareness.

Research question:

The research question for this research is: “How can managers raise awareness of cybersecurity in SMBs in Norway?”

The research objectives for answering the research question are:

RO1: Review the cybersecurity threats facing SMBs and what previous research suggests for raising cybersecurity awareness in SMBs.

RO1a: Investigate theories for how managers can influence employees’ attitudes and follow security protocols.

RO2: Collect experiences and knowledge from managers in SMBs in Norway to explore their practices for cybersecurity in their businesses and what they recommend for raising cybersecurity awareness. Moreover, analyse the findings toward the literature.

RO3: Based on the literature and analysis of the manager’s experiences and recommendations, provide recommendations for how managers can raise cybersecurity awareness in SMBs in Norway.

1.3 Structure

Following the introduction, the research is structured with a chapter of relevant literature about cybersecurity awareness, including threats and challenges for SMBs, cybersecurity culture, the theory of planned behaviour and the psychological attachment theory, which are both frequently used in cybersecurity awareness research. Furthermore, the research methodology is explained in chapter three, followed by the data analysis process. The fourth chapter presents the findings from the research. Moreover, chapter five discusses the findings in relation to literature to finally provide recommendations for managers in SMBs to raise cybersecurity awareness. Lastly, chapter six presents the conclusion of the research, including limitations and further research.

2.0 Literature Review

This chapter provides an overview of the literature regarding cybersecurity awareness and what previous research suggests for raising cybersecurity awareness in SMBs. The chapter consists of recognized theories and literature to examine RO1 and RO1a to answer the research question further. First, the chapter examines the challenges and the most significant cyber threats facing SMBs: malware, DDoS, phishing, and ransomware. Furthermore, cybersecurity awareness training programs and their effect will be presented. Following, we will see the impact and importance of developing a cybersecurity culture, including the management's role and the importance of communication. Moreover, security awareness and behaviour, including the theory of planned behaviour and the psychological attachment theory.

2.1 Challenges and Threats

Cybersecurity assessments require cybersecurity experts and key personnel that SMBs often do not have (van Haastrecht et al., 2021). As many SMB employees tend to have many different responsibilities, it makes it challenging to create sophisticated IT processes (Norek et al., 2007). Therefore, SMBs should outsource IT and security to trusted software vendors to have a proper IT infrastructure and minimise the risk (Forbes, 2021). However, only relying on third-party software vendors is not enough to reduce the risks; it can also cause new risks. For example, the attack on the Microsoft Exchange server compromised many of their customers, also Norwegian businesses (Microsoft, 2021). The employees are the first line of defence, the weakest link, and the most significant threat in cybersecurity (Aigbefo et al., 2020; Ifinedo, 2012; Bulgurcu et al., 2010). Moreover, employees tend not to be aware of the potential threats information security incidents can bring (Li et al., 2019). As a result, SMBs are increasingly targeted due to a lack of knowledge and resources to prevent and face cybersecurity threats (van Haastrecht et al., 2021; Aigbefo et al., 2020).

Businesses can face internal and external cybersecurity threats (Armenia et al., 2021). Internal cyberattacks often come from employees with irrational behaviour and lack of job satisfaction triggered by frustration from the employee towards the organisation (Lachen et al., 2020). However, this research focuses on external cyberattacks and threats to the organisation, primarily through phishing.

2.1.1 Malware and DDoS

The most frequently encountered cyber threat is malware (Mutalib et al., 2021). Through phishing attacks, hackers plant malware to harm the infrastructure, computer, and network to disrupt the operation (ibid.). Malware threats are continuously evolving and changing with new tactics and techniques, making it vital for SMBs to be aware of the danger and put in measures as they are increasingly targeted due to new technologies. Moreover, malware is used in phishing attacks to plant ransomware (ibid.). The three main targets of cybersecurity attacks are confidentiality threats, integrity threats, and availability attacks. In confidentiality threats, the attacker target databases, and servers. Moreover, in integrity threats, hackers target financial data and damage the organisation’s image. Furthermore, in availability attacks, the attackers target distributed denial of service (DDOS) and physical destruction (Lachen et al., 2020).

As a result of the difficulty in identifying, DDoS attacks have increased (Donno et al., 2018). Recently, important private and public businesses in Norway were attacked by DDoS (Reuters, 2022; NSM, 2022). These attacks are powerful because hackers take advantage of the internet’s design and functionality, which is challenging to detect. DDoS attacks mimic traffic to the website to downgrade the server, locking people out (Odusami et al., 2020).

2.1.2 Phishing

One significant cyber threat is phishing. The Cisco Umbrella report from 2021 on cybersecurity threat trends shows that phishing is the most common threat for businesses. Phishing is an old but effective tactic, though it targets the weakest links, the employees (Cisco, 2021). It is one of the most common techniques to deliver malware to acquire personal and financial data (Georgescu, 2021; Baillon et al., 2019). Phishing attacks are when cyber criminals attempt to redirect to malicious websites from what can seem like trustworthy sources (Qabajeh et al., 2018). Ninety-six per cent of phishing attacks come through email, and 67,5 per cent of those who click on a phishing link is likely to give sensitive information on a malicious website (Cisco, 2021).

Moreover, one technique of phishing used to gain access to businesses is spear phishing. In spear phishing, the attackers send an email, pretending to be from a trustworthy source, often the manager, to target the company's computer system (Qabajeh et al., 2018). Phishing emails often contain a link or an attachment; when someone clicks on the link, one gets redirected to another website. When the employees attempt to log in, the credentials transfer to another server which gives the hackers access to use these credentials to log in to the organisation's servers and plant malware or trojans (Qabajeh et al., 2018, p46; Weaver et al., 2021).

Many automated anti-phishing tools and software systems prevent phishing attacks (Weaver et al., 2021). However, these attacks are constantly changing (Qabajeh et al., 2018; Georgescu, 2021), which makes it essential to increase employee awareness and knowledge. Furthermore, since the attacks are constantly changing, phishing software and tools cannot detect everything. The final decision on whether an email is safe lies with the user, the employees (Weaver et al., 2021).

2.1.3 Ransomware

Ransomware is one of the worst cyberattacks that can happen to an SMB, and the threat has increased drastically after and during the COVID-19 pandemic (Georgescu, 2021). Malware through phishing emails is one of the leading causes of ransomware (Georgescu, 2021; Budke and Enko, 2020; Silva et al., 2019). Ransomware attacks have three phases: first, the infection of the virus. The second phase is when the attacker finds essential assets in the business, often sensitive data. Based on the severity of the sensitive data, the attackers find and set an amount of estimated ransom (Georgescu, 2021). The third phase is where the attackers launch the attack. Unfortunately, it can take time between the last two steps. In some cases, businesses do not know they are under attack until they cannot access their data or receive a message demanding payment (Budke and Enko, 2020).

Given the severity of ransomware attacks, businesses must take measures immediately to minimise the damage (Georgescu, 2021). The risks of a ransom attack are not only loss of money, but the attackers can also release the sensitive data they have gathered and therefore risk the business's reputation (Georgescu, 2021). And not least, SMBs often do not have the most resources, and an attack like this can end the company. Implementing antimalware software can help to detect the most common malware threats; however, these attacks change and evolve fast (Silva et al., 2019). As it is difficult to see these kinds of attacks, it is prevalent that employees receive training in detecting phishing emails (Budke and Enko, 2020).

2.2 Education and Training

It is vital to develop good security behaviour for employees in SMBs and build a cybersecurity culture to address issues and breaches in companies (Bada and Nurse, 2019). Cybersecurity knowledge and skills are the ability to handle digital threats using policy guidelines through education and awareness strategies for all employees (Bada and Nurse, 2019). Previous research suggests using training programs to increase employees' knowledge and awareness regarding cybersecurity (Arachchilage et al., 2016; van Haastrecht et al., 2021; Ghafir et al., 2018; Bada and Nurse, 2019). For example, Arachchilage et al. (2016) proposed a mobile game application tool to increase awareness and educate computer users. Moreover, there are online courses, for example, SANS' cyber security courses, where employees go through an assessment to recognise phishing emails (Ghafir et al., 2018).

However, these training programs are often expensive and time-consuming. Therefore, Ghafir et al. (2018) propose a framework for a security awareness training programme that can help to understand the potential cyber threats and how to protect them, such as password security. Furthermore, van Haastrecht et al. (2021) propose that shared incident information is vital to prevent further cybersecurity incidents and can help to improve SMBs' cybersecurity. Moreover, they suggest the framework Malware Information Sharing Platform (MISP), which is a sharing platform for threat information (van Haastrecht et al., 2021). However, not all SMBs use these intelligent solutions to prevent attacks; therefore, it is crucial to increase awareness at the employee level.

Awareness training is vital for the employees; however, Ghafir et al. (2018) point out that after courses, most employees forget some of the knowledge they acquired about security awareness. Therefore, these cybersecurity awareness training programmes must suit the organisation and be designed for the context of the business and relevant to its culture (Bada and Nurse, 2019). As most employees receive many emails every day, having training directed to their emails might be beneficial. Baillon et al. (2019) had an experiment where they tested the effect of simulated experiences to reduce the risks of phishing emails. The study was to see how receiving simulated phishing emails would affect employees. The experiment revealed that with personal experience, the subjects saw that they could be future victims and threats more probable (Baillon et al., 2019). Moreover, the experience increased employees perceived risk.

2.3 Cybersecurity Culture

In order to increase cybersecurity awareness in organisations, it is vital to have a sound cybersecurity culture. Cybersecurity culture can be described as the behaviour of humans in organisations to protect information through understanding how to implement requirements and information security policies through training, awareness, and education (Alshaikh, 2020, p1). In addition, influential cybersecurity culture is essential for preventing cybersecurity breaches caused by employee ignorance and lack of knowledge (Alshaikh, 2020).

There are different factors organisations should focus on to develop a sound cybersecurity culture. In Uchendu et al.’s (2021) literature research on cybersecurity culture and elements that are crucial to implementing to achieve this, the most prominent factor is the leadership and support from the management team. Furthermore, the security policy and security awareness and training. Developing a cybersecurity culture starts by formulating policies that guide employees on how to react in different situations (Ioannou et al., 2019). The guidelines must be well-developed, have a clear description of potential threats, and have available measures on how to react (ibid.).

2.3.1 Management

There are different reasons why management is essential in developing a sound cybersecurity culture. The managers are responsible for providing enough resources and ensuring that the resources are managed correctly (Uchendu et al., 2021). Moreover, the management needs to ensure that cybersecurity has the attention it requires, as employees often do not tend to focus on cybersecurity in their day-to-day work (ibid.). At SMBs, all the people working must have some knowledge and awareness since they often do not have departments regarding this. Therefore, the management must aim to develop a trust-based culture. A culture based on trust and communication can reduce employees' resistance and uncertainty and lead to an openness to change (Zainab, 2021).

2.3.1.1 Communication

Communication is crucial in every business context, especially regarding cybersecurity. Communication is vital in the cybersecurity culture because it can determine if the policies are perceived as laws the employees must follow or if the culture is for the business's greater good (Ioannou et al., 2019). The main goal of communication is to transfer the goals, where one must understand the business environment, commitment, belonging, and awareness (Ioannou et al., 2019; Welch and Jackson, 2007). Communication makes employees feel a sense of belonging, and commitment focuses on day-to-day management communication (Welch and Jackson, 2007). Feeling a sense of belonging will increase awareness, and employees get influenced to follow the security protocols of the business. Moreover, seeking transparent communication is vital for internal communication in businesses. Being open and communicating openly with the employees will provide trust between employees and the management (Zainab, 2021).

2.4 Security Awareness and Behaviour

Cybersecurity threats have increased drastically in Norway over the last decades; with more technologies emerging and rapid digitalisation, having cybersecurity awareness is vital (Regjeringen, 2019). Cybersecurity is not only a technological issue but comprises human factors (Armenia et al., 2021). Security awareness is not training but focusing on security and allowing individuals to recognise security concerns and respond (Alruwaili, 2019). Moreover, security awareness is a state in which employees are aware of and preferably devoted to the security goals of their organisation (Bulgurcu et al., 2010). Employees gain security awareness from life experiences, if one has been a part of an attack, consequences of not complying with security rules, gaining information through training, workshops or reading about it (ibid.). Moreover, not only learning from personal experiences but sharing and talking about experiences from attacks happening to other businesses can increase awareness (Cisco, 2021).

Employees' cybersecurity behaviour gets influenced by their peers and previous experience (Li et al., 2019). The two most used theories for cybersecurity awareness are the Theory of Planned Behaviour and the Psychological Attachment Theory. The theory of planned behaviour argues that individuals' background can influence security behaviour, for example, one's demographic, experience, and knowledge (Bulgurcu et al., 2010). Moreover, the Psychological Attachment Theory is used to find strategies to influence employees' security behaviour and explains how individuals react and get influenced by others (Alshaikh and Adamson, 2021).

2.4.1 Theory of Planned Behaviour

The theory of planned behaviour (TPB) is one of the most used theories in research to identify and explain factors that affect people's security behaviour (Li et al., 2019; Bulgurcu et al., 2010). Ajzen (1991) introduced TPB, which has since become one of the most used theories for predicting humans' behaviour social and security behaviour (Ajzen, 2011). TPB explains employees' behaviour regarding their normative beliefs and how they comply with information security (Lebek et al., 2014; Aigbefo et al., 2020). TPB consist of three components: attitude, subjective norms, and perceived behavioural control (Ifinedo, 2012, p85).

2.4.1.1 Attitude

Attitude refers to the employee's beliefs and positive or negative feelings toward a specific behaviour (Ifinedo, 2012, p85; Bulgurcu et al., 2010). This research refers to the employee's attitude to cybersecurity. Employees with a positive attitude toward cybersecurity often comply and follow security protocols. Moreover, employees with a negative attitude tend not to comply and do not follow the organisation's security protocols (Aigbefo et al., 2020). When employees comply with security protocols, they consider the effort or cost of doing this and consider the benefit this would give them of complying (Bulgurcu et al., 2010), for example, doing the different training programs the business provides or changing the password regularly. On the other hand, if employees choose not to comply with the security protocols, they make an active choice and still consider the consequences (ibid.). The more costly and time it takes for employees to comply and perform security requirements, the less likely they are to follow this (Bulgurcu et al., 2010, p530). Bulgurcu et al.'s (2010) study indicate that their beliefs affect individuals' attitudes.

2.4.1.2 Subjective Norms and Perceived Behavioural Control

Subjective norms are employees' perceptions of what key personnel or other people that are important to them think about a behaviour (Ifinedo, 2012). Aigbefo et al. (2020) have studied the factors that influence the security behaviour of SME employees; their study shows that subjective norm influences the intention to comply with security. Employees get influenced by social relationships in the decisions to comply or not to comply with security procedures (Aigbefo et al., 2020; Lachen et al., 2020). However, their study also shows that employees who are not motivated enough to be aware of what others expect, do not comply with security behaviour intentions (Aigbefo et al., 2020).

Perceived behavioural control refers to the employee's perception of how easy or difficult it is to accomplish or facilitate a specific behaviour (Ifinedo, 2012). Moreover, it reflects the impact of personal capacities and perceived limits on intentions concerning the desired behaviour (Hagger and Chatzisarantis, 2005, p514). Perceived behaviour control has two components, controllability, and self-efficacy (Hagger and Chatzisarantis, 2005). Controllability refers to the extent people have access to the means to control their behaviour. Furthermore, self-efficacy refers to people's self-confidence in engaging in the behaviour and the capabilities and abilities to perform the behaviour (Hagger and Chatzisarantis, 2005, p517).

2.4.2 Psychological Attachment Theory

The Psychological Attachment Theory is another frequently used theory on people's behaviour in cybersecurity. To find strategies to influence employees' security behaviour, one should find out how individuals' psychological attachment is and how they react to different behaviour. Kelman's (1958) psychological attachment theory explains how individuals react and get influenced by others. Moreover, the theory can guide organisations on how employees get influenced by security-related behaviour (Alshaikh and Adamson, 2021) by analysing how communication and social influence affect attitudes in organisations (Kelman, 1985, p59). The psychological attachment theory has three concepts: the level of attitude change, the power of influencing and the condition for behaviour adoption (Alshaikh and Adamson, 2021). Moreover, attitude change has three processes: compliance, identification, and internalisation.

2.4.2.1 Compliance

Compliance is the lowest level of influence. Compliance is when individuals adopt a behaviour not because they believe in it but because they are expected to avoid punishment or receive a reward (Alshaikh and Adamson, 2021; Park and Chai, 2018). Here the managers in the organisation have the power to either reward or punish based on rules. Moreover, on the compliance level, managers monitor the behaviour of the employees, and the employees comply because they are monitored (Alshaikh and Adamson, 2021). The managers' attitude toward information security influences employees' compliance (Park and Chai, 2018). Therefore, managers must follow the policies themselves. However, studies have shown that punishing or rewarding employees regarding security policies does not impact the influence of getting employees to follow protocols (Cram et al., 2017; Park and Chai, 2018).

2.4.2.2 Identification and Internalisation

Identification happens when individuals adopt the behaviour and accept the influence because they want to establish a relationship with the manager or people they identify with, not because they believe in it (Alshaikh and Adamson, 2021). Moreover, individuals perceive an issue's importance and are willing to comply (Park and Chai, 2018). To reach this level of influence, one needs to establish a good and trusted relationship and environment (ibid.).

Internalisation is the highest level of influence. Internalisations occur when employees adopt the behaviour because they believe in it, and it is consistent with their values (Alshaikh and Adamson, 2021). As a result, the employees' and the organisations' values are aligned, and employees feel a sense of achievement, which again increases their intent to comply with security regulations (Park and Chai, 2018). It is argued that employee internalisation is essential for maintaining a sound organisational information security environment long term (Park and Chai, 2018). At this level of influence, the cybersecurity culture is well-maintained and implemented (Alshaikh and Adamson, 2021).

To reach internalisation, managers need to communicate in a way that is understood and relatable by the employees (Alshaikh and Adamson, 2021). To improve employees' awareness, the internalisation level of influence is essential. Internalisation leads to sustainable and continuous change in behaviour, and the employees' norms are consistent with the organisation (ibid.), which increases the organisation's information security.

2.5 Summary and Gap in the Literature

Employees and businesses tend to believe cybersecurity is the IT department's responsibility and implementing different software systems in the organisation can eliminate the risk (Bulgurcu et al., 2010; Bada and Nurse, 2019). However, most cyberattacks during the last years have come through phishing emails, making the employees the first line of defence. Employees are the weakest link and, therefore, an essential aspect of reducing the threats (Aigbefo et al., 2020; Ifinedo, 2012; Bulgurcu et al., 2010). Various research on cybersecurity awareness in SMB/Es focuses on implementing different training programs to increase awareness of cybersecurity (Arachchilage et al., 2016; van Haastrecht et al., 2021; Ghafir et al., 2018; Bada and Nurse, 2019).

Moreover, the literature focuses on the importance of developing a cybersecurity culture (Alshaikh, 2020; Ioannou et al., 2019) and provides different aspects that will affect cybersecurity awareness for the employees, how the culture is, what the management responsibilities are for implementing, and the importance of communicating the different cybersecurity protocols in the business. Furthermore, how one influences an employee's security behaviour and factors that affect the security behaviour through the psychological attachment theory and TPB.

The gap identified in the literature is how managers can increase cybersecurity awareness in SMBs based on their experiences. Moreover, how the management is aware and works with cybersecurity awareness and explore what they recommend for raising awareness for employees in the Norwegian context, though most SMBs in Norway have adopted digital technologies and are increasingly targeted for cyberattacks (DESI, 2022; Regjeringen, 2019). Therefore, this research will address the question: “How can managers raise awareness of cybersecurity in SMBs in Norway?”.

3.0 Research Methodology

This chapter presents the research design for the study. Firstly, the researchers' research philosophy, and the chosen approach, qualitative methodology, are explained, followed by how data has been collected and analysed. Lastly, the analysis is described with the coding process.

3.1 Research Philosophy

Research philosophy is the researchers' beliefs and assumptions on developing knowledge which underpins the choice of methodology, research strategy, and data collection (Saunders et al., 2019, p130). Saunders et al. (2019) argue that there are five philosophical research approaches in business and management research: critical realism, positivism, interpretivism, postmodernism, and pragmatism. In comparison to the positivism paradigm, which is based on realism and focuses on descriptive answers with no further in-depth knowledge, the interpretivism paradigm is more aware of the in-depth variables and human factors (Alharahsheh and Pius, 2020). This research and the researcher's philosophy are subjective interpretive, given that this study aims to gain managers' experiences and knowledge on how one can raise cybersecurity awareness.

The researcher's philosophy is subjective and interpretive because one wants to make sense of the meanings expressed by the study (Saunders et al., 2019, p179; Goldkuhl, 2012). In the interpretivism paradigm knowledge is socially constructed with information, values, and expert insight (Turyahikayo, 2021). Moreover, it is based on people's experiences and understanding to gain knowledge (ibid.). The interpretive paradigm enables the researcher to gain insight, knowledge, and understanding of how managers influence the organisational life regarding cybersecurity awareness using a smaller sample of in-depth interviews (Saunders et al., 2019, p141).

3.2 Qualitative Methodology

Choosing the suitable method for the research is vital. One needs to consider the research's aim, the data collection method, and the research philosophy. As this study wants to understand the participants' experiences and knowledge to build a richer theoretical perspective on the literature, the proper methodology for this research is qualitative (Saunders et al., 2019, p179). Compared to quantitative research, where one needs much data, qualitative research focuses on the richness of smaller samples of data in the form of words. Moreover, we want to know their experiences as managers in SMBs in Norway on how to increase cybersecurity awareness.

Furthermore, the strategy for this research is using grounded theory. The grounded theory provides new insights and generates new concepts (Charmaz and Thornberg, 2020; Corley, 2015). However, as grounded theory is the development of theory grounded in data, most researchers use an inductive approach. However, this research utilizes an abductive approach, moving between induction and deduction to gain insight into creating new concepts (Saunders et al., 2019, p206-209). In the next sub-chapters, the data collection method is described.

3.3 Data Collection

3.3.1 Interviews

The approach for this research is grounded theory, and the data collection method is interviewing. Interviews were conducted because they allowed to easily understand the respondents' feelings about the study and gain the managers' personal experiences and knowledge about the subject (Mwita, 2022; Chara and Neely, 2021). For this research, nine one-on-one, in-depth interviews were conducted. The interviews were online in Norwegian. The initial plan was to have the interviews in person; however, because of the timing and the informant's schedule, it was more convenient to do these online, as the informants could schedule a 1-hour meeting online more manageable. The interviews were conducted in the informants' mother tongue for them to elaborate and express their experiences and meanings without any language barriers.

Interviewing online has become more popular due to new technologies (Janghorban et al., 2014) and more prevalent after the COVID-19 pandemic. However, although interviewing face-to-face elaborates a more personal connection, conducting the interviews online provides similar authenticity as the in-person interviews as one can see the facial expressions (ibid.). Moreover, online interviews provide a safer environment, as the informants can choose the location (Jenner and Myers, 2019).

3.3.2 Sampling

The non-probability sampling method was used for this research. The non-probability method is primarily used in qualitative research as one focuses on smaller samples, examines real-life experiences, and does not make statistical inferences (Taherdoost, 2016). The snowball method was used to get in touch with the informants by asking people for recommendations to talk to for this research (Kirchherr and Charles, 2017). Moreover, the requirement for the informants was that they work in or have previous experience in management positions in SMBs in Norway.

Two respondents work with businesses at a national level to consult SMBs regarding cybersecurity as a speaking tool between the government and businesses. Moreover, all the respondents have or work in management positions in SMBs in Norway. Table 1 illustrates the positions and experiences of the respondents. The description of what the respondents work with is vague to keep them anonymous.

Table 1 Respondents

Respondents	Position and experience
R1	Consultant for cybersecurity at a national level.
R2	Consultant for cybersecurity at a national level.
R3	Senior cloud consultant, experience as a project manager for digitalisations projects.
R4	Work in IT operations and security
R5	CCO, commercial director
R6	Founder of the business acts as a strategic manager. Has previously worked as the general manager for the business.
R7	Finance, personnel, and head of administration.
R8	Chief operational officer.
R9	General manager.

3.3.3 Interview Guide

The most common data collection method for qualitative research is semi-structured interviews (Kallio et al., 2016). Hence, the interviews conducted for this study were semi-structured, allowing more flexibility than structured interviews and allowing the researcher to have follow-up questions for clarification and further elaboration about the subject (Mwita, 2022; Kallio et al., 2016). The follow-up questions were both pre-designed and spontaneous if needed.

The interview guide (Appendix 1) consists of 11 questions, with follow-up questions to get the respondents to elaborate and provide more details. The order of the questions is progressive. The first questions are designed to be more straightforward warm-up questions to start the interview to get to know the respondents and get insights into what they know about the cyber threats their businesses face (Krosnick, 2018, p264). Then, following more in-depth questions (Kallio et al., 2016). To get descriptive answers, open questions, like "How" and "What" was used to get more insights, letting the interviews take a natural part and allowing the respondents to answer in their own words and elaborate freely (Krosnick, 2018, p266; Kallio et al., 2016). The last questions were more reflective to get the respondents to summarise their meanings and recommendations. Lastly, the interview ended with allowing the respondents elaborate additional thoughts about the subject or provide more information they see as important.

Given that two respondents work towards businesses with cybersecurity as experts, the questions are directed in two ways. For example: "Which position in the business do you have? /What do you work with?", "How do you communicate with the employees regarding cybersecurity? /How should one communicate?". However, during the interviewing process, the researcher noted that framing more questions towards "What do you recommend?" regarding, for example, communication or training programs made the respondents critically elaborate on their opinions, which was the focus of this research. There was not conducted a pilot interview before the interviews; however, during the first interviews, the researcher changed some of the structure of the interview guide.

3.3.4 Validity and Reliability

To ensure the trustworthiness of the research, validity and reliability are essential (Morse et al., 2002). One factor for ensuring validity in the research is having the correct informants for the research (Hayashi Jr. et al., 2019). All informants have been or are in management positions in SMBs in Norway and have many years of experience in the field. The expert informants work with cybersecurity awareness daily. Moreover, the respondents were given the opportunity to be sent the transcribed interviews to see the accuracy (Saunders et al. 2019, p218). Another point of ensuring validity is triangulation. The literature gathered for the study, and the data collected combined will increase the understanding of the research and improve the results' reliability. Moreover, triangulation is used to avoid possible biases (Hayashi Jr. et al., 2019; Lub, 2015). Coding is also essential for ensuring validity and that the questions asked are answered (Linneberg, 2019).

Hayashi Jr. et al. (2019) point out reaching data saturation as a factor ensuring both validity and reliability in a study. Data saturation occurs when there are no new information or themes, and respondents provide similar stories relating to the research question (Constantinou et al., 2017; Charmaz and Thornberg, 2020; Hayashi Jr. et al., 2019). The interviews show that the manager's recommendations for raising awareness were the same factors. Given that the data sample is small, having more interviews could result in more general recommendations and findings; however, for this intended study, saturation was reached. Moreover, the researcher tries to be transparent during the research process to ensure the reliability of the study (Saunders et al., 2019, p214).

3.4 Ethical Consideration

Researchers must be aware of the ethical considerations during the whole project. One must ask oneself if the research is worthwhile, the risks, roles, and responsibilities of the research, and whom the research will benefit (Roth and von Unger, 2018). For business studies, the relationships with the respondents are the most sensitive (Ghauri et al., 2020). Preserving the anonymity of the respondents in the research is crucial, moreover being honest and allowing the respondents to withdraw from the study at any time (ibid.). To withhold the anonymity of the respondents, the researcher holds their identity and the business they work in confidential (Roth and von Unger, 2018), hence the description of the respondents in table 1.

Prior to the interviews, the respondents received a participant information sheet and consent form they needed to sign before the interview. (Appendix 2) The participant information sheet includes a description of the research, data collection method, and information about the interviews being recorded and transcribed. Moreover, it includes information about confidentiality, their right to withdraw from the study and the right not to answer questions. The signed consent forms are stored separate from the transcribed interviews and the report.

3.5 Data Analysis

To answer the research question for the research, experiences and knowledge was collected from managers in SMBs in Norway to explore their practices for cybersecurity in their businesses and what they recommend for raising cybersecurity awareness (RO2). During the interviews, all the informants answered all the questions; however, all the interviews did not have the same order of questions though the interviews were semi-structured and took a natural path as the respondents talked. The average duration of the interviews was 40 minutes. The interviews were conducted in June 2022. The respondents will be referenced with "R" following a number, for example, R4.

3.5.1 Transcribing

During the process of processing the data, the interviews were first transcribed. Transcription is essential in qualitative research as it makes it easier to pull out themes or keywords from the interviews (Parameswaran et al., 2019). In the first round of transcribing the interviews, the dictation function from Microsoft Word was used. The dictation function was used to speed up the process, following a second round of transcribing to check for spelling errors and add punctuation. The researcher did the transcribing to reduce errors (ibid.). Moreover, the data was transcribed directly as the respondents' meanings, and words were.

Furthermore, the next step of data handling was to read over the transcribed interviews again, and the parts of the interviews that were not relevant to the research were removed. Finally, the rest of the interviews directed to the research were highlighted and translated into English. Figure 1 illustrates a word cloud over the transcribed interviews.

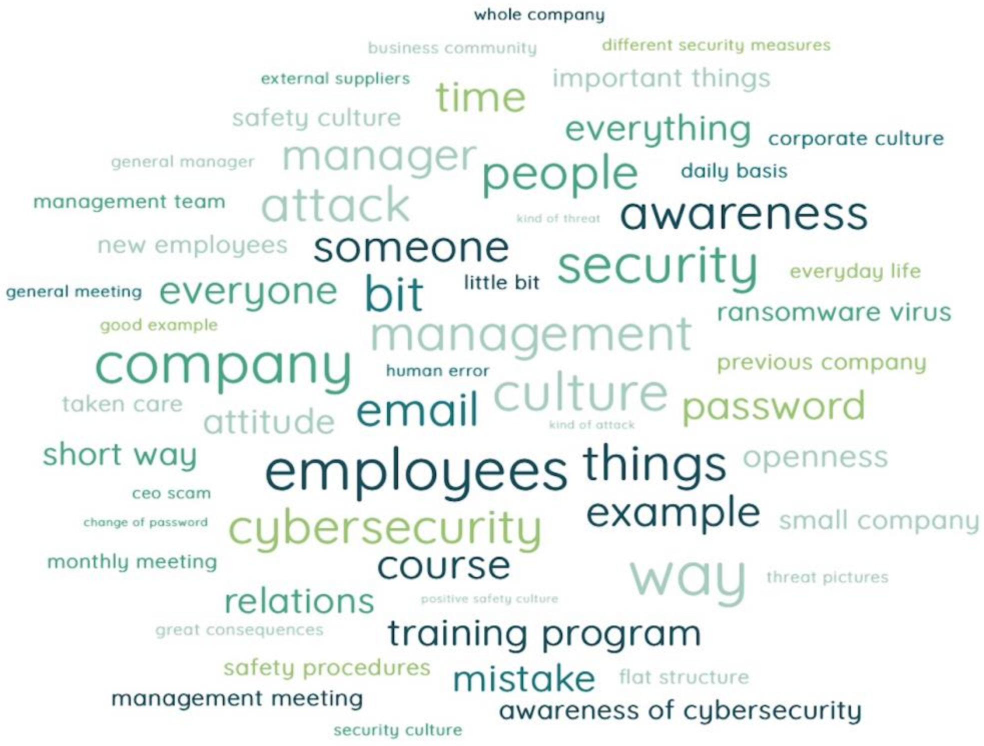


Figure 1 Word Cloud

(Source: MonkeyLearn.com)

3.5.2 Coding Process

The translated part was transferred into an excel file, where all the respondents' interviews were put on the same sheet in columns in the order of the interview guide. Furthermore, the interviews were coded to make the data accessible and retrievable for analysis and to acquire comprehensive, profound, and thorough insights into the data (Linneberg, 2019). The researcher chose to code manually and not use software like NVivo, to have more control over the material and to find the informants' meanings and experiences.

Many researchers suggest using software like NVivo to process the data and ease the process of coding a large amount of data (Linneberg, 2019; Feng and Behar-Horenstein, 2019). Even though nine in-depth interviews create a lot of text, coding manually made the researcher more involved in the themes created and highlighted keywords. Crowston et al. (2012) point out that using software to code is best for projects with content analysis, large data sets and projects analysing multiple data sets over time. In addition, using this software requires a trained analyst to develop rules and needs substantial inputs of data (Linneberg, 2019). Moreover, using coding software still requires sufficient manual effort from the researcher (Crowston et al., 2012). The data was coded to find words or paragraphs that express their experiences, meanings, and recommendations about the subject.

3.5.2.1 Codes

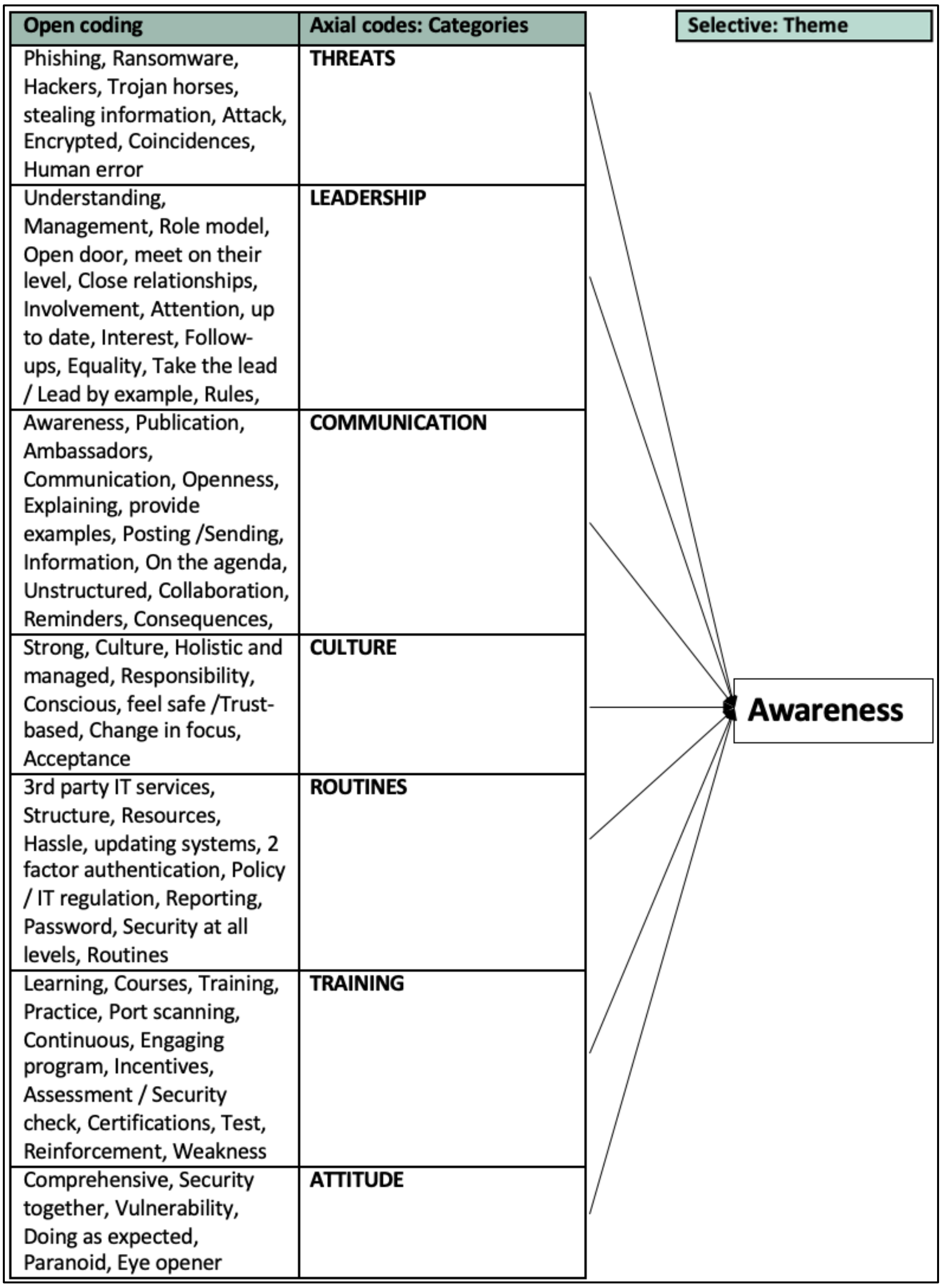
The chosen approach for coding was inductive. The coding process went through three steps, open coding, axial coding, and subjective coding, where the theme was identified (Williams and Moser, 2019). The coding process is illustrated in table 2. The first step of coding was open coding, where the codes were created line-by-line to identify and construct the meaning from the respondents (Williams and Moser, 2019; Charmaz and Thornberg, 2020). Moreover, using terms and phrases from the participants to have the codes close to the data mirroring the participants' words and ideas (Linneberg, 2019). From the first coding process, the researcher noted that the first 2-3 interviews created the most codes, and the following interviews added an average of 4 codes each. The line-by-line open coding resulted in 80 different codes.

3.5.2.2 Coding Categories

In the second step, axial coding, the codes were aligned and categorised into seven themes (Williams and Moser, 2019). The threat category includes the most significant threats the respondents mentioned; moreover, "encrypted" is included because what happened to the respondents' businesses that were attacked was that virus encrypted their whole file systems. Furthermore, "coincidences" and "human error" are included in the threat category because the respondents also state that an attack can happen by coincidence and from employee mistakes.

The leadership category consists of codes regarding how the management should act and the importance of a good relationship where one must be involved and meet at their level. Moreover, the respondents point out that the management must lead by example, be understanding toward the employees, be up to date about the threats, and be interested in cybersecurity. Furthermore, communication includes how the manager should communicate with employees by including the consequences of a cyberattack and constantly communicating by having this on the agenda of meetings.

Table 2 Coding Process



Open coding	Axial codes: Categories	Selective: Theme
Phishing, Ransomware, Hackers, Trojan horses, stealing information, Attack, Encrypted, Coincidences, Human error	**THREATS**	**Awareness**
Understanding, Management, Role model, Open door, meet on their level, Close relationships, Involvement, Attention, up to date, Interest, Follow-ups, Equality, Take the lead / Lead by example, Rules,	**LEADERSHIP**	
Awareness, Publication, Ambassadors, Communication, Openness, Explaining, provide examples, Posting /Sending, Information, On the agenda, Unstructured, Collaboration, Reminders, Consequences,	**COMMUNICATION**	
Strong, Culture, Holistic and managed, Responsibility, Conscious, feel safe /Trust-based, Change in focus, Acceptance	**CULTURE**	
3rd party IT services, Structure, Resources, Hassle, updating systems, 2 factor authentication, Policy / IT regulation, Reporting, Password, Security at all levels, Routines	**ROUTINES**	
Learning, Courses, Training, Practice, Port scanning, Continuous, Engaging program, Incentives, Assessment / Security check, Certifications, Test, Reinforcement, Weakness	**TRAINING**	
Comprehensive, Security together, Vulnerability, Doing as expected, Paranoid, Eye opener	**ATTITUDE**	

The category for culture includes how the respondent’s culture is in their business and how a good security culture should look like. One should have a responsible culture where one feels safe to come to the management and accept mistakes. Moreover, have a culture where change is in focused after an attack and is holistic and managed. The routines were identified by how the routines in their businesses are regarding security, recourses like third-party services, and password security. Moreover, “hassle” is included though the respondents point out that it can be a hassle following the routines for employees, even if they are essential. Moreover, they note that it must be “security at all levels”.

The training category consists of the different training processes the respondents have or could have. There should be a continuous, engaging program with incentives that get them to do these. Moreover, it includes “port scanning” and “assessment/security check”, though some respondents have done this to check their security and to find out what they need to focus on. Finally, attitude is the attitude the respondents think is essential to change; moreover, how their attitude has changed over the years and recent attacks have been an eye opener.

3.5.2.3 Main Category Theme

In the last step of the coding process, the selective level, the axial codes are integrated and organised in meanings, selecting the main thematic category (Williams and Moser, 2019). The overall theme created from the coding process is awareness. First, cybersecurity awareness is affected by the threat picture and how the leadership should be, followed by communication, culture, routines, training and education in the business, and the attitude toward cybersecurity. The interview findings will be presented and discussed in the next chapter.

4.0 Findings

This chapter presents the findings from the qualitative research on how managers can raise awareness of cybersecurity in SMBs in Norway (RO2). The chapter is divided into sub-chapters describing and providing findings on what threats are prominent and how aware they are of cybersecurity. Moreover, what the businesses exposed to cyberattacks have learned and how this changed their attitude. Secondly, findings regarding what training programs one should implement and how these create awareness. Thirdly, how the security culture is, the importance of a strong culture and how one can build a strong culture, the practices, and recommendations on how to communicate regarding cybersecurity, and findings on the importance of talking openly and that cybersecurity is everyone's responsibility. Lastly, this chapter presents the respondent's recommendations on how managers can raise awareness of cybersecurity in SMBs.

4.1 Threats and Cyberattacks

The findings show that most respondents have cybersecurity on the agenda and are aware of the potential threats. All but one respondent said cybersecurity is being discussed on different occasions in businesses, in meetings, emails or published on the intranet. However, one respondent states they do not discuss cybersecurity and leave everything handling IT externally at their IT supplier (R7). Therefore, they are unaware of the threats.

The most significant cybersecurity threats the respondents feared and talked about corresponded to the Cisco Umbrella report from 2021; ransomware and phishing attacks, i.e., director fraud and CEO scams (R1; R2; R3; R4; R5; R6; R8). R1 and R2 have experience with attacks happening in businesses they work with. Moreover, three of the respondents have had cyberattacks happen in the business they work in recently (R4; R6; R8). Two of the attacks were phishing attacks and CEO scams where the attacker pretended to be someone trusted in the company, which ended in ransomware. One attack happened due to a lack of password security and poor infrastructure (R4).

Findings show that the focus has changed drastically in the businesses after the attack. Both the structure and attitude had changed (R1; R2). The attacks were a wake-up call for all the employees and more people saw IT security as an essential aspect of the business and something everyone in the business needs to focus on, not only the IT department (R4, R8). One respondent said that: "*We learned one thing (…) we must ensure that all employees receive very, very good training in what to open and not open*" (R6), referring to phishing emails. Moreover, R8 stated that:

> *"[We have] been perhaps more aware. [put cybersecurity] high on the agenda and make objective assurance as good as possible, and that there must be something that is discussed frequently between employees".*

4.2 Training

Findings show that it differs whether they provide training programs for the employees towards cybersecurity. Two of the respondents regularly send out training modules to the employees (R4, R8). One of the respondents has implemented nano learning, which sends out one weekly email with information about threats and frequently used bots. They include what to think about when one checks addresses and what to open and not. Moreover, some of the emails are simulated phishing emails, contributing to extra learning and awareness to see how the employees react to them (R8). Both respondents point out that it is vital to have the learning as close to the environment as possible (R8; R4).

R4 points out that they have noticed a change in attitude for the employees after implementing the training modules:

> *"I have noticed a difference; it is simply that people get it a little more in their everyday life, (…) you are reminded if it is a slightly more frequent interval. (…) a little change of attitude in relation to the fact that we should not lose data".*

The respondents who have not implemented training programmes or modules have discussed doing it and are researching what type of training program to implement (R5; R7). However, two respondents point out that they do not think they need to implement training programs because they already talk so much about it daily and share experiences about what is happening. Hence, it is not anything new for the employees (R9). Furthermore, one respondent points out that when the company grows, this is something they would consider; a more regular engaging program over time that captures both new and existing employees.

> *"I feel that you should have, in regard to programmes, maybe have some incentives, not necessarily in money, (…) like in Oslo where we have a ride bike to work campaign, and those who have cycled the most days or kilometres to work during summer gets something, (…) do something like that, make it a bit catchy"* (R3).

Findings show that some of the respondents' businesses have undertaken assessments to check the IT security, where an external agency simulates an attack, to check their vulnerabilities (R5; R6). The assessments have helped increase awareness and determine what they need to focus on when implementing training programs (R6).

4.3 Culture

Overall, findings show that the security culture is strong in the different businesses and that awareness is affected by the culture of the business. For example, R2 states: "*Awareness helps culture, so if you manage to make employees aware, then you will also get a better security culture*". The most prevalent finding is that cybersecurity needs to be put on the management team's agenda to influence employees to follow protocols and have a sound security culture (R5; R1; R4; R9), which underpins Uchendu et al.'s (2021) literature research about the managements role in creating a cybersecurity culture.

To build a strong security culture and influence employees to follow security protocols, R1 states:

> *"If you manage to build a security culture rooted in the management and some strong role models, then you manage to get the vast majority to follow it. A positive security culture is to find some ambassadors in the company who says, "Yes, it is a bit of a hassle with this 2-factor authentication, but you know what, it is so much safer, and that is why we should do this"".*

R4 are working to build a new and robust security culture after the attack, and the most important factors are that it must be anchored at the top:

> *"It starts with the management. It must be anchored at the top, and they must be aware. [The management] cannot sit and want to have simple passwords, simple solutions. (…) Go out with information to the employees; that in this company we focus on IT security and cybersecurity. It can also be a little tool in a way to talk about the consequences if you do not think about [cyber] security, what are the consequences financially, what can be a consequence for me and you in relation to our work situation. In the worst case you will be without a job"* (R4).

4.4 Communication

On questions about the informants' practices and recommendations regarding communication in the businesses amongst cybersecurity, all the respondents suggest using the communication channels they already have. For example, use email, Slack, and Teams, and publish on the intranet when new threats occur with "tips and tricks" on how to spot a phishing email regularly. In addition, in meetings, use more time to communicate the threats against the business (All respondents).

"One should communicate first and foremost with being the examples that go before oneself" (R1).

"Explain why, why we must take action, why it is important that you also contribute" (R2).

The respondents agree that the managers need to put this on the agenda, and the managers must act and communicate regularly with the employees, being present and communicating in the hallways. Create a culture that talks about it. R6 point out:

> *"Talking to people and walking around being present to hear and talk to people and tell what is happening. (…) Speak in a way with people that one understands the importance of it".*

Moreover, the management needs to understand the importance of cybersecurity. R2 states: *"If the management does not understand the importance of it, and prioritise it, one cannot expect any particular awareness from the employees either".*

The respondents were asked if one should consider incentives to get the employees to follow security protocols. Findings shows, similar to Cram et al. (2017) and Park and Chai's (2018) studies that most respondents believe one should not be rewarded for doing what is expected (R1; R5; R6). However, R2 point out that one cannot expect a specific behaviour if one has not been given the necessary conditions to avoid mistakes. Therefore, the management must first and foremost lay the grounds for following these protocols and policies.

4.5 Openness and Equality

Findings show that being open and having a culture that builds on openness from the management to the employees and transparency regarding attacks is essential for building a solid security culture (R2; R3; R6). In addition, sharing and being open after a cyberattack will contribute to businesses learning from each other and standing stronger together against the threats.

> *"One does not necessarily need to go public with the details of the attack, but the experiences you have gained in handling, and the consequences, are good awareness measures"* (R2).

Equality is another important factor the respondents point out. Equality regarding following different measures and policies in the businesses.

> *"Even the manager must be responsible for cybersecurity, even the manager must do 2-factor logins, everyone, there is equality really for everyone, and it is simply with a good example, and then it is by encouraging that all our employees are important for the values in our company"* (R1).

Findings from the data show that all the different businesses have or try to have a short way to the management and see this as an essential factor in raising awareness (all respondents). R2 points out: *"If you are going to have a hope of increasing the employees' awareness, then it must at least be with the board and management; that is a prerequisite".* Furthermore, the short way to the management builds a culture where the employees feel they can tell if one made a mistake, e.g., opening an email they were not supposed to, one can put measures in right away (R6; R7; R1).

4.6 Recommendations

The recommendations the respondents have for managers raising awareness for cybersecurity in SMBs is that first and foremost, one must take charge and lead by example (R1; R2; R3; R4; R5). Furthermore, one must be aware of the threat picture and familiarise oneself with the outside world (R1). R6 points out:

> *"Be aware of what great consequences it can have (…) I think it is important that you have a leader who cares and thinks that there is something we have to take responsibility for".*

Managers need to read up (R8) and send out information regularly to the employees using the communication channels used in the business (R3), moreover, communicate openly around the office and in meetings (R2; R4; R7; R6). Furthermore, all the respondents use third-party services for IT and recommend buying services from other trustworthy, reputable vendors (all respondents).

One respondent points out that it all starts with the culture:

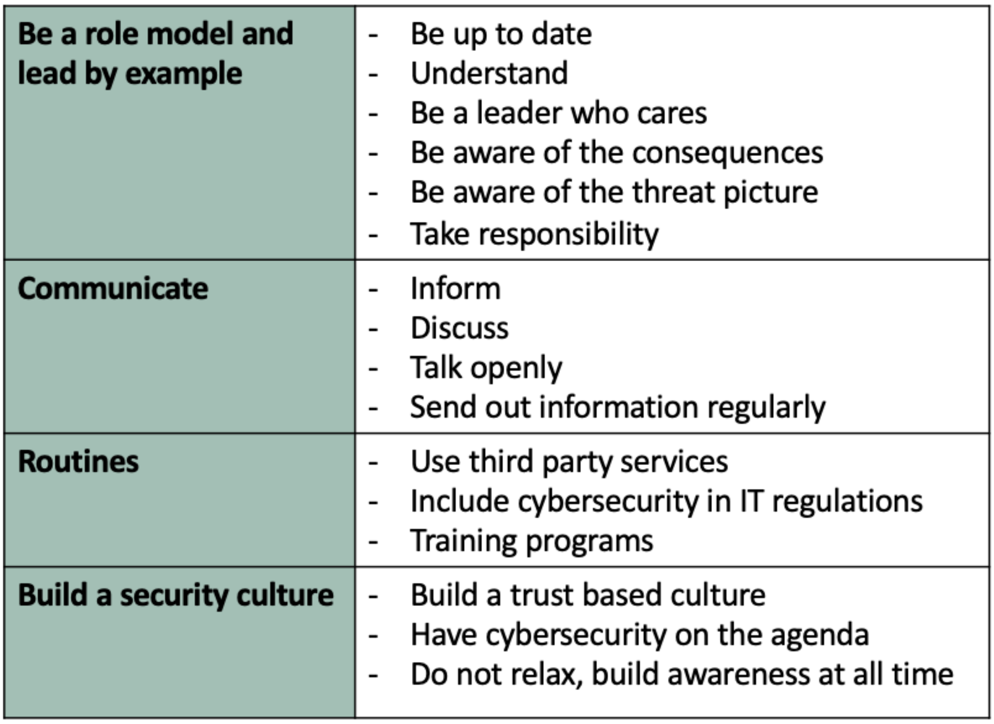
> *"I come back to culture, I mean, it all must start somewhere, and if we work together and you dislike me because you do not trust me, it does not matter what I say and try to influence people to do. People do not bother to hear if they do not think that there are not things that somehow affect them directly".* (R9)

> *"Build a culture at work that is trust-based, where people feel, and you build a sense of security to be able to speak out and make mistakes"* (R9).

Another point the respondents emphasize is that raising awareness must start at the onboarding stage. Have a chapter about cybersecurity in the IT regulation and training programs, as there always are new employees (R3). R6 reflects that their attack happened to a new employee, so providing training right away on this is vital. They have learned the importance of taking action and raising awareness from the beginning (R6).

Summarised in table 3 are keywords highlighted from the findings for recommendations on how managers can raise awareness of cybersecurity in SMBs:

Table 3 Keywords from the findings for recommendations



Be a role model and lead by example	- Be up to date - Understand - Be a leader who cares - Be aware of the consequences - Be aware of the threat picture - Take responsibility
Communicate	- Inform - Discuss - Talk openly - Send out information regularly
Routines	- Use third party services - Include cybersecurity in IT regulations - Training programs
Build a security culture	- Build a trust based culture - Have cybersecurity on the agenda - Do not relax, build awareness at all time

5.0 Discussion

In this chapter, the findings from the analysis will be discussed in relation to the literature to provide recommendations for how managers can raise cybersecurity awareness in SMBs in Norway (RO2 and RO3) and answer the research question, "How can managers raise awareness of cybersecurity in SMBs in Norway?". This chapter is divided into sub-chapters building up with the meanings and experiences of the respondents to provide recommendations for managers.

5.1 Awareness and Training Programs

The increase in cybersecurity threats and incidents over the last few years in Norway makes it vital for SMBs to focus on cybersecurity awareness (Armenia et al., 2021), as employees are the first line of defence and the weakest link (Li et al., 2019). Findings from the analysis show different factors managers can use to contribute to raising cybersecurity awareness. Awareness allows individuals to recognise security concerns and respond accordingly (Alruwaili, 2019). As SMBs often do not have the same resources as larger companies (van Haastrecht et al., 2021; Armenia et al., 2021), it is prevalent that all employees are aware and know the consequences as one attack could result in overthrowing the whole company (R5). Different factors contribute to raising cybersecurity awareness in businesses. First, one needs to be aware of the threat picture (R1). Some of the most prevalent threats for SMBs that the respondents and literature focus on are malware, phishing emails, integrity threats and ransomware (Cisco, 2021; Lachen et al., 2020; R1; R2; R3; R4; R5; R6; R8).

Previous research focuses on implementing training programs to develop proper security behaviour in SMBs and raise awareness (Arachchilage et al., 2016; van Haastrecht et al., 2021; Ghafir et al., 2018; Bada and Nurse, 2019). There are various forms of training programs one can implement; however, as many SMBs lack resources (van Haastrecht et al., 2021; Aigbefo et al., 2020), these training programs are often the last thing on their mind. This research shows that only two out of nine respondents use training programs actively in their business. The training programs used are training modules or emails containing information about the latest threats and trends. One respondent (R8) uses nano learning which also includes simulated phishing emails to make the learning as close to the environment as possible (Bada and Nurse, 2019). Moreover, as Baillon et al. (2019) study suggests, having simulated phishing emails increases employees' perceived risk. Furthermore, findings show that having a continuous, shorter, more engaging training program would raise more awareness than having a full day with information (R3; Ghafir et al., 2018).

5.2 Security culture must be rooted at the top

Implementing training programs in a business alone will not raise cybersecurity awareness. Culture, however, is a vital aspect of raising awareness. Cybersecurity breaches are often caused by employees' lack of knowledge and ignorance (Alshaikh, 2020), making it vital for management to prioritise this and provide the attention it requires. Therefore, cybersecurity must be put on the agenda to raise awareness and goes hand in hand with the culture.

> *"Awareness helps culture, so if you manage to make employees aware, then you will also get a better security culture"* (R2).

Moreover, to build a good security culture, it must be rooted in the management, and the management needs to do the work themselves. It must be equality for everyone, and as the managers' attitude influences the employee's compliance, they must go in front as a good example (Park and Chai, 2018; R1; R4).

> *"It really starts at the top; it must be anchored at the top, they [the management] must be aware"* (R4).

The management must prioritise and act as role models. As the psychological attachment theory suggest, and findings from the interviews point out, the more involved the management is with building awareness, the more it influences the employees. Building a relationship between managers and employees is vital in raising awareness; the better the relationship is, the more the employees will identify with the business and the culture, and the more they are likely to comply (Alshaikh and Adamson, 2021; Park and Chai, 2018). Moreover, the employees' attitude toward security information must be acknowledged (Lebek et al., 2014). If employees have a negative attitude to security or the culture, it is harder to get them to comply (Aigbefo et al., 2020). Therefore, the managers and other key people in the business need to lay the grounds for how cybersecurity is handled and how they influence people to comply with security (Ifinedo, 2012; Li et al., 2019; Bulgurcu et al., 2010).

The psychological attachment theory suggests using incentives to get employees to comply (Alshaikh and Adamson, 2021); however, findings show that to influence employees, one should not have incentives but instead act as a good role model. Moreover, respondents point out that one should not get rewarded for doing expected behaviour (R1; R5; R6). However, if someone takes responsibility for others learning, that should be recognised positively (R1).

> *"This is not something you should do as an extra. This is something you have to do because you have a job, and it applies wherever you are"* (R6).

5.3 Communication

Communication is one of the most critical factors for building a good security culture. Through communication, the management transfers the goals and makes the employees understand the business environment whilst creating belonging, commitment, and awareness (Ioannou et al., 2019; Welch and Jackson, 2007). Explaining why cybersecurity is critical, why we must act and what the consequences are if one gets attacked is vital (R2; R6). Furthermore, communication makes employees feel a sense of belonging (Welch and Jackson, 2007), which helps build awareness. The findings show that using the communication channels already used by businesses, e.g., mail, Teams, Slack, or frequently posting on the intranet if new threats are emerging, is essential. Moreover, talking casually in the corridors or during lunch will increase awareness and the relationships between the managers and employees.

It is vital to communicate and speak so that people understand the importance of cybersecurity and meet at their level (R6; R3). Moreover, transparency is vital, as open communication provides trust (Zainab, 2021). The managers must know their audience and meet at the employee level (Alshaikh and Adamson, 2021). Talking technical about cybersecurity and cyber threats can lead to confusion; therefore, one must communicate the consequences of getting attacked, so they are aware of the impact it can have.

5.4 Cybersecurity Is Everyone's Responsibility

Cybersecurity is everyone's responsibility, not only the IT departments (Aigbefo et al., 2020; Ifinedo, 2012; Bulgurcu et al., 2010). Moreover, the management also needs to follow the policies and regulations. Findings show that the respondents point out that the management cannot expect the employees to follow them if they do not do this themselves. The management must lead by example and be good role models for cybersecurity to get the employees to follow (R1). A short way to the management and a flat structure are essential factors findings show. To increase the awareness of cybersecurity, it is vital that the employees feel a sense of belonging. Moreover, they should feel safe to report incidents or if they have opened an email that later has shown to contain a virus (R6; R7; R1).

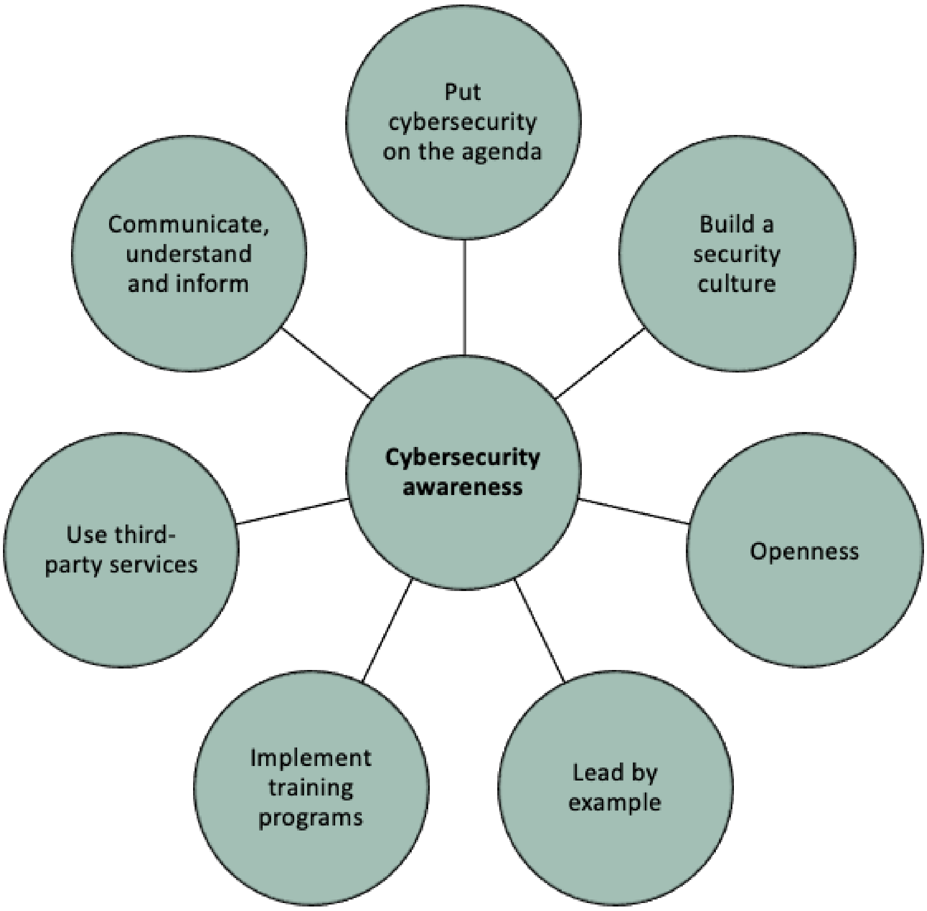
Following the importance of equality, openness is another vital aspect of creating a culture that builds awareness between the management and employees and transparency in the business environment around attacks. Following some significant attacks on businesses in Norway, who have gone public with what they have learned have created more awareness for other businesses. The respondents see this as necessary to create employee awareness; showing them that this could also happen to them. However, one does not necessarily need to go public with the details; sharing the experiences and consequences and how one handled it will contribute to raising awareness (R2). Openness between management and employees is also essential to create awareness. A culture of openness, where everyone feels safe to discuss and talk about new threats and what one is insecure or unsure about, is vital (R3; Zainab, 2021). One should be allowed to make mistakes without being looked down at.

> *"Create culture and awareness around security as a whole"* (R3).

5.5 Recommendations for Managers to Raise Cybersecurity Awareness in SMBs

To summarise and partly conclude the research question, “How can managers raise awareness of cybersecurity in SMBs in Norway?” based on the discussion from the analysis and reviewed literature, the recommendations for managers to raise awareness are presented in table 4. For managers in SMBs, this research recommends raising cybersecurity awareness by putting cybersecurity high on the agenda, building a security culture based on openness and leading by example. Furthermore, it is vital to implement an engaging training program directed at the employees’ work and use third-party services. Finally, communicate, understand, and inform about the threats.

Table 4 Recommendations for Raising Cybersecurity Awareness in SMBs



Put cybersecurity on the agenda

Findings from the analysis and literature show that managers must put cybersecurity on the agenda and prioritise and provide enough resources for cybersecurity (Uchendu et al., 2021). As employees that do not work with IT tend not to have the knowledge and focus on cybersecurity, the management must provide enough information about the topic. The management must be aware of the threat picture. Talk about cybersecurity, the threats, and what is happening with other businesses. What are the latest trends? One must prioritise cybersecurity as one attack could end the company (R1).

Build a sound security culture

Moreover, one must build a good security culture. If security is not rooted in the culture of the business, then it is much harder to get the employees to be aware. Sound cybersecurity culture is essential to prevent breaches due to a lack of knowledge from the employees (Alshaikh, 2020). The analysis implies that culture and awareness go hand in hand. Without a proper security culture, it is hard to follow security strategies. The most critical factors in building a good security culture are leadership and support from the management (Uchendu et al., 2021). One needs to build a trust-based culture where people can be able to speak out and be able to make mistakes (R9; Zainab, 2021). If the employees do not trust the management, it does not matter what they say or tries to influence if they do not think it affects them directly (R9).

Openness

As a manager, one must create a culture based on openness. Managers and employees should have a trusted relationship and be allowed to make mistakes, learn, and develop. In addition, one needs to create a culture where one openly discusses threats that occur and where the employees can come and discuss and talk to the leaders if there is something they are insecure or unsure about (R3).

Lead by example

Furthermore, the security culture must be rooted at the top; the management must be aware, go in front, and lead by example (Park and Chai, 2018). To create and increase cybersecurity awareness for the employees, managers need to be good role models or find some good ambassadors in the business that has the power to influence (Alshaikh and Adamson, 2021). The manager's attitude toward information security influences the employees' attitude (Park and Chai, 2018). Therefore, the management must follow the security policies and procedures in the business, use 2-factor authentication, and change passwords regularly. Most importantly, the management must care about cybersecurity. They must read up and understand the importance (R1; R2).

Implement training programs

Implementing training programs can also contribute to increasing cybersecurity awareness. Moreover, when implementing training programs, it is vital to make sure it suits context of the business (Bada and Nurse, 2019). One should implement training programs directed at the employees' work. Furthermore, including some simulated phishing emails will also increase awareness and make people think twice before clicking on a link and learn how important it is to read the whole email and check the address correctly. Implementing training programs in the day-to-day work environment, such as using nano learning, will provide more awareness because one receives many emails daily, and a significant threat is phishing emails. Moreover, the training program should be continuous, not only once every sixth month (R3).

Use third-party services

In order to protect the company, it is found that SMBs use third-party services regarding their software systems. Findings show that using trusted software vendors will strengthen their security; having someone who holistically manages and updates will allow the businesses to concentrate and work with what they focus on (R1; Forbes, 2021). However, using an extensive software system like Microsoft Azure can make one vulnerable because one is a part of a larger organisation if someone attacks them. For example, the attack on Microsoft Exchange affected many smaller businesses (Microsoft, 2021). However, it is a security to know that one does not stand alone against the threats (R1). It makes one stronger to be a part of something bigger, and one does not stand alone if an attack happens. However, it is essential to note that using third-party services does not eliminate cyber threats. Third-party services are an addition to the other awareness recommendations.

Communicate, understand, and inform

Communication is the most critical factor and recommendation for managers in SMBs to increase cybersecurity awareness (Ioannou et al., 2019). Managers must explain why cybersecurity is critical, why one must act, and the consequences of an attack. Talking regularly and non-structured in the hallways or at lunch with the employees will increase awareness. Moreover, sending emails and posting on the intranet to inform about new threats and what is happening is vital. At business meetings, one should include one slide of the presentation about cybersecurity and the threats to make the employees more aware that this also can happen to them. Finally, and most importantly, talk about the consequences, what can happen if one gets attacked, and the financial sufferings that can happen; it can be as catastrophic as the end of the business and loss of jobs.

One last point to make is how to communicate. It is crucial to meet at the employee level (Alshaikh and Adamson, 2021). Talking technical about cybersecurity for most employees does not mean anything and can lead to confusion. Therefore, the management needs to know their audience and talk in a way that one knows that they will understand and take the time to let there be questions. Cybersecurity is everyone's responsibility.

6.0 Conclusion

Cybersecurity is everyone's responsibility, not only the IT department (Aigbefo et al., 2020; Ifinedo, 2012; Bulgurcu et al., 2010). Following the rapid digitalisation in Norway, the country is increasingly targeted by cybercriminals in both public and private sectors (Regjeringen, 2019). As SMBs have smaller budgets and fewer resources, they are more and more targeted by cybercriminals because they lack the capability to protect themselves and cybercriminals see them as a path to larger organisations. Moreover, a significant proportion of cyberattacks happen due to employees' lack of knowledge and awareness, making it vital to raise employee awareness. Previous research focuses on implementing training programs to raise cybersecurity awareness; however, only implementing training programs will not contribute to awareness in the long run. Many SMB managers do not see the importance of cybersecurity because they do not see themselves as a likely target and cannot justify the extent of resources to use (Benz and Chatterjee, 2020). However, the management's role in raising cybersecurity awareness for employees in SMBs is vital.

This research has explored how managers can raise cybersecurity awareness in small and medium-sized businesses in Norway and provided recommendations for managers in SMBs to raise awareness. In doing so, it has assessed the research question: "How can managers raise awareness of cybersecurity in SMBs in Norway?".

Based on this research, there are seven recommendations for managers to raise cybersecurity awareness in SMBs in Norway. First and foremost, managers must **put cybersecurity on the agenda**. Managers need to talk and provide information about cybersecurity. One should look at what is happening to other businesses and read up about the threats. Secondly, one must **build a cybersecurity culture**. Culture and awareness go hand in hand. Without a proper cybersecurity culture, one cannot expect to raise awareness. Moreover, build a trust-based culture with support from the management where employees can speak out and make mistakes.

Thirdly, build a culture based on **openness**. There should be openness between the managers and employees and openness between businesses regarding attacks. One needs to learn from each other and create a culture where one openly discusses threats and the severity of cybersecurity. Furthermore, one need to **lead by example**. The security culture must be rooted at the top. Managers need to go in front as good examples; if the management does not follow security protocols or cares about cybersecurity, they cannot expect the employees to follow protocols or care about cybersecurity.

Furthermore, one should consider **implementing training programs**. Most cyberattacks happen through phishing, and previous research and findings from the analysis show that implementing continuous and engaging training programs in the context of the employees' work will contribute to raising awareness. Furthermore, in addition to the recommendations for raising awareness, SMBs should **use third-party services**. As most SMB employees have responsibility for different parts of the business, one should outsource IT and security to other trusted vendors to strengthen the business and allow employees to focus on the day-to-day business. Lastly, the most important recommendation for managers in SMBs is to **communicate, understand and inform**. Managers must explain why cybersecurity is critical and what the consequences are. Talk regularly and non-structured about what is happening with other businesses and send regular updates about the threat picture to the employees.

6.1 Limitations and Future Research

The limitation of this research is that the data is collected from one country. Therefore, the recommendations cannot be generalised; however, they can be used as a base for raising awareness for SMB managers. Moreover, the interviews are only conducted from the manager's perspective. Including the employee's perspective could contribute to a better understanding of what factors will raise awareness and confirm or contradict what the management sees as necessary.

Cybersecurity is an increasingly important theme. More and more research should focus on the non-technical aspect, as this strategic security viewpoint is equally as important as the technical aspect of cybersecurity. For this research, the suggestion for further research is to use employees' meanings and experiences on the importance of cybersecurity in SMBs. See what they suggest for raising awareness. Moreover, gain an understanding of employees' knowledge about cybersecurity.

References

Aigbefo, Q. A. et al. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour and Information Technology*. Available from: https://doi-org.uow.idm.oclc.org/10.1080/0144929X.2020.1856928 (Accessed: 27. April 2022).

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health* 26(9) pp. 1113-1127. Available from: https://doi.org/10.1080/08870446.2011.613995 (Accessed: 5. May 2022).

Alharahsheh, H. H. and Pius, A. (2020). A Review of key paradigms: positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences* 2(3) pp. 39-43. Available from: DOI: 10.36348/gajhss.2020.v02i03.001 (Accessed: 29. July 2022).

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advances Research in Computer Science*. Available from: DOI: http://dx.doi.org/10.26483/ijarcs.v10i5.6476 (Accessed: 26. April 2022).

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. *Computer & Security* 98. Available from: https://doi.org/10.1016/j.cose.2020.102003 (Accessed: 7. May 2022).

Alshaikh, M. and Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing* 25 pp. 829-841. Available from: https://doi.org/10.1007/s00779-021-01551-2 (Accessed: 6. May 2022).

Arachchilage, N. A. G. et al. (2016). Phishing threat avoidance behaviour: An Empirical investigation. *Computers in Human Behaviour* 60. Available from: http://dx.doi.org/10.1016/j.chb.2016.02.065 (Accessed: 27. April 2022).

Armenia, S. et al. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems* 147, 1113580. Available from: https://doi.org/10.1016/j.dss.2021.113580 (Accessed: 27. April 2022).

Bada, M. And Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security* 27(3) pp. 393-410. Available from: DOI 10.1108/ICS-07-2018-0080 (Accessed: 26. April 2022).

Baillon, A. et al. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PLoS ONE* 14(12). Available from: https://doi.org/10.1371/journal.pone.0224216 (Accessed: 1. August 2022).

Benz, M. and Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons* 63 pp. 531-540. Available from: https://doi.org/10.1016/j.bushor.2020.03.010 (Accessed: 3. August 2022).

Budke, C. A. and Enko, P. J. (2020) Physician Practice Cybersecurity Threats: Ransomware. *Missouri medicine* 117(2) pp. 102-104. Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7144701/ (Accessed: 1. August 2022).

Bulgurcu, B. et al. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly* 34(3) pp. 523-548. Available from: 10.2307/25750690 (Accessed: 5. May 2022).

Chara, M. and Neely, A. (2021). Grounded Theory: A Guide for Exploratory Studies in Management Research. *International Journal of Qualitative Methods* 20. Available from: DOI:10.1177/16094069211013654 (Accessed: 5. July 2022).

Charmaz, K. and Thornberg, R. (2020). The pursuit of quality in grounded theory. *Qualitative Research in Psychology* 18(3) pp. 305-327. Available from: https://doi.org/10.1080/14780887.2020.1780357 (Accessed: 25. July 2022).

Cisco. (2021). Think Before You Click. Available from: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf (Accessed: 27. April 2022).

Cisco. (2021). Thriving as a Small or Midsize Business with a Strong Cybersecurity Strategy. Available from: https://www.cisco.com/c/dam/en/us/products/collateral/security/2021-outcomes-study-for-smb.pdf?dtid=osscdc000283 (Accessed: 4. August 2022).

Cisco. (2021). 2021 Cyber security threat trends – phishing, crypto top the list. Available from: https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list (Accessed: 4. August 2022).

Constantinou, C. S. Et al. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research* 17(5) pp. 571-588. Available from: DOI: 10.1177/1468794116686650 (Accessed: 25. July 2022).

Corley, K. G. (2015). A Commentary on “What Grounded Theory Is…”: Engaging a Phenomenon from the Perspective of Those Living it. *Organizational Research Methods* 18(4) pp. 600-605. Available from: doi:10.1177/1094428115574747 (Accessed: 5. July 2022).

Cram, W. A. et al. (2017). Seeing the forest *and* the trees: A meta-analysis of information security policy compliance literature. *Proceedings of the 50th Hawaii International Conference on System Sciences.* Available from: http://hdl.handle.net/10125/41649 (Accessed: 6. May 2022).

Crowston, K. Et al. (2012). Using natural language processing technology for qualitative data analysis. *International Journal of Social Research Methodology* 15(6) pp. 523-543. Available from: http://dx.doi.org/10.1080/13645579.2011.625764 (Accessed: 22. July 2022).

DESI (2022). The Digital Economy and Society Index – Countries' performance in digitalisation: Norway. Available from: https://digital strategy.ec.europa.eu/en/policies/countries-digitisation-performance (Accessed: 9. August 2022).

Donno, M. Et al. (2018). DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks*. Available from: https://doi.org/10.1155/2018/7178164 (Accessed. 18. August 2022).

Feng, X. and Behar-Horenstein, L. (2019). Maximizing Nvivo Utilities to Analyse Open-Ended Responses. *The Qualitative Report* 24(3) pp. 563-571. Available from: https://doi.org/10.46743/2160-3715/2019.3692 (Accessed: 9. August 2022).

Forbes. (2021). Managed IT Services: The Small Business' Security Savior. Available form: https://www.forbes.com/sites/acronis/2022/01/12/managed-it-services-the-small-business-security-savior/?sh=44ac03b53083 (Accessed: 5. August 2022).

Gartner. (No date) "Small and Midsize Businesses (SMB)". Gartner Glossary. Available from: https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses (Accessed: 03. August 2022).

Georgescu, T-M. (2021). A study on how the Pandemic Changes the Cybersecurity Landscape. *Informatica economica* 25(1) pp. 42-60. Available from: DOI: 10.24818/issn14531305/25.1.2021.04 (Accessed: 1. August 2022).

Ghafir, I. Et al. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing* 74 pp. 4986-5002. Available from: https://doi.org/10.1007/s11227-018-2337-2 (Accessed: 27. April 2022).

Ghauri, P. et al. (2020). *Research methods in business studies*. Cambridge: Cambridge University Press. Fifth edition.

Goldkuhl, G. (2012). Pragtmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems: Special Issue: Qualitative Research Methods* 21(2) pp.135-146. Available from: https://doi.org/10.1057/ejis.2011.54 (Accessed: 27. July 2022).

Hagger, M. S. and Chatzisarantis, L. D. (2005). First-and higher-order models of attitudes, normative influence, and perceived behaviour control in the theory of planned behaviour. *British Journal of Social Psychology* 44 pp. 513-535. Available from: DOI:10.1348/014466604X16219 (Accessed: 6. May. 2022).

Hayashi Jr. P. et al. (2019). Validity in Qualitative Research: A processual Approach. *The Qualitative Report* 24(1) pp. 1-14. Available from: https://doi.org/10.46743/2160-3715/2019.3443 (Accessed: 26. July 2022).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computer & Security* 31. Available from: doi:10.1016/j.cose.2011.10.007 (Accessed: 5. May 2022).

Ioannou, M. et al. (2019). Cybersecurity Culture in Computer Security Incidents Response Teams. *IEEE Electronic Library (IEL)* 6. Available from: https://ieeexplore-ieee-org.uow.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8885240 (Accessed: 11. May 2022).

Janghorban, R. et al. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-being* 9(1). Available from: https://doi.org/10.3402/qhw.v9.24152 (Accessed: 25. July 2022).

Jenner, B. M. and Myers, K. C. (2019). Intimacy, rapport, and exceptional disclosure: a comparison of in-person and mediated interview contexts. *International Journal of Social Research Methodology* 22(2) pp. 265-177. Available from: https://doi.org/10.1080/13645579.2018.1512694 (Accessed: 25. July 2022).

Kallio, H. et al. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advances nursing* 72(12) pp. 2954-2965. Available from: DOI: 10.1111/jan.13031 (Accessed: 26. July 2022).

Kelman, H. C. (1958). Compliance, Identification, and Internalization: Three Processes of Attitude Change. *The Journal of Conflict Resolution* 2(1) pp. 51-60. Available from: http://www.jstor.org/stable/172844 (Accessed: 6. May 2022).

Kirchherr, J. and Charles, K. (2017). Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia. *PLoS ONE* 13(8). Available from: https://doi.org/10.1371/journal. pone.0201710 (Accessed: 25. July 2022).

Krosnick, J.A. (2018). Questionnaire design. In *The Palgrave handbook of survey research* pp. 439-455. Palgrave Macmillan, Cham.

Lachen, M. et al. (2020). Review and insights on the behaviour aspects of cybersecurity. *Cybersecurity* 3(10). Available from: https://doi.org/10.1186/s42400-020-00050-w (Accessed: 6. May 2022).

Lebek, B. et al. (2014) Information security awareness and behaviour: a theory-based literature review. *Management Research Review* 37(12) pp. 1049-1092. Available from: DOI 10.1108/MRR-04-2013-0085 (Accessed: 5. May 2022).

Li et al. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour. *International Journal of Information Management* 45. Available from: https://doi.org/10.1016/j.ijinfomgt.2018.10.017 (Accessed: 26. April 2022).

Linneberg, M. S. (2019). Coding qualitative data: a synthesis guiding the novice. *Qualitative Research Journal.* 19(3) pp. 259-270. Available from: https://doi.org/10.1108/QRJ-12-2018-0012 (Accessed: 21. July 2022).

Lub, V. (2015). Validity in Qualitative Evaluation: Linking Purposes, Paradigms, and Perspectives. *International Journal of Qualitative Method* 14(5). Available from: https://doi.org/10.1177/1609406915621406 (Accessed: 26. July 2022).

Microsoft. (2019). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. Available from: https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (Accessed: 3. August 2022).

Microsoft. (2021). HAFNIUM targeting Exchange Servers with 0-day exploits. Available from: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (Accessed: 10. August 2022).

MonkeyLearn.com (2022). No-Code Text analysis: Word cloud. Available from: https://monkeylearn.com

Morse, J. M. et al. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods* 1(2) pp.13-22. Available from: https://doi.org/10.1177/160940690200100202 (Accessed: 26. July 2022).

Mutalib, M. M. A. et al. (2021). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. *IEEE International Conference on Recent Advances and Innovations in Engineering -ICRAIE.* 6 pp- 1-6. Available from: DOI: 10.1109/ICRAIE52900.2021.970399 (Accessed: 18. August 2022).

Mwita, K. M. (2022). Research in Business & Social Science. *International Journal of Research in Business and Social Science* 11(4) pp. 414-420. Available from: DOI:10.20525/ijrbs.v11i4.1776 (Accessed: 25. July 2022).
Norek, C. D. et al. (2007). SMB? You Can Transform Your Supply Chain, Too. *Supply Chain Management Review.* Available from: http://chainconnectors.com/SCMR_SMB.pdf (Accessed: 5. August 2022).

NSM. (2021). Nasjonalt digitalt risikobilde 2021. Available from: https://nsm.no/getfile.php/137495-1635323653/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf (Accessed: 10. August 2022).

NSM. (2022). Tiltak for å unngå tjenestenektangrep. Available from: https://nsm.no/aktuelt/tiltak-for-a-unnga-tjenestenektangrep (Accessed: 18. August 2022).

Parameswaran, U. D. et al. (2019) To live (code) or to not: A new method for coding in qualitative research. *Qualitative Social Work*. 19(4) pp. 630-644. Available from: DOI: 10.1177/1473325019840394. (Accessed: 21. July 2022).

Park, M. and Chai, S. (2018). Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance. *Proceedings of the 51st Hawaii International Conference on System Sciences.* Available from: http://hdl.handle.net/10125/50484 (Accessed: 6. May 2022).

Pollini, A. et al. (2021). Leveraging human factors in cybersecurity: an integrated methodical approach. *Cognition, Technology & Work* 24 pp. 371-390. Available from: https://doi.org/10.1007/s10111-021-00683-y (Accessed: 3. August 2022).

PWC. (2021). SMEs in the world of Cyber- An Insight. Available from: https://www.pwc.com/mt/en/publications/technology/smes-in-the-world-of-cyber.html (Accessed: 03. August 2022).

Qabajeh, I. et al. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review* 29. Available from: https://doi.org/10.1016/j.cosrev.2018.05.003 (Accessed: 27. April 2022).

Regjeringen. (2019). National Cyber Security Strategy for Norway. Available from: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf (Accessed: 03. August 2022).

Reuters. (2022). Norway blames “pro-Russian group” for cyber attack. Available from: https://www.reuters.com/world/europe/norway-targeted-by-cyber-attack-security-agency-2022-06-29/ (Accessed: 18. August 2022).

Roth, W-M. and von Unger, H. (2018). Current Perspectives on Research Ethics in Qualitative Research. *Qualitative Social Research* 19(3). Available from: https://doi.org/10.17169/fqs-19.3.3155 (Accessed: 27. July 2022).

Saunders, M. N. K. Et al. (2019). Research Methods for business students Ebook. Pearson Education, Limited. ProQuest Ebook Central. Available from: https://ebookcentral.proquest.com/lib/westminster/detail.action?docID=5774742.

Silva, J. A. H. et al. (2019). A Survey on Situational Awareness of Ransomware Attacks-Detection and Prevention Parameters. *Remote Sensing* 11(10). Available from: doi:10.3390/rs11101168 (Accessed: 1. August 2022).

Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management* 5(2) pp. 18-27. Available from: https://ssrn.com/abstract=3205035 (Accessed: 25. July 2022).

Turyahikayo, E. (2021). Philosophical paradigms as the bases for knowledge management research and practice. *Knowledge Management & E-learning* 13(2) pp. 209-224. Available from: https://www.proquest.com/scholarly-journals/philosophical-paradigms-as-bases-knowledge/docview/2559469688/se-2 (Accessed: 27. July 2022).

Uchendu, B. et al. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security* 109. Available from: https://doi.org/10.1016/j.cose.2021.102387 (Accessed: 7. May 2022).

Van Haastrecht, M. Et al. (2021). A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics*. 10, 2913. Available from: https:// doi.org/10.3390/electronics10232913 (Accessed: 27. April 2022).

Van Haastrecht, M. et al. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied science* 11, 6909. Available from: https://doi.org/ 10.3390/app11156909 (Accessed: 27. April 2022).

Weaver, B. W. et al. (2021). Training Users to Identify Phishing Emails. *Journal of Educational Computing Research* 59(6) pp. 1169-1183. Available from: DOI: 10.1177/0735633121992516 (Accessed: 23. May 2022).

Welch, M. and Jackson, P. R. 2007. Rethinking internal communication: a stakeholder approach. *Corporate Communications: An International Journal* 12(2) pp. 177-198. Available from: DOI 10.1108/13563280710744847 (Accessed: 11. May 2022).

Williams, M. and Moser, T. (2019). The Art of Coding and Thematic Exploration in Qualitative Research. *International Management Review* 15(1). Available from: https://www.proquest.com/docview/2210886420/fulltextPDF/FD18FDAE164E4586PQ/1?accountid=14987 (Accessed: 22. July 2022).

Zainab, B. et al. (2021). Impact of transformational leadership and transparent communication on employee openness to change: mediating role of employee organization trust and moderated role of change-related self-efficiency. *Leadership & Organisation Development Journal* 42(1) pp.1-13. Available from: DOI 10.1108/LODJ-08-2020-0355 (Accessed: 1. August 2022).

Appendices

Appendix 1. Interview Guide

Questions for interview

1. Which position in the business do you have? / What do you work with?

2. What kind of cybersecurity threats do the business face?
    - For example: Ransomware, phishing, confidentiality threats (personal data), integrity threats (financial data, stealing money etc.).

3. What are the practises in the business regarding cybersecurity?
    - For example, changing passwords, update software etc.
        - How often?

4. What kind of attention do you provide for cybersecurity in the day-to-day work?
    - For example: do you have posters around remembering people to look twice if something is suspicious?

5. Has your business, or a business you work with been targeted by a cyberattack?
    - If so, what kind of attack was this?
        - what did you learn?
        - How did this affect the culture of the business? And did you/they change processes after? How?
        - Have you/they noticed any changes in the employee's attitude? Did this increase the awareness? How?
    - If not, what do you think have prevented this from happening?

6. Do you/they offer any training programmes regarding cybersecurity awareness?
    - If so, how have these worked?
        - Have the programs contributed to raising awareness?
        - Have you noticed a change in behaviour after implementing this?
    - If not, have you thought about implementing this?
        - What kind of training programs would you use?
        - What kind of training programs would you suggest?

7. What is the security culture like in the business?
    - What protocols to you use?
        - How do these work?
    - How are the attitudes and norms towards cybersecurity?
        - Do the employees follow the cybersecurity protocols? – password security etc.
        - How are the employees' norms towards cybersecurity, do you know how/if they get influenced to comply with security procedures?

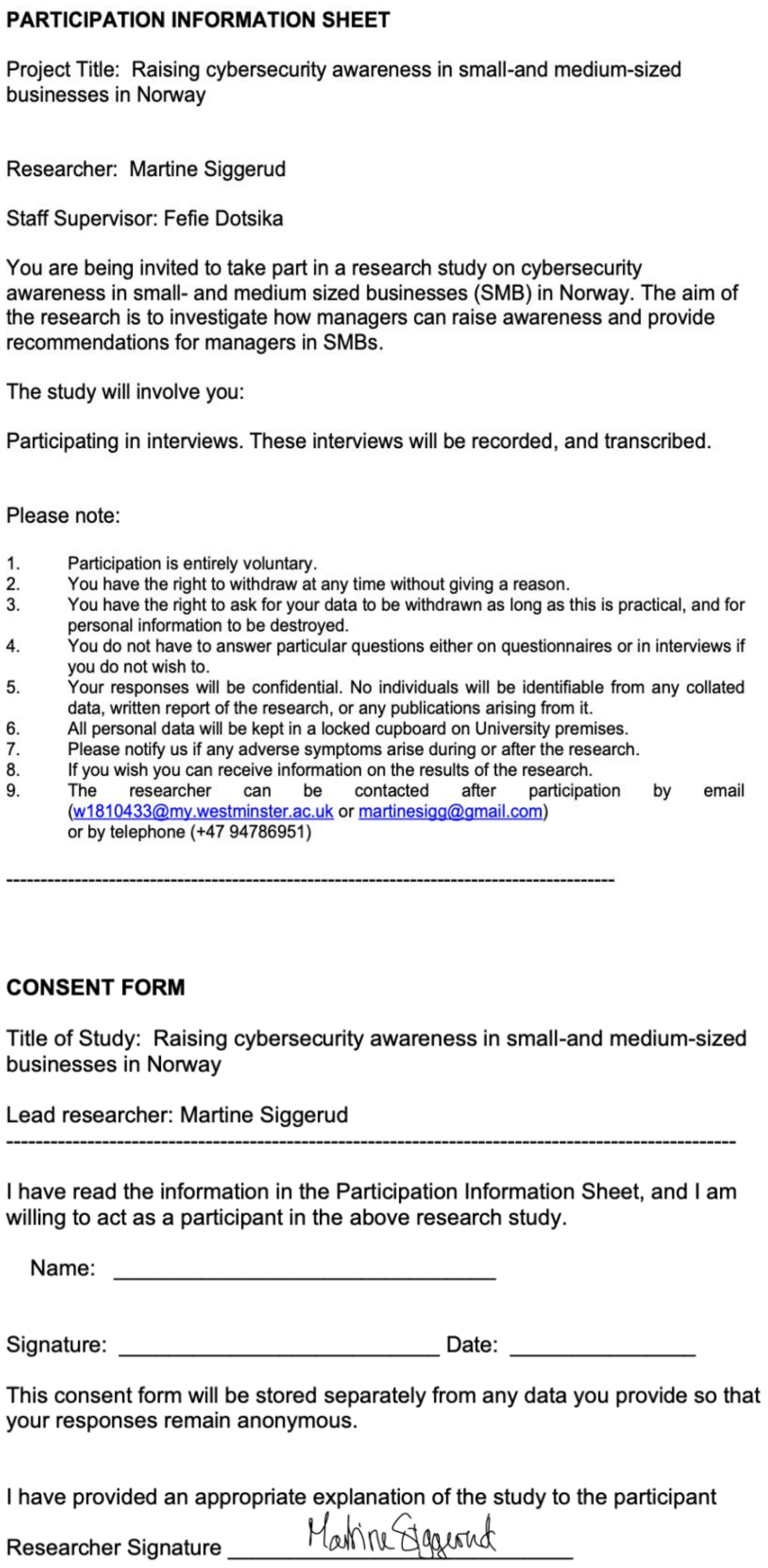
8. How do you communicate with the employees regarding cybersecurity? / How should one communicate?
    - For example, do you /should one offer incentives (rewards) if employees follow protocols?
        - If they do not follow, how do you make the training compulsory? Should one include penalties?
    - How are the relationships between the managers and the employees in the business? Is it hierarchic?
        - How do you think this effect the cybersecurity awareness for the employees?
            - How?

9. How do you think the culture affects the awareness of cybersecurity in the business?

10. What are your recommendations on how managers could increase awareness of cybersecurity in SMBs?

11. Do you have any additional thoughts about this you want to elaborate on?

Appendix 2. Participant information sheet and Consent form



PARTICIPATION INFORMATION SHEET

Project Title: Raising cybersecurity awareness in small-and medium-sized businesses in Norway

Researcher: Martine Siggerud

Staff Supervisor: Fefie Dotsika

You are being invited to take part in a research study on cybersecurity awareness in small- and medium sized businesses (SMB) in Norway. The aim of the research is to investigate how managers can raise awareness and provide recommendations for managers in SMBs.

The study will involve you:

Participating in interviews. These interviews will be recorded, and transcribed.

Please note:

1. Participation is entirely voluntary.
2. You have the right to withdraw at any time without giving a reason.
3. You have the right to ask for your data to be withdrawn as long as this is practical, and for personal information to be destroyed.
4. You do not have to answer particular questions either on questionnaires or in interviews if you do not wish to.
5. Your responses will be confidential. No individuals will be identifiable from any collated data, written report of the research, or any publications arising from it.
6. All personal data will be kept in a locked cupboard on University premises.
7. Please notify us if any adverse symptoms arise during or after the research.
8. If you wish you can receive information on the results of the research.
9. The researcher can be contacted after participation by email (w1810433@my.westminster.ac.uk or martinesigg@gmail.com) or by telephone (+47 94786951)

CONSENT FORM

Title of Study: Raising cybersecurity awareness in small-and medium-sized businesses in Norway

Lead researcher: Martine Siggerud

I have read the information in the Participation Information Sheet, and I am willing to act as a participant in the above research study.

Name: ________________________________

Signature: ___________________________ Date: _______________

This consent form will be stored separately from any data you provide so that your responses remain anonymous.

I have provided an appropriate explanation of the study to the participant

Researcher Signature Martine Siggerud