Investigating Cybersecurity Awareness in SME Organisations

Rune Bråthen &
Eva Kristine Lie

SUPERVISORS
Jaziar Radianti
Paolo Spagnoletti

University of Agder, 2021
Faculty of Social Sciences
Department of Information Systems

Preface

This study was conducted by two students over one semester as the master thesis in the master's degree of Cybersecurity in the Department of Information Systems at the University of Agder. The master thesis was conducted in the time period of January 2021 until June 2021.

The purpose of this study has been to investigate cybersecurity awareness in small to medium-sized organisations. The challenge with this study was the data collection process, where organisations were unwilling to participate in the questionnaire.

We would like to thank our supervisors for their guidance and support through this study. Their feedback and help have been much appreciated and this master thesis would not have been the same without. We would also like to thank the companies that participated and cooperated with us for this study. Their responses on the surveys were an important factor for this master thesis and contributed to more research on cybersecurity awareness.

Lastly, we would like to thank our friends and families for encouraging and motivating words when they were needed.

Kristiansand

4th June 2021

Rune Bråthen   Eva Kristine Lie

Rune Bråthen   Eva Kristine Lie

Abstract

Cyberattack incidents against small to medium-sized enterprises (SMEs) increase nowadays, thus cybersecurity awareness is becoming an important issue to enhance the security of the SME organisations. However, despite the importance of cybersecurity awareness in many organisations including SMEs, such awareness is not yet fully absorbed as day-to-day practice in organisations. In this study, we have investigated cybersecurity awareness in small to medium-sized organisations (SMEs) in Norway. The purpose of this study is to provide knowledge, empirical data and relevant literature about cybersecurity awareness for SMEs that operate with security protocols and policies among their employees. This study tries to answer the following research questions: First, what does cybersecurity situational awareness mean to an employee in a small to medium-sized organisation (SMEs)? Second, what types of behaviours do the SMEs employees perceive as factors that cause cyber incidents in SMEs?

For answering these research questions, we conducted qualitative methods, i.e., a systematic literature review and a survey. The systematic literature review in this thesis used the following digital libraries, i.e., Google scholar database, Scopus library, the ISI library and the EBSCO database. The articles found in the review process have been analysed and sorted based on the findings, consisting of three categories “Meaning”, “Behaviour” and “Knowledge”. The three categories represent different aspects of cybersecurity awareness. We made use of these three concepts further representing the dimensions of cybersecurity awareness, for designing our survey questionnaire. The questionnaire resulted with a total of 21 respondents from several SMEs.

In our survey, 38% of the respondents say that one to five cybersecurity incidents happen a month which highlights the need for cybersecurity awareness in SMEs. The fact that 71% of the respondents answered that less than 20% of all business activities are being used for cybersecurity-related activities seems to suggest that cybersecurity might not be the top priority of SMEs. Our study also suggests that humans as the weakest link can put the organisation at risk by their behaviour regarding passwords and personal devices at the workplace. This is also supported by 39% who agree, strongly agree or neutral, that it is acceptable to connect a private USB into an office/company computer. The implications of this study suggest the need for more focus on cybersecurity awareness among SMEs.

In the “Meaning” category, 83% responded that they think their organisations should provide guidance on cybersecurity. In the “Behaviour” category the use of USB devices and behaviour regarding passwords may put the organisation at risk. In the “Knowledge” part of the questions in the survey, the respondents responded high in relation to their knowledge on viruses, malware, trojans, phishing, ransomware and how to avoid it.

Based on our literature review and the study conducted on the SMEs we have suggested further research in the cybersecurity awareness field. The gap here is the lack of cybersecurity awareness among SME employees and the need for more research as to why this is the case. There could also be more research on how to increase the cybersecurity behaviour among SME employees and why it can lead to cybersecurity incidents.

Table of Contents

List of Tables

List of Figures

1.0 Introduction

In the past years, the number of attacks increased dramatically with an estimated around 60% and even 70% of attacks on small and medium-sized enterprises (SMEs). Unfortunately, more than half of the hacked SMEs are not able to recover and are going bankrupt within 6 months after the attack, (Ponsard & Grandclaudon, 2020). With such dramatic reports, it is in all organisations' interest to look into why this is happening, and how to prevent it from happening. In an increasingly digitized economy, all the world's important institutions depend on “information assets” structured and unstructured information such as customer data, intellectual property, and business plans, as well as on online processes that include everything from customer service to vendor payments. Cyber-attacks compromise information assets to further attackers personal, economic, political or national-strategic objectives, (Kaplan et al. 2015).

1.1 Motivation

Since the threats in the cybersecurity domain increases, Ponsard & Grandclaudon (2020), suggests that there is a great need for more research on cybersecurity and awareness. From different cybersecurity reports, we have seen increased trends of security breaches in organisations (ENISA, 2020; NORSIS, 2020)” and want to uncover more facts on cybersecurity awareness. We consider this is an interesting and relevant topic with the possibility to find literature and empirical data in an important field. We want to find answers to our research questions that can help both management of organisations as well as for further research on the topic. The purpose of this study is to provide knowledge, empirical data and relevant literature about cybersecurity awareness for SMEs that operate with security protocols and policies among their employees.

1.2 Prior Research

Recent security reports show that a significant proportion of cybersecurity breaches are caused by employee noncompliance with organizational information security policies, (Alshaikh, 2020). Ponsard & Grandclaudon and Bal (2019), states it is well known that technological tools alone cannot guarantee the security of an IT system. This also requires collaboration with the employees inside their organisation. Hence, cybersecurity awareness must be considered and tailored for both employees and their organisation.

Even small organisations maintain a mailing service to communicate with employees, clients and stakeholders. Malicious emails can ruin the reputation of an organisation. It is extremely hard for an employee to judge the validity of the emails and to decide whether to click the link or not. Therefore, this ability to decide and differentiate the valid from not valid emails could be supported by appropriate training about information security awareness (Al-Mohannadi et al. 2018).

The challenge is to transform human beings from weak to strong links, becoming a powerful firewall and a solid line of defence in their organisation. We concur with Correandi (2020), that employees' education is the best key to win this challenge.

Information security awareness gives the users more understanding about the importance of the best practice of cybersecurity behaviour (Al-Mohannadi et al. 2018).
Most SMEs seem to have a good and even increased level of awareness. However, when looking at attack statistics, they still fail to make it effective (Ponsard, Grandclaudon, (2019).
Smaller organisations require specific attention because of their lower level of protection, the capability of reaction and recovery while they are increasingly being targeted by cyberattacks. In order to improve their level of cybersecurity and resilience, a first step is to raise awareness, (Ponsard & Grandclaudon, 2020).

1.3 Key Concepts

With awareness, we refer to having knowledge of a certain situation and behaving consequently, (Corradini, 2020).

Shaw et al. (2009) defines awareness as: The degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organisation's data and networks. Situation awareness is a dynamic cognitive process whereby an individual or a group of individuals need to continuously modify and update their situational awareness with new information from the environment, (Rajivan & Cookie, 2017).

Often used with awareness is the cybersecurity concept in today's digital age. Cybersecurity awareness is an approach to enabling a broad, organisation-wide understanding of information security and motivating employees to practice good cyber hygiene to help protect valuable and sensitive information (Lee, 2017).

Promoting cybersecurity awareness is very closely related to the way humans act and react towards the information presented to them, (Zani et al. 2018). In the literature articles the concepts "Meaning", "Behaviour" and "Knowledge" are frequently used, and they represent different aspects of cybersecurity awareness. We will use these dimensions to further investigate cybersecurity awareness.

The explanation of these key concepts is expanded further in Chapter 2.0.

1.4 Research Questions

Despite the importance of cybersecurity awareness in many organisations including SMEs, such awareness is not yet fully absorbed as day-to-day practice in organisations.
Based on the increasing reports of incidents, which also include SMEs, we want to investigate cybersecurity awareness in SMEs. We have defined the following research questions to seek an answer to:

RQ1: What does cybersecurity situational awareness mean to an employee in a small to medium-sized organisation (SME)?

RQ2: What types of behaviours do the SME employees perceive as factors that cause cyber incidents in SMEs?

These two research questions are important in order to get an overview of cybersecurity situational awareness in an organisation. By investigating this we can get a better understanding of cybersecurity awareness among employees, then possibly a direction on how to avoid cybersecurity incidents in the future based on the literature review and the empirical data from our questionnaire.

1.5 Research Strategy

The method used to investigate this topic will be a questionnaire with organisations that are categorized as SMEs as targeted respondents, and a systematic literature review to provide an overview of the existing literature on this topic. The perspective this study will take is the categories based on “Behaviour”, “Meaning” and “Knowledge”. The reason for choosing these three categories is that these three are different dimensions of cybersecurity awareness and should be explored further.

Other related concepts and disciplines that are often linked to cybersecurity awareness such as digital maturity, and technical approaches are not in the focus of this research study.

1.6 Thesis Structure

The rest of the thesis is organized as follows.

Chapter 2 - Theoretical Background
This chapter presents the literature found in the field of cybersecurity awareness through a literature review. This is the most relevant article cited and is based on literature that is state of the art from the previous 10 years. In addition, a detailed table of the study’s screening process and delimitation is included. Lastly, this chapter defines concepts that are used throughout this study.

Chapter 3 - Research Approach
This chapter explains the scientific method used for this study. Furthermore, an overview of the research strategy, and a brief discussion of limitations and potential ethical issues. In addition, an explanation of the research design for finding respondents for the data collection. This chapter

also includes a detailed overview of the data analysis method that was used in this study and an overview of the data quality from the data collection method. This chapter also explains how the research approach was conducted. In addition, how the data collection method in the form of a questionnaire was formed and developed, as well as a detailed insight into how it was distributed for the respondents to access.

Chapter 4 - Results and Findings

This chapter presents the definitions on the different concepts that were used in this paper, and the findings from the literature review that was conducted. The chapter presents the results from the data collection method for this study, the questionnaire, and an overview of the answers from the respondents.

Chapter 5 - Discussion

This chapter forms a discussion based on the theory and literature found in the field of cybersecurity awareness and the findings from the data collection method of a questionnaire and discusses the differences between the two processes.

Chapter 6 - Conclusion and Implications

The chapter concludes based on the previous literature, study and the implications. It also suggests new potential research in the field of cybersecurity awareness.

2.0 Theoretical Background

This chapter presents previous research articles and the literature to get an overview of the existing research in the field and presents the defined concepts that are used in the study.

2.1 Previous research

Reviews of research literature are conducted for a variety of purposes. They include providing a theoretical background for subsequent research; learning of the breadth of research on a topic of interest; or answering practical questions by understanding what existing research has to say on the matter, (Okoli, 2010).

In a study by Renaud & Weir, (2016) it was explored whether Scottish SMEs were taking the cyber threat seriously, and a high percentage confirmed that SMEs were not. Only 15% of the participants had anything close to an accurate perception of their vulnerability to attack. The two-folded reason for this was that communication was fact-based whereas human nature prefers to relate to emotional and experimentally. The other reason was too much advice to SME getting overwhelmed and disagreements between security experts.

Cultivating a cybersecurity culture is regarded as the best approach for addressing the human factors that weaken the cybersecurity chain. It has been found that even users who possess more cybersecurity knowledge can behave no differently from those who lack any form of cybersecurity awareness, (Gcaza & Solms, 2017). The article suggests that cultivating a cybersecurity culture is regarded as the best approach for addressing the human factors that weaken the cybersecurity chain.

In the book by Ponsard & Grandclaudon, (2020), called "Guidelines and Tool support for building a cybersecurity awareness program for SMEs" in the conclusion section; Raising cybersecurity awareness in an organisation is a prerequisite to initiate improvement actions and start building a cybersecurity culture on top of a good knowledge but also with the right attitude and behaviour.

In order to nurture a security-aware culture users should at least have a basic security awareness knowledge and understand the organisational security measures, as specified in the information security policies and instructions, as well as the possible outcomes following their actions. (Zani et al. 2018).

In a literature review by Abd Rahim et al. (2015), called "*A systematic review of approaches to accessing cybersecurity awareness",* 23 studies that matched their criteria were found. The articles were retrieved from the year 2005 to 2014 and seem to be focusing on youngsters and awareness. One of their conclusions was: Categorising users when accessing cybersecurity awareness is deemed essential to ensure the right cybersecurity message is delivered to the right audience, (Abd Rahim et al. 2015). Meanwhile, their study is interesting; it still does not address the organisation's cybersecurity awareness.

In the literature review by Franke & Bryniellson (2014), called "*Cyber situational awareness - a systematic review of the literature*" 102 articles about cyber situational awareness are found. The findings are discussed from the perspective of both national cyber strategies and science. Franke & Bryniellson (2014), says it is evident that some aspects of cyber situational awareness are more mature than others. For example, there is plenty of work dedicated to cyber situational awareness in industrial control systems or general work on algorithms and information fusing in introduction detection systems (IDS).

In the study of Parson et al. (2013), it was checked whether a positive relationship between respondents' knowledge of policy and procedures, attitude towards policy and procedures and their self-reported behaviour when using a work computer. Their results suggest that employers can be relatively confident that improving their employees' knowledge of policy and procedures will have a positive impact on both attitudes towards those policies and procedures and employee behaviour. It also indicates that generic courses that do not attempt to influence attitude and instead simply lecture on knowledge of policy and procedure will be far less effective, (Parson et al. 2013).

According to De Bruijn and Janssen (2017), it has often been stated that humans are the weakest link in the cybersecurity chain. This requires policies to be in place and that people understand what is required, as we know that unawareness on the part of users can introduce further vulnerabilities; for example, by using weak passwords, installing untrustworthy software and using insecure devices and applications. Ignorance, and a limited understanding of what needs to be done, limited awareness of the issue despite its significance and urgency, have resulted in a lack of action, planning and policies. The consequences of this problem not being solved can result in, for example, social engineering, phishing attacks, server attacks, hacking scenarios as well as other human errors and incidents.

Employee's vulnerability is another element of cybersecurity threat appraisal. An employee who perceives high vulnerability to his organisation's information systems will be more willing to take protective actions. (Li et al, 2018).

Corradini (2020) writes about awareness, training and education. Since training contents should be consistent with the current procedures, employees should be informed and educated on security updates. The success of training initiatives is subordinated to employees' partition, to their reactions and their real behaviour change, (Corradini, 2020).

In a study done by Zwilling et al. (2020), results show that respondents are aware of the term "cybersecurity". Therefore, their respondents understand that using the internet may expose them to multiple threats such as violation of privacy, loss of money or data, damage to devices, surveillance of themselves or any organization to which they belong, etc. However, Zwilling et al. also found a discrepancy between respondent attitude and behaviours. Zwilling et al. found that respondents take only basic and insufficient action such as using strong password protection and installing antivirus software. Only a minority engage in more sophisticated protection activities that require a deeper knowledge of cybersecurity, such as avoiding using an open free network, performing computer security audits, or avoiding using public computers. (Zwilling et al. 2020).

Based on the research by He & Zhang (2019), who have compiled recommended guidelines for organisations on cybersecurity awareness. Their study resulted in four points of which they mention; "offer actionable guidelines that interested organizations can use to enhance the performance of their enterprise cybersecurity training and awareness programs."

The four points from this study are as follows; Relating cyber awareness to employees' personal life, Reinforcing security procedures and guidelines, Instilling a "relaxed alert" state of employees, and Minimizing security fatigue for employees. According to He & Zhang (2019), "In order to improve individual employees' cybersecurity behaviour, organizations must develop relevant and engaging cybersecurity training and awareness programs that can motivate their employees to really care about such training and to use their due diligence to stay alert and aware". Therefore, the guidelines they proposed in their study may be a way to resolve this issue.

In a study by Muhirwe & White (2016), cybersecurity awareness was studied in a group of college students, which will be the employees of tomorrow. Their finding was that cybersecurity awareness significantly impacts one's cybersecurity practice, while not effectively predicting one's awareness, cybersecurity training did show a significant relationship to cybersecurity awareness. The study suggests that the college organize cybersecurity awareness events for different students at different levels of the study.

Bada et al. (2019), has a review of literature based on the psychological theories of awareness and behaviour in the area of cybersecurity and considers them to gain insight into the reasons why security-awareness campaigns often fail. Based on these several success factors enhancing the effectiveness of current and future cybersecurity campaigns have been suggested:

1. Security awareness has to be professionally prepared and organised in order to work.
2. Invoking fear in people is not an effective tactic, since it could scare people who can least afford to take a risk.
3. Security education has to be more than providing information to users - it needs to be targeted, actionable, doable and provide feedback.
4. Once people are willing to change, training and continuous feedback are needed to sustain them through the change period.
5. Emphasis is necessary on different cultural contexts and characteristics when creating cybersecurity-awareness campaigns, (Bada et al. 2019).

To help employees recognize and change their computing security behaviour, organizations need to invest in cybersecurity training and awareness programs to encourage their employee's active engagement in complying with their security policies, (He & Zhang 2019). The authors claim if this is not done then security training programs are unlikely to be successful in changing their employee's actual behaviour. A better understanding of the ways in which people learn can help design a personalized learning environment that will enhance people's understanding of cybersecurity.

The result of a study by He et al. (2019), shows that an evidence-based malware report is a relatively better training method in affecting employees' intentions of engaging in recommended cybersecurity behaviours. The conclusion forms around that a lot of cybersecurity awareness training is not effective. He et al. (2019), states that providing employees with security requirements, guidelines and policies is essential. It is implied in the research that the individual employees may have general knowledge about information security but many of them lack experience in dealing with various malware attacks as malware continues to increase in frequency and complexity.

Another topic as a part of cybersecurity awareness is the confidentiality of information. Confidentiality concerns about cybersecurity information have an impact on companies' willingness to share their information, Shojaifar and Fricker (2020). Small and Medium-sized Enterprises (SME) are considered an essential part of the EU economy; however, they are highly vulnerable to cyber-attacks. The article suggests that to mitigate the cybersecurity adoption issues and raise their awareness of cyber threats, a self-paced security assessment and capability improvement method Cybersecurity Coach (CYSEC) has been designed. It is a training method that utilises self-reporting questionnaires to collect companies' information about cybersecurity awareness, practices and vulnerabilities to generate automated recommendations for counselling. Their findings demonstrate that online consent with multiple options for indicating a suitable level of agreement improved motivation for information sharing. This allows many SMEs to participate in security information sharing activities and supports security experts to have a better overview of common vulnerabilities, (Shojaifar and Fricker, 2020).

The Norwegian Center for Information Security (Norsk Senter for Informasjonssikring (NorSIS)) is an independent organisation and partner to the government, business and research facilities in the subject of cybersecurity, (NorSIS, 2021).
NorSIS aids the Norwegian citizenry, business and public sector in creating a safe digital society. We achieve this through building awareness of threats, and vulnerabilities, providing information on specific solutions and influencing good attitudes and information security habits, NorSIS (2021). NorSIS has a yearly survey among Norwegian citizens from age 18 to 74, with questions related to security.
A question in the NorSiS report where people consider digital safety the most important, 15% replied at work, 6% replied at home, and 73% of the respondents said: “equally important at home and at work”.
In a question to whether they are positive to use new technology, 40% replied “partially agree” and 50% replied, “completely agree”.
In a question to where they know what digital safety is, 50% replied “partially agree” and 38% “completely agree”.
The survey also has a question of whether or not the workplace has rules for digital security, where 45% replied “yes”, 8% “no”, 33% “don't have a job” and 14% “don't know”. The questions have been asked over several years and there is very little change from year to year.

In a question by NorSiS (2021, 2) to whether people think they get sufficient information about internet threats 22% replied “partly disagree”, 50% replied “partly agree”, 19% “completely agree”.
Concerning the questions on “Other gets more secure online when my computer or mobile is secure” 38% answered “partially agree”, 38% “completely agree”, 17% “don't know”.
The question “I put myself at risk when I'm using the internet”, 51% of the respondents replied, “partly agree”, 21% “partly disagree” and 19% “completely agree”

The NorSIS (2021) report, is based on a survey on cybersecurity awareness among the Norwegian people, this includes smaller and bigger organisations, and citizens that may not be part of these organisations. It is interesting to see the answers although our questionnaire will be based on SME organisations only, which is more focused than the NorSIS (2021) survey.

The Organisation for Economic Co-operation and Development (OECD) uses the term “Digital Security” instead of “Cybersecurity”. Digital security refers to the economic and social aspects of cybersecurity as opposed to purely technical aspects and those related to criminal law enforcement, national or international security, (OECD). In the report digital security risk management from 2015, OECD operates with eight principles of digital security which are divided into two broad categories.
The first category includes general principles (one to four, see Table 1) addressing all stakeholders, such as governments, public and private organisations and the individuals who directly or indirectly rely on the digital environment for all part of their economic and social activities, (OECD, 2015).

The second group is operational principles (five to eight, see Table 1) addressing more specifically leaders and decision-makers who, due to their highest level of leadership in government and in public and private organisations, are best placed to steer their organisation towards the adoption of an appropriate digital security risk management governance framework, (OECD, 2015).

The eight OECD principles are listed below in table 1:

1.	**Awareness, skills and empowerment**	Awareness raising and skills acquisition to empower stakeholders to manage risk. OECD mentions here the difference between incident and its consequences, the example used is many people are aware that their equipment can be infected by a virus but do not necessarily understand the potential consequences, such as identity theft, financial fraud or theft of trade secrets.
2.	**Responsibility**	All stakeholders should take responsibility for their management of digital security risk, according to their role, the context and their ability to act, (OECD, 2015).
3.	**Human rights and fundamental values**	The measures taken to security can affect the core values of human rights, this demands a responsible approach to managing digital security risk. For example, security can enhance privacy protection and provide anonymity.
4.	**Co-operation**	Cooperation between different organisations or within an organisation can provide useful information in sharing intelligence on threats and vulnerabilities. It also required

		cooperation to transfer skills and knowledge to other employees, strengthening the security.
5.	**Risk assessment and treatment cycle**	Identifying the risks, analysing the risks and the consequences of the risks is an important task to ensure security-related decisions are made. It is about accepting the risk and reducing it to a lower chance of impact, as well as transferring the risk to more specialized units or organisations and avoiding the risk to potentially eliminate it.
6.	**Security Measures**	The security measures implemented may have unwanted effects on other aspects, thus making decisions based on the risk assessment model is preferred. One way to reduce such side effects is to use standards and provide the users with information and provide assistance to the risk assessment.
7.	**Innovation**	By implementing a new or improved product the exposure to security risk can be reduced. This applies to both technological and social processes such as policies and payment systems. By innovating new methods or policies in the risk assessment process, security can be improved and create value.
8.	**Preparedness and continuity**	Digital security risk should include preparedness and continuity plan to define in advance the mechanisms that will reduce risk when incidents occur, by reducing their adverse effects on economic and social activities and enable continuity and resilience of these activities, (OECD, 2015).

Table 1: The eight OECD principles.

Tirumala, Valluri & Babu, (2019), conducted a research on cybersecurity awareness of internet users. A survey questionnaire regarding cybersecurity was distributed among internet user participants, through a reputed organization called InternetNZ. The most crucial part of the survey is assessing the awareness of security concerns and user responsibilities. From the results, it is evident that more awareness needs to be enhanced for a better understanding of various security aspects and their implementation. (Tirumala, Valluri & Babu, 2019).

Based on their survey results involving about 4800 participants, the authors derived the following conclusions:

1. It is necessary to provide practical sessions on various cyber restriction and monitoring tools.
2. A guide on how to install cyber restriction monitoring tools particularly about parental locking, website blocking etc. must be provided.
3. Two-factor authentication must be made mandatory.

4. Clear guidelines on password management have to be provided to internet users as a part of training procedures.
5. Internet users must be provided with clear guidelines on creating strong passwords as well as enforcing stringent rules.
6. Instruction and practical awareness must be provided on various browser-based security and built-in protection options.
7. Awareness must be provided on internet cookies, temporary data, private mode and other security aspects of browsers.
8. Practices are on different search engine restrictions and enforcements must be explained in detail. (Tirumala, Valluri & Babu, 2019).

Summary of the literature review

To conclude this literature review, we believe that there is a small gap in the previous research on the “Knowledge” field. The literature also seems to suggest there's a gap in the lack of cybersecurity awareness among employees (Ponsard & Grandclaudon, 2020, Renaud & Weir, 2016). The category “Knowledge” which we described earlier defines whether or not the employees have the knowledge of certain topics in cybersecurity, - seem to have less previous research. In the category “Meaning” we have seen through the literature review that there also are few cybersecurity awareness guidelines for SMEs to follow. In the category “Behaviour” the literature seems to suggest the employees don't always follow the guidelines (Ponsard & Grandclaudon, 2020, Bada et al. 2019, Zwilling et al. 2020).

This research will improve the knowledge of cybersecurity awareness by providing further research in the categories “Meaning”, “Behaviour” and “Knowledge”. This research will also get a broader view of cybersecurity awareness in general, as well as provide suggestions for further research in the field.

2.2 Concepts

As we have seen different studies in the literature and different usage of the cybersecurity awareness terms, in this section we present the different terms or concepts of words or phrases that are used throughout the research in order to provide a better understanding of the study.

Small to Medium-size organisations (SME)	In Norway the definition of SMEs is up to 100 staff headcounts, The Confederation of Norwegian Enterprise, (NHO). The European Commission defines SME as up to 250 employees, (European Commission, 2003). In this thesis, we adopt the definition of SMEs from the European Commission. This means that all companies that have up to 250 employees are considered SMEs.
Awareness	Here we gradually introduce the concept of awareness, situational awareness and then Cybersecurity and Security awareness. With awareness, we refer to having knowledge of a certain situation and behaving consequently (Corradini, 2020). The National Institute of Standards and Technology (NIST) in the U.S. has a report NIST SP 800-50, NIST SP-800-16 that claims the purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. It is important to recognize that the “awareness” in situation awareness resides neither with the analyst alone, nor with the technology alone, but with the joint human-technology system, (Rajivan & Cookie, 2017).
Situational Awareness	The cognitive side of situational awareness concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to come up with informed decisions. Cognitively it is therefore interesting to measure to what extent a human decision-maker is aware of the situation i.e., has reached a certain level of situational awareness, and how well he/she manages to maintain and develop this awareness as time progresses, (Franke & Brynielsson, 2014). Situation awareness is a dynamic cognitive process whereby an individual or a group of individuals need to continuously modify and update their situational awareness with new information from the environment, (Rajivan & Cookie, 2017). We take cyber situational awareness to be a subset of situational awareness i.e., cyber situational awareness is the part of situational

	awareness which concerns the “cyber” environment. Such situational awareness can be reached e.g., data from IT censors (intrusion detection systems), that can be fed to a data fusion process or to be interpreted directly by the decision-maker, (Franke & Bryniellson, 2014).
Cybersecurity Awareness and Security Awareness	Cybersecurity awareness: An approach to enabling a broad, organisation-wide understanding of information security and motivating employees to practice good cyber hygiene to help protect valuable and sensitive information (Lee, 2017). Although researchers and practitioners exercise ongoing efforts in this area, their work often lacks a concise definition of the term “security awareness”. Since there is no agreement on the term, different (and sometimes not compatible) ways of raising and measuring security awareness exist, (Hänsch & Benenson, 2014). Promoting cybersecurity awareness is very closely related to the way humans act and react towards the information presented to them, (Zani et al. 2018). Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organisation data and networks, (Shaw et al. 2009).

Table 2: Definitions of the main concepts.

The concepts below, “Meaning”, “Behaviour” and “Knowledge” are important parts of the cybersecurity awareness literature. It is three different concepts which focus on three different perspectives. We want to focus on these three aspects of cybersecurity awareness among many concepts. The concepts are defined in the table below.

Meaning	The concept of “Meaning” is intended to find out what the employees think about certain topics such as policies and rules & regulations on cybersecurity awareness. Understanding of the “meaning” concept is important as it will be a lead to whether the employees will follow the organisational policies or not. This is also known as cybersecurity compliance. This topic also includes cybersecurity awareness culture and training.
Behaviour	Human beings are complex, and their behaviour is quite influenced by organisational norms and habits through the pressure of their peers, even despite their knowledge. For example, even if people are

	told to use strong passwords and not reuse them, they may not behave like that, (Ponsard & Grandclaudon, 2020). Attackers often choose the path of least resistance which is mainly the unintentional vulnerabilities created by human factors. As a result, cybersecurity threats that exploit human behaviour are constantly evolving (Abawajy, 2012).
Knowledge	Knowledge is another related concept that forms awareness. We can have knowledge of a certain situation, but we become aware only when we act attentively on the basis of this knowledge. We, therefore, denote with "awareness" something more than just knowledge, considering part of the concept both the cognitive and behavioural components, (Corradini, 2020). There are examples showing how individuals do not always assume safe behaviour despite their knowledge of the risk: people drive without the seatbelt fastened putting a risk to their own safety, even though they probably know the negative consequences. The knowledge part defines if the user/employee has knowledge of a certain topic.

Table 3: Definitions "Meaning", "Behaviour", and "Knowledge".

3.0 Research Methodology

This chapter examines the research methodology and the reasoning behind the choices made in the research approach. The chapter also has information about the data collection strategy and the reasons for the different choices made.
The research approach follows a qualitative methodology, with the qualitative tools available. With the type of study to be conducted with few respondents, the qualitative methodology is best suited.

Qualitative research is a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures, data typically collected in the participant setting, data analysis inductively building from particulars to general themes, and the researcher making interpretation of the meaning of the data, (Creswell, 2009). This study uses a qualitative approach, aided by a survey and systematic literature review method which will be explained further in section 3.2 and section 3.4.

In this chapter, the thesis presents the overall approach and methodology of the study, covering the survey methods and data analysis, as well as the literature review process.

3.1 Research Strategy and Design

In the diagram below we can see the research approach. First, we conducted a broad literature search by examining the relevant journal articles found in library databases, and then conducted the literature review process. The results were used for identifying the research gaps and served as a basis for developing the research method and defining the data collection method. The data collection method was followed by analysing the collected data and presentation of the findings. In the discussion stage, the findings from the questionnaire and the journal articles found in the literature search were brought further for deeper analysis and for gaining insights from the findings. The final step is the conclusion where we derived lessons learned from our findings and explained what impact this study might have. In figure 1 the process is displayed.

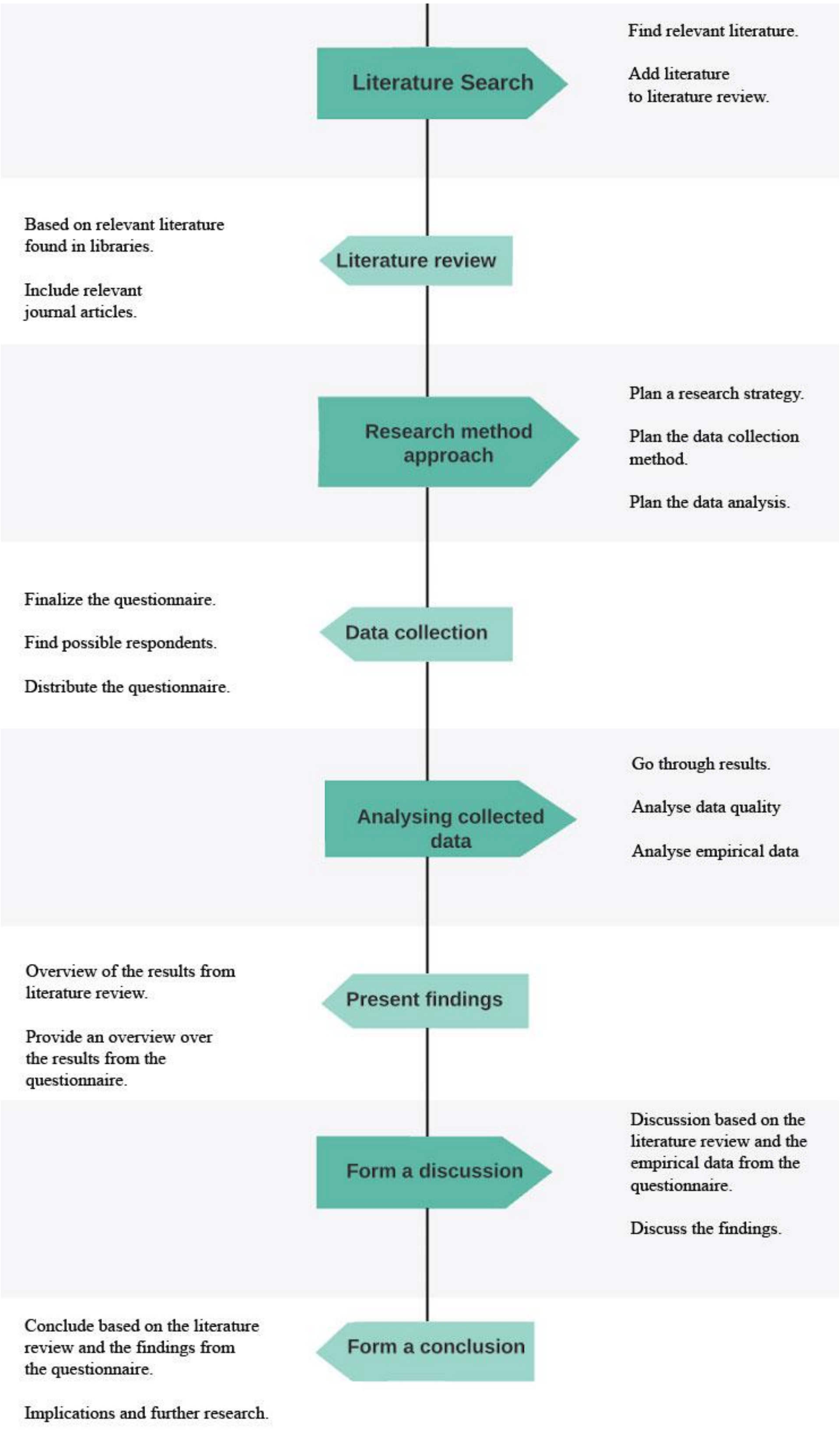
Literature Search
Find relevant literature.
Add literature to literature review.
Literature review
Based on relevant literature found in libraries.
Include relevant journal articles.
Research method approach
Plan a research strategy.
Plan the data collection method.
Plan the data analysis.
Data collection
Finalize the questionnaire.
Find possible respondents.
Distribute the questionnaire.
Analysing collected data
Go through results.
Analyse data quality
Analyse empirical data
Present findings
Overview of the results from literature review.
Provide an overview over the results from the questionnaire.
Form a discussion
Discussion based on the literature review and the empirical data from the questionnaire.
Discuss the findings.
Form a conclusion
Conclude based on the literature review and the findings from the questionnaire.
Implications and further research.

Figure 1: Research Approach.

By determining the research design for this project, it further helped the planning process and deciding the research parameters such as what exactly will be included or excluded in the research process. In addition, it also helped for defining how to collect data, analyse, evaluate the results and finally come to a conclusion, as described earlier.

3.2 Qualitative Questionnaire

In this section and the following sections, we will present an overview of the process of forming a questionnaire for this study. A detailed look into the distribution of the questionnaire to the respondents in addition to the method used to choose and contact organisations for the research approach.

3.2.1 Data Collection

The method used for data collection for this research project will be a questionnaire (Appendix A). According to Creswell (2009), a survey design provides a qualitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population. From sample results, the researcher generalizes or makes claims about the population.

The questionnaire has multiple questions and is also divided into the subjects we would like to look into, “Meaning”, “Behaviour” and “Knowledge” of cybersecurity awareness.
The questionnaire was created after reviewing the literature, with some general and some more specific questions on cybersecurity and awareness in their organisation. The data collection leans toward inductive data collection, where we don't have much theory on the questions we are looking into. There are theories that mention some parts of the questionnaire, but for the main part, it is new territory in this field of research.
The questionnaire is distributed by e-mail and online, where an URL link is provided and sent to the participants to a website that includes the questionnaire. The data from the respondents will be anonymous and handled anonymously, given we did not collect the IP-address, and other personal data. This means we will not differentiate between the organisations’ respondents, thus there is no link between the answers and where the answers come from.

3.2.2 Forming the Questionnaire

The questionnaire (See Appendix A) was developed with a survey tool provided via a partnership with UiA, called SurveyXact. This 3rd party tool allows users to assemble a survey online, the user is free to add as many questions as needed and one can edit the format of the question type. Once all of the questions are added and the format of the questions are as needed, the questionnaire is ready to be distributed to the respondents. Based on the theory from previous research, as well as the categories defined earlier in this paper, “Meaning”,” Behaviour”, and “Knowledge”. We developed a questionnaire that includes 26 questions regarding employees' cybersecurity awareness as well as “Meaning”,” Behaviour”, and “Knowledge” in SME organisations.

3.2.3 Finding Respondents and Distribution of Questionnaire

The ideal respondents for this study are small and medium-sized enterprises (SME), or organisations that operate with security protocols and policies among their employees. The target organisations of our survey could be of any size as long as it is within SME definition related to the headcount, and which might not specifically be into IT or cybersecurity. However, since all organisations need cybersecurity and awareness, the criteria of the respondent were not strict. The topic of cybersecurity awareness is relevant to many employees regardless of the employees’ positions in the organisations, and most if not all SMEs. The intention of the questionnaire was to get answers to the questions relevant to the awareness topics and possibly an idea to further research on this topic.

Cybersecurity awareness is important for the whole SME and all employees should have cybersecurity awareness and a basic understanding of the different cybersecurity challenges and therefore, also be able to answer these questions. The demographic population to answer the questionnaire was not specific in terms of gender or age.

The process of finding and contacting organisations was two-folded. One approach under advisement from our supervisors was to use the university's counsellor to forward the survey request, as well as the intentions of this study, to SMEs that currently are partners with the university. This was an important process to build a trust between the student researchers and the companies. This way, we gained contact with some organisations. Three organisations responded to the email regarding the study's purpose and were willing to cooperate.

The other approach was with the network of Digin where emails were sent to the listed SMEs. The SMEs websites were checked in advance for the number of employees, to meet the SME criteria. During this process, we got in contact with an organisation that could help forward the survey to a number of SMEs.

In order to maintain the anonymity of the respondents, the SMEs would not be named in this report. All organisations are located in Norway but vary in the number of employees. However, all organisations that responded to the questionnaire in this study, qualified to be called SME.

As mentioned earlier, there are no specific ideal respondents for this questionnaire, apart from they must be employed in an SME. Cybersecurity is important for all employees in an organisation. The questionnaire was distributed through e-mail to the organisation's employee or contact points e-mail address, and in some cases forwarded to among their employees. The questionnaire concluded with a total of 21 respondents, in about 40 SMEs.

3.3 Analysis

In this section of research methodology, the methods used for analysing the collected data is presented, in addition to how the data quality from the questionnaire was maintained. In addition, the section with validity and reliability, then thesis limitations and potential ethical issues are discussed.

3.3.1 Data Analysis

The data will be analysed according to qualitative methodology.
Data analysis involves collecting open-ended data, based on asking general questions and developing an analysis from the information supplied by participants, (Creswell, 2009).

After collecting data from the questionnaire, the next step is to do qualitative data analysis. Since the data gathered anonymously, the analysis would aggregate, i.e., on the collection of data are gathered as a whole, and not differentiate various organisations involved in the survey. Since qualitative data analysis focuses on understanding patterns and social context and meaning, we consider this method is best suited for this research. In addition, new information might emerge after the data collection. The data is collected through a questionnaire with multiple choice answers, which will make the interpretation easier to handle than personal opinions in long answers of text.
The survey tool provided by UiA, SurveyXact supports some features for analysis of data that helps the users organising, analysing and presenting the data. With this tool, we are able to choose different data visualisations, such as charts, pie diagrams etc.

3.3.2 Data Quality from Questionnaire

The questions in our questionnaire have been discussed with the supervisors. In order to ensure the right data quality, the question itself is important. Regarding long questionnaires and data quality Andreadis & Kartsounidou, (2020), says long self-administered questionnaires may suffer from lower response rates, higher dropouts, and lower quality responses. A shorter questionnaire reduces the burden of respondents.
With this in mind, the questionnaire created was rather short with only 26 questions which would take 10-15 minutes to answer. We assumed that this would increase the chances of replies and ensured a more specific focus on the different topics in the questions. The questions were open-ended with short answers that were predefined which made it easier to answer, and also to analyse in the alter stage and would make less confusion as opposed to free-text fields. These steps would increase the data quality to a higher level. The number of responses is also important to ensure a broader variance in the data collected. Thus, the survey was sent to multiple SMEs with a total of over 400 possible respondents, and still within the SME definition. The same survey was sent to all identified organisations, with no changes to the survey, to ensure data collection was consistent.

3.3.3 Validity and Reliability

Concerning the reliability and validity issues, Creswell, (2009) says that although validation of findings occurs throughout the steps in the process of research, this discussion focuses on enabling a researcher to write a passage into a proposal on the procedures for validating the findings that will be undertaken in a study.

Qualitative validity means the researcher checks for the accuracy of the findings by employing certain procedures, while qualitative reliability indicates that the researcher's approach is consistent across different researchers and different projects, (Creswell, 2009).

Creswell suggests eight different validity strategies, where one of the points suggests using an external auditor to review the entire project.
Creswell (2009), says as distinct from a peer debriefer, engaging a person that is not familiar with the researcher or the project and can provide an objective assessment of the project throughout the process of research, or at the conclusion of the study.

The empirical data in our report have been cross-checked with the data on the SurveyXact tool, to ensure there are no obvious mistakes during transition from questionnaire data. The data is also checked by both authors from this thesis to ensure consistency. In addition, the thesis itself has been reviewed both by the authors, in addition to the supervisors to ensure high quality.

3.3.4 Challenges and Potential Ethical Issues

The challenge of this study could stem from organisations/subject of this study that are not comfortable with a public study on cybersecurity that seems to evaluate their organisation. This can both be a challenge to get adequate response for this study and the willingness to allow sharing openly the findings of our study. There is always a possibility to have the research classified, but it would create quite a lot of extra work following the guidelines that apply. Other ethical aspects can also be on the individual that replies to a survey or interview, they might have mixed feelings about the questions they answer, if it will open their personal information, or being identifiable. A research study is dependent on honest answers and the respondents might be reluctant to answer for fear of repercussions.

To anticipate these challenges, we have gone through the data settings for which Personal Identifiable Information, (PII) we collected and kept this at a minimum, such as the survey did not collect names, e-mail addresses or other PIIs in the study. The legal aspects might be challenged depending on the organisation chosen to reply to the questionnaire as the data possessed might be of personal value. The European GDPR has defined rules on privacy and needs to be followed in a research study. The Norwegian Center for Research Data, (NSD) has approved scientific specifications and the data collection in our study.

Another limitation to our study is also the deadline to conduct a literature review and a data collection with multiple SME organisations. The scope is defined in advance to reach the goal of doing both, however, the literature on the field of cybersecurity awareness is quite wide. Further narrowing of the scope and goal for the literature review and research questions has been defined in detail.
The data gathered from questionnaires were of a small sample size and might not be significant in terms of statistical significance, this is another limitation for this study due to the number of the responses of our survey were relatively low. This can limit the generalizability of the study. However, for explorative purpose, the number of responses is somehow acceptable.

3.4 Literature Review

This thesis also applied a systematic literature review (SLR) approach. In this subchapter, we explain how the SLR was done. The publications we found through the literature review are mainly from the Google Scholar database as well as the library databases such as Scopus, the ISI library and the EBSCO database. Other relevant publications and articles have been identified by exploring the reference list in relevant literature from the early literature review stages.

A literature review creates a foundation for the study and to further build upon. By conducting a literature review, one can better understand and be familiarised with the most relevant research on the topic, which is in our case about cybersecurity awareness in organisations.
The qualitative literature review views the results of relevant studies and provides a summary of the articles. In order to review the research that has been done on this topic, a VPN connection to the university has been used. This has been beneficial for accessing publications from the wide collaboration that the University of Agder has with other Universities around the world. UiA also has access to articles in other library databases, such as the findings on Google Scholar, and subscribes to other library databases, which means that more articles are found in our searches. The timing of the literature review is of importance as well, as Okoli, (2010), says we believe that a comprehensive literature review should include all available evidence as to at the time that the article is at least submitted for publication. So, the literature review has been conducted a few times to check if any new literature articles have been added. The findings from the review are presented in the results chapter of this study, “4.1 Findings from the literature review”.

3.4.1 Screening Process and Delimitation

We focus on articles that mention cybersecurity awareness, *meaning*, *behaviour* or *knowledge*. However, if our search resulted in articles about cybersecurity, but were not specifically discussing the topic in the context of awareness, would not fit into our specifications and were discarded.

Presented below, in Table 4, listing the criteria for the literature search.

Search Library	Scopus library, Google Scholar, ISI and EBSCO
Keywords	● Cybersecurity Awareness OR Cyber Security Awareness. ● Cybersecurity situational awareness OR Cyber Security Situational Awareness. ● SME OR Small to Medium Enterprises.
Subject Areas	Meaning, Behaviour, Knowledge
Total articles	27 articles reviewed in the thesis.
Language	English
Inclusion	● Scientifically published papers with proper citations and found

	in library databases. ● Articles published between 2010-2021 to cover the most state of the art articles. ● Only journal articles. ● Only English written publications.
Exclusion	● Outdated publications from before the year 2010. ● Articles about cybersecurity that are not linked to awareness.

Table 4: Literature review criteria for research and inclusion/exclusion.

Library databases	**Description**
Scopus	Abstract and citation database, allows saving search phrases.
Google Scholar	Free accessible search engine for indexed articles.
ISI	Subscription based access to multiple databases.
EBSCO	Fee based online research service.

Table 5: Library databases for journal articles.

The journal articles found in the search will form the theory used, as seen in Chapter 2.0 “Theoretical Background”, where the literature is presented. The literature will also be used in the discussion chapter to discuss the findings with our questionnaire results. The purpose of this is to form a conclusion based on the literature and the questionnaire results.

4.0 Results/findings

This chapter will present the results from multiple processes that have been conducted for this study. The findings from the literature in this field on cybersecurity are listed in tables. Both the results from the theoretical background and the results from the literature review are placed under the categories of either “Meaning”, “Behaviour”, “Knowledge” or “General” in a cybersecurity awareness view. By placing the literature articles in these categories, one can better understand and gain control over the whole picture. In order to get an overview of the existing literature in the field of cybersecurity awareness, and to see what areas might be lacking in specific research.
In addition, the chapter also presents the results of the data collection method of questionnaires as well.

4.1 Findings from the Literature Review

The findings from Chapter 2.0, “Theoretical Background” in this paper, consists of both definitions and theory in the selected categories such as “Meaning”,” Behaviour”, and “Knowledge” as well as “General” articles about cybersecurity awareness. In the table 6 are the journal articles found from the literature review as well as the journal articles from the concepts research used in Chapter 2.0 “Theoretical Background”.

Article author(s)	**Behaviour**	**Meaning**	**Knowledge**	**General**
Abawajy, (2012)	**x**			
Abd Rahim et al. (2015)				**x**
Bada et al. (2019)	**x**			
Corradini, (2020)	**x**		**x**	
De Bruijn and Janssen, (2017)				**x**
European Commission, (2003)				(SME definition)
Franke & Bryniellson, (2014)				**x**
Gcaza & Solms, (2017)		**x**	**x**	
Hänsch & Benenson, (2014)				**x**
He et al. (2019)	**x**		**x**	
He & Zhang, (2019		**x**		
Lee, (2017)				**x**

Li et al. (2018)		**x**		**x**
Muhirwe & White, (2016)		**x**		**x**
NIST SP 800-50, NIST SP-800-16				**x**
NorSIS, (2021)				**x**
The Confederation of Norwegian Enterprise, (NHO)				(SME definition)
OECD, (2015)				**x**
Parson et al. (2013)	**x**	**x**		
Ponsard & Grandclaudon, (2020)		**x**		**x**
Renaud & Weir, (2016)				**x**
Rajivan & Cookie, (2017)				**x**
Shaw et al. (2009)				**x**
Shojaifar and Fricker, (2020)				**x**
Tirumala, Valluri & Babu, (2019)				**x**
Zani et al. (2018)		**x**		**x**
Zwilling et al. (2020)	**x**		**x**	

Table 6: Findings from the literature and the main concepts used in this study.

4.2 Results from Questionnaire

This section of the thesis will present the results from the questionnaire.

Summary of major findings
In our survey, 38% of the respondents say that one to five cybersecurity incidents happen per month, which highlights the need for cybersecurity awareness in SMEs. The cybersecurity activities were considered to be less than 20% of all business activities which seem to indicate a lack of focus on cybersecurity activities.

In the “Meaning” category, nearly 62% strongly agree that the company should provide guidelines on cybersecurity. 90% strongly agree or agree that company should show how to comply with laws and regulations for security.
In the “Behaviour” category 24% of the responses showed that they were either neutral or

strongly agree that it is ok to share passwords with others. Question number 19 showed that as much as 38% agree or strongly agree that it is ok to use a personal device such as a phone, tablet or computer at work.
The “Knowledge” category showed that the respondents seem to have high knowledge of cybersecurity, i.e., 95% strongly agree or agree that they can identify an email scam and avoid it. 90% strongly agree or agree that viruses, malware and Trojans can spread from email attachments. 76% strongly agree or agree that they know what phishing is and how to avoid it. 66% strongly agree or agree that they know what ransomware is and how to avoid it.

Below are tables and diagrams based on the results of the questionnaire. Questions one to five are categorised as “General Questions”, questions six to eight are categorised as “Meaning”, nine to nineteen are under “Behaviour”, and twenty to twenty-six are under the “Knowledge” category. See Appendix B for the specific answers to the questionnaire in its entirety.

We can see in Table 7, presenting the results from question one where the majority, (81%) of the respondents are full-time employees. Figure 2 illustrates the results from question one.

1 - What is your position within the company?		
Full time employee	17	81%
Part time employee	-	-
Partner	3	14%
Other	1	5%

Table 7: Questionnaire results for "General Questions", question one.

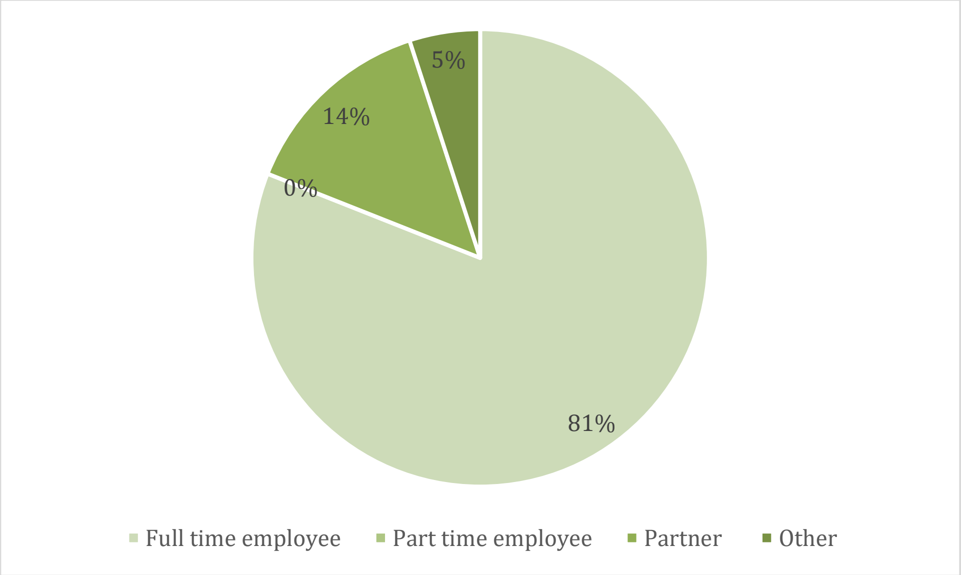

Figure 2: Diagram of questionnaire results for "General Questions", question one.

Table 8, presenting question two, “How does your company tackle the cybersecurity aspect” we can see the answers vary, with the most answers in “A part of IT job” (52%). Figure 3 illustrates the results from question two.

2 – How does your company tackle the cybersecurity aspect?		
The company has a dedicated security team	4	19%
The company has one-two staffs that handles security	6	29%
A part of IT job	11	52%
Outsourced to the third party	3	14%
I do not know	3	14%
Other	1	5%

Table 8: Questionnaire results for “General Questions”, question two.

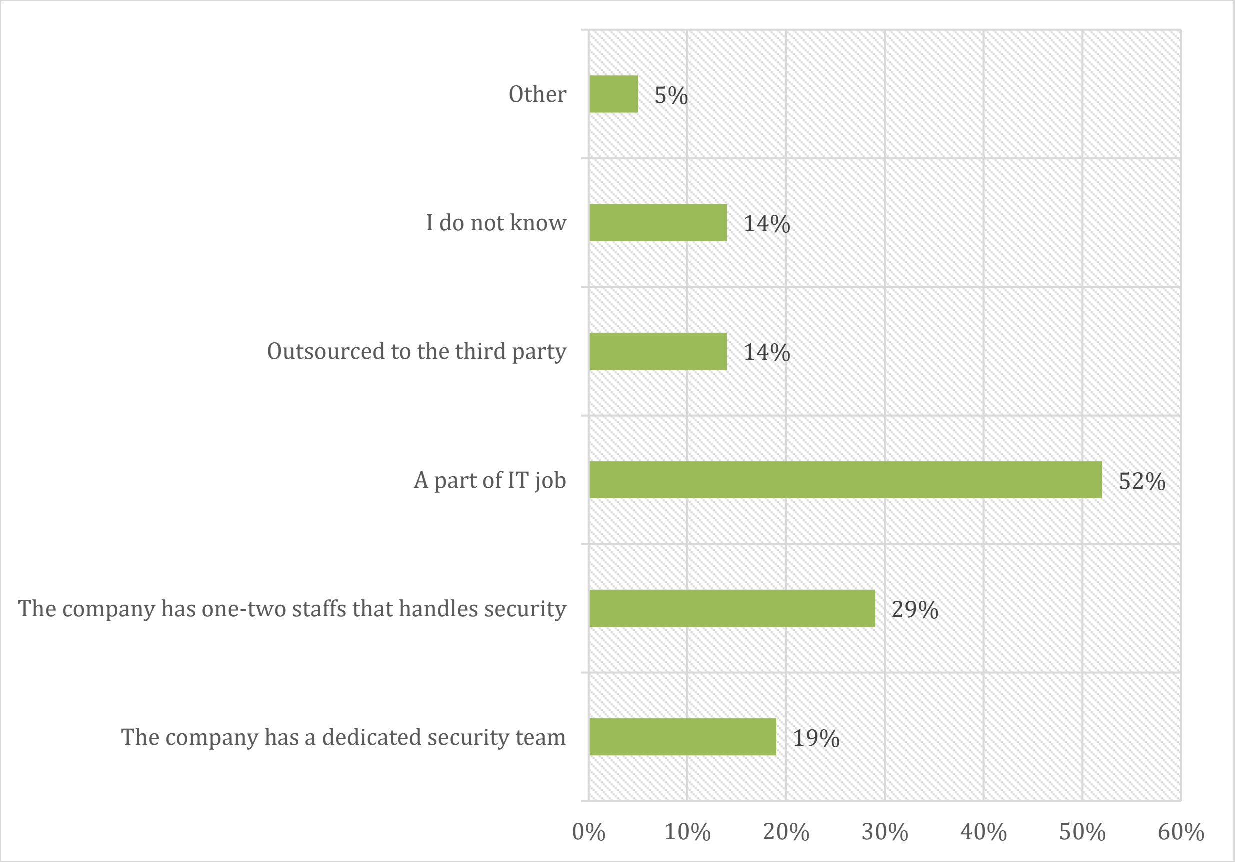

Figure 3:Diagram of questionnaire results for “General Questions”, question two.

As we can see in Table 9, presenting question three, “How much of all business activities in your company are being used for security-related activities” most of the respondents (71%) answered “Low. Less than 20% of all business activities”. Figure 4 illustrates the results from question three.

3 - How much of all business activities in your company are being used for security-related activities?		
Low. Less than 20% of all business activities.	15	71%
Medium. 20-30% of all business activities.	4	19%
Top priority. More than 30% of all business activities.	2	10%

Table 9: Questionnaire results for "General Questions", question three.

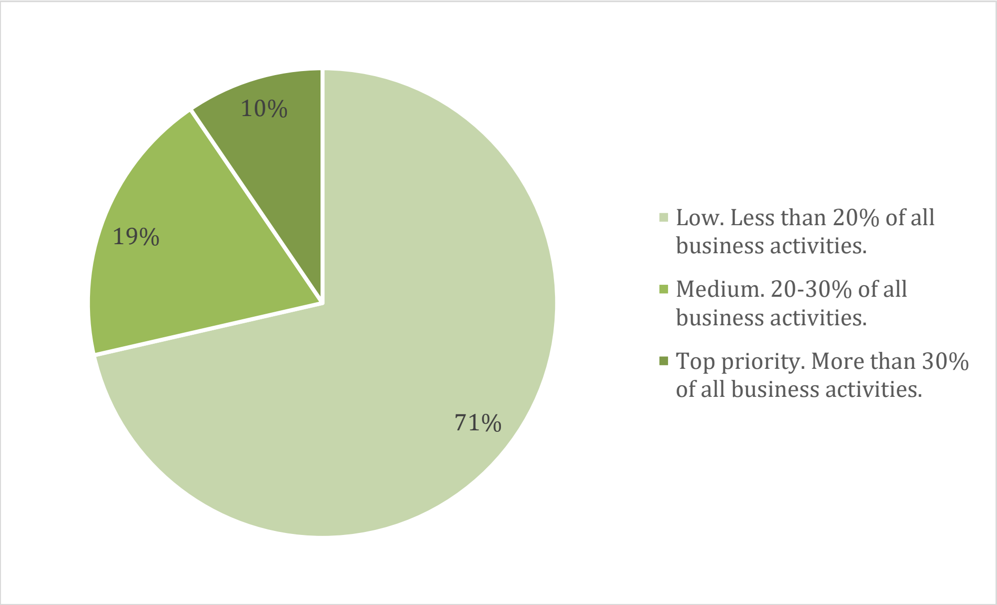

Figure 4: Diagram of questionnaire results for "General Questions", question three.

In Table 10, presenting question four, “How often does a cybersecurity incident occur in your company”. The answers vary from “1-5 times per month.”, “never register incidents” and “I don’t know”. However, most answers are received for “1-5 times per month” with 38%. Figure 5 illustrates the results for question four.

4 - How often does a cybersecurity incident occur in your company?		
1-5 times per month.	8	38%
5-10 times per month.	-	-
More than 10 times per month.	-	-
Never register incidents.	7	33%
I do not know.	6	29%

Table 10: Questionnaire results for "General Questions", question four.

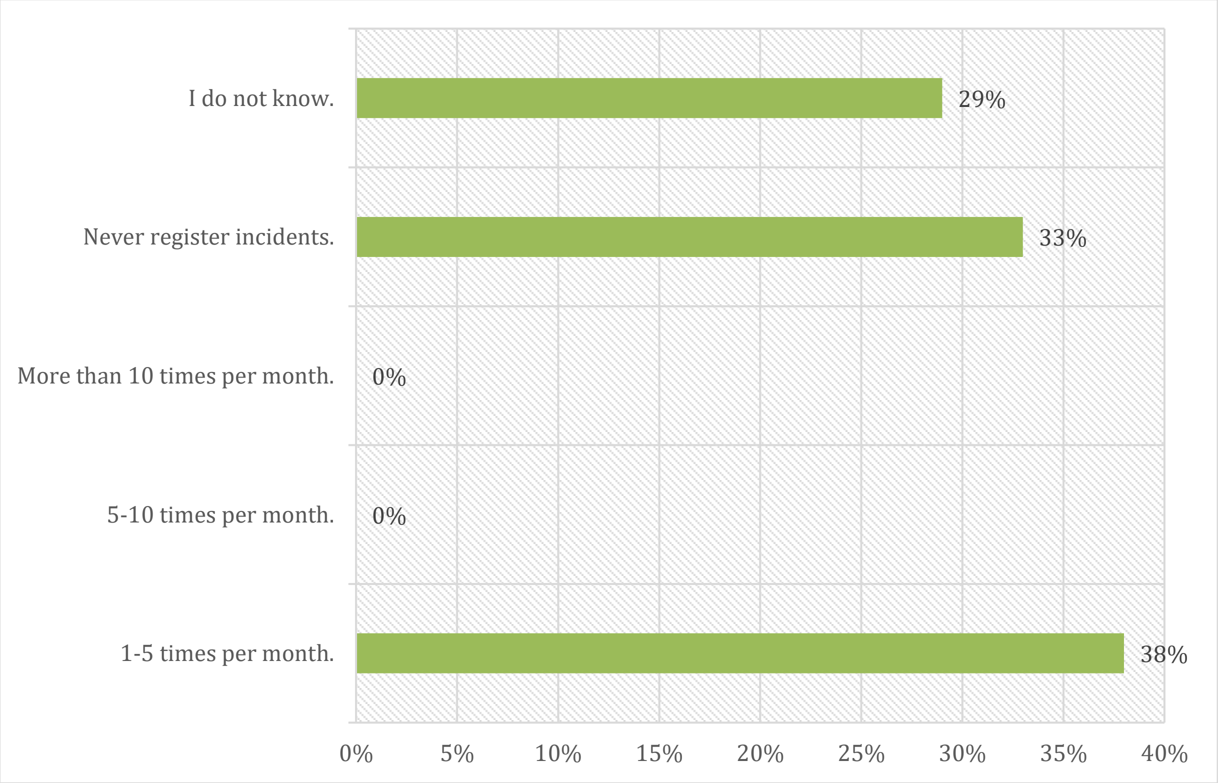

Figure 5: Diagram of questionnaire results for "General Questions", question four.

In Table 11, presenting question five “What kind of online systems are used in your company?”. Here the respondents had the option to select multiple answers. However, all respondents answered, “E-mail for organization and companies”, the majority had “Website, blog” and about half of respondents answered “Social media accounts” in their company. Figure 6 illustrates the results for question five.

5 - What kind of online systems are used in your company? (Possible to select multiple answers)		
E-mail for organisations and companies.	21	100%
Website, blog.	15	71%
Online bank accounts.	10	48%
Personal information of customers stored electronically.	9	43%
Social media accounts.	12	57%
Online order, booking and payment.	6	29%
Industrial control system.	4	19%
Other.	3	14%

Table 11: Questionnaire result for "General Questions", question five.

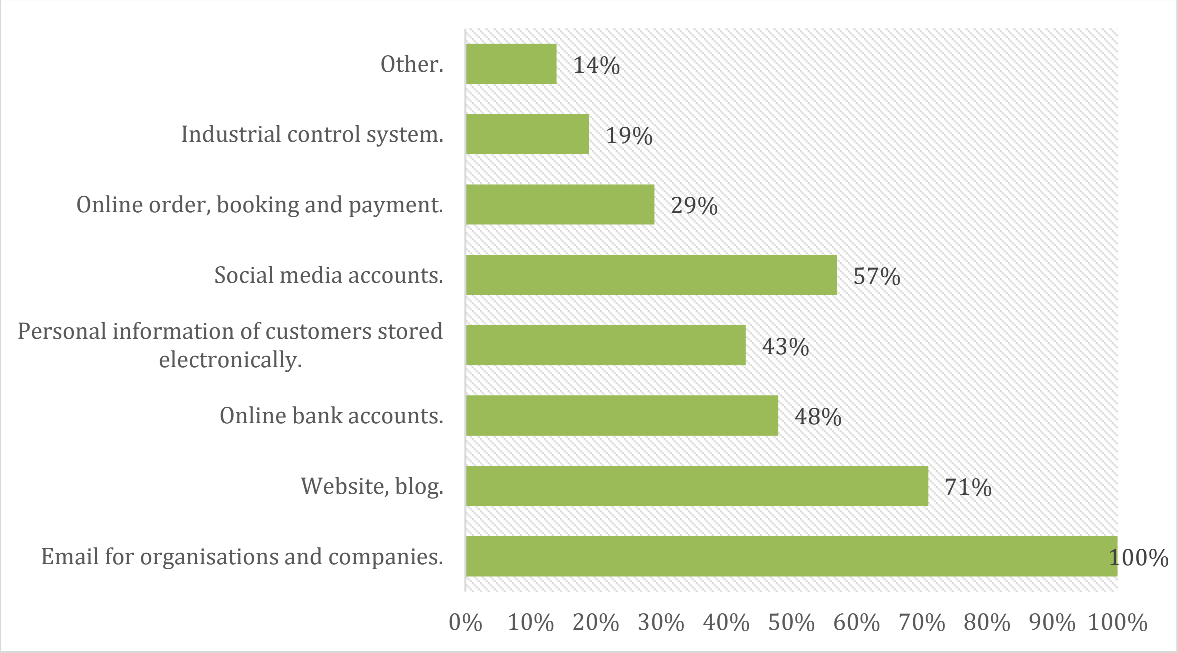

Figure 6: Diagram of questionnaire results for "General Questions", question five.

In the category “Meaning” most respondents think “the company should provide guidance on cybersecurity”. In addition, the respondents also think “the company should comply with laws and regulations for security”. In Table 12, from the “Meaning” category the results are presented. Figure 7 provides an illustrated view.

	Meaning – Questions 6-8					
	Questions	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
6	The company should provide guidance on cybersecurity.	61,9 %	23,8 %	4,8 %	4,8 %	4,8 %
7	The company should show how to comply with laws and regulations for security	52,4 %	38,1 %	-	9,5 %	-
8	The company has security newsletters, briefings or meetings about security	23,8 %	28,6 %	33,3 %	-	14,3 %

Table 12: Questionnaire results for "Meaning".

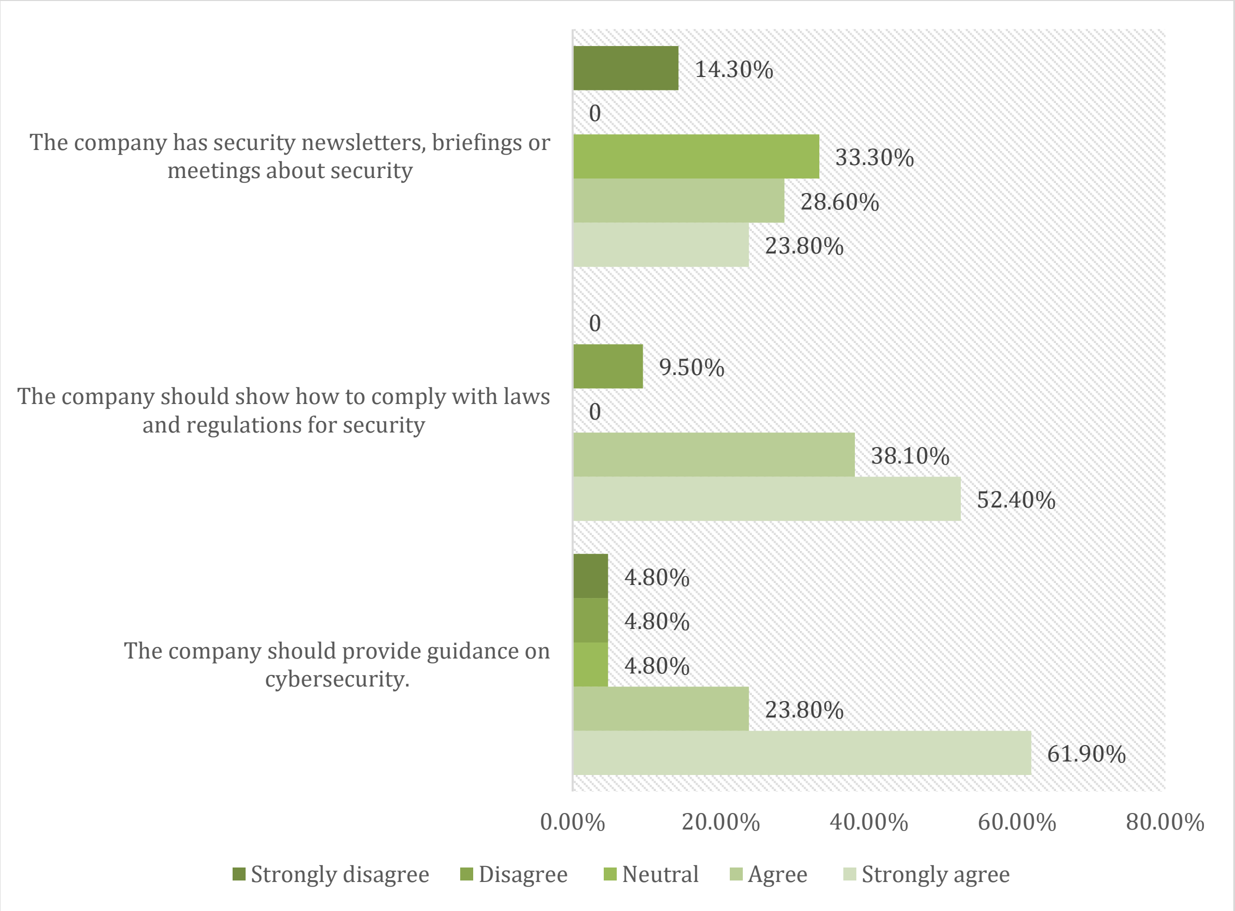

Figure 7: Diagram of questionnaire results for "Meaning".

In the category “Behaviour” are questions about the use of private USB devices and behaviour regarding sharing passwords and using personal devices (phones, tablets, computers). In Table 13, the results based on the “Behaviour” category are presented. Figure 8 provides an illustrated view of the results.

	Behaviour – Questions 9-19					
	Questions	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
9	It is ok to share passwords with others.	4,8 %	-	19 %	14,3 %	61,9 %
10	It is ok to open carelessly every email attachment.	-	4,8 %	4,8 %	-	90,5 %
11	It is ok to easily trust an email that you believe looks legitimate.	4,8 %	-	14,3 %	23,8 %	57,1 %
12	It is ok to connect private USB into an office/company computer.	4,8 %	4,8 %	28,6 %	38,1 %	23,8 %
13	Updating computers/software is necessary to maintain security.	66,7 %	23,8 %	9,5 %	-	-
14	Backups are necessary to maintain security.	76,2 %	19 %	4,8 %	-	-
15	It is ok to visit illegitimate websites.	-	-	4,8 %	38,1 %	57,1 %
16	It is ok to never change passwords.	-	4,8 %	19 %	14,3 %	61,9 %
17	It is ok to use weak passwords (no numbers, uppercase, words etc.).	-	-	-	38,1 %	61,9 %
18	It is ok to use the same password for multiple websites and social media.	-	-	-	71,4 %	28,6 %
19	It is ok to use personal devices (phone, tablet, computer) at the office.	4,8 %	33,3 %	38,1 %	9,5 %	14,3 %

Table 13: Questionnaire results for "Behaviour".

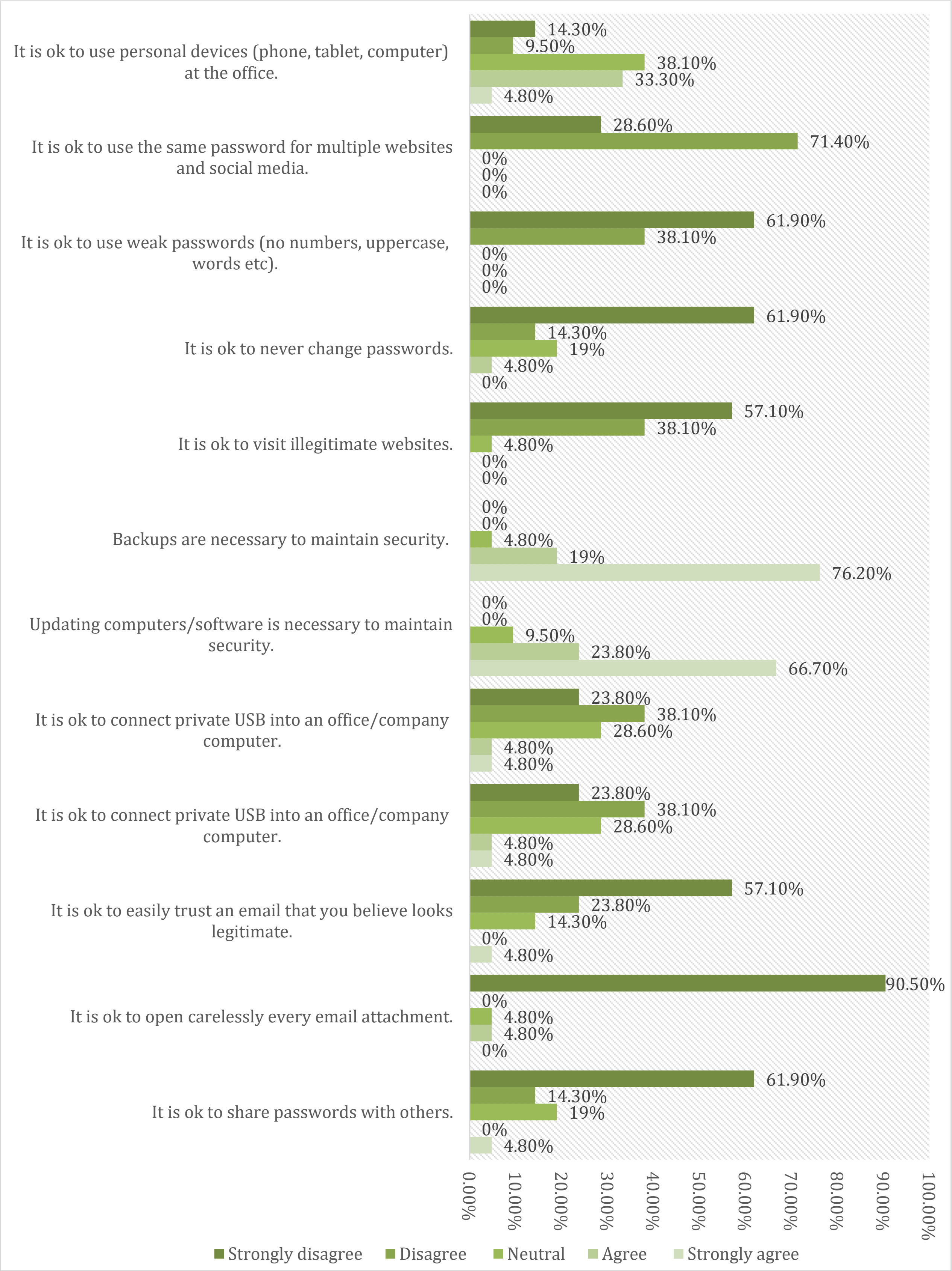

Figure 8: Diagram of questionnaire results for "Behaviour".

In the “Knowledge” category of the questions in the survey, the respondents responded high in relation to their knowledge on viruses, malware, trojans, phishing, ransomware and how to avoid it. In Table 14 below are the results from the “Knowledge” category. Figure 9 provides an illustrated view of the results.

	Knowledge – Questions 20-26					
	Questions	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
20	Virus, malware and Trojans can spread from email attachments.	61,9 %	28,6 %	4,8 %	-	4,8 %
21	Virus, malware and Trojans can spread when clicking on an insecure link on a website.	52,4 %	33,3 %	9,5 %	4,8 %	-
22	I know what phishing is and how to avoid it	57,1 %	19 %	23,8 %	-	-
23	I know what email scams are and how to avoid it	71,4 %	23,8 %	4,8 %	-	-
24	I know what ransomware is and how to avoid it.	38,1 %	28,6 %	28,6 %	4,8 %	-
25	I know what GDPR is.	52,4 %	42,9 %	4,8 %	-	-
26	I know how to support my company by following GDPR and to avoid fines because of data breaches.	33,3 %	47,6 %	14,3 %	4,8 %	-

Table 14: Questionnaire results for "Knowledge".

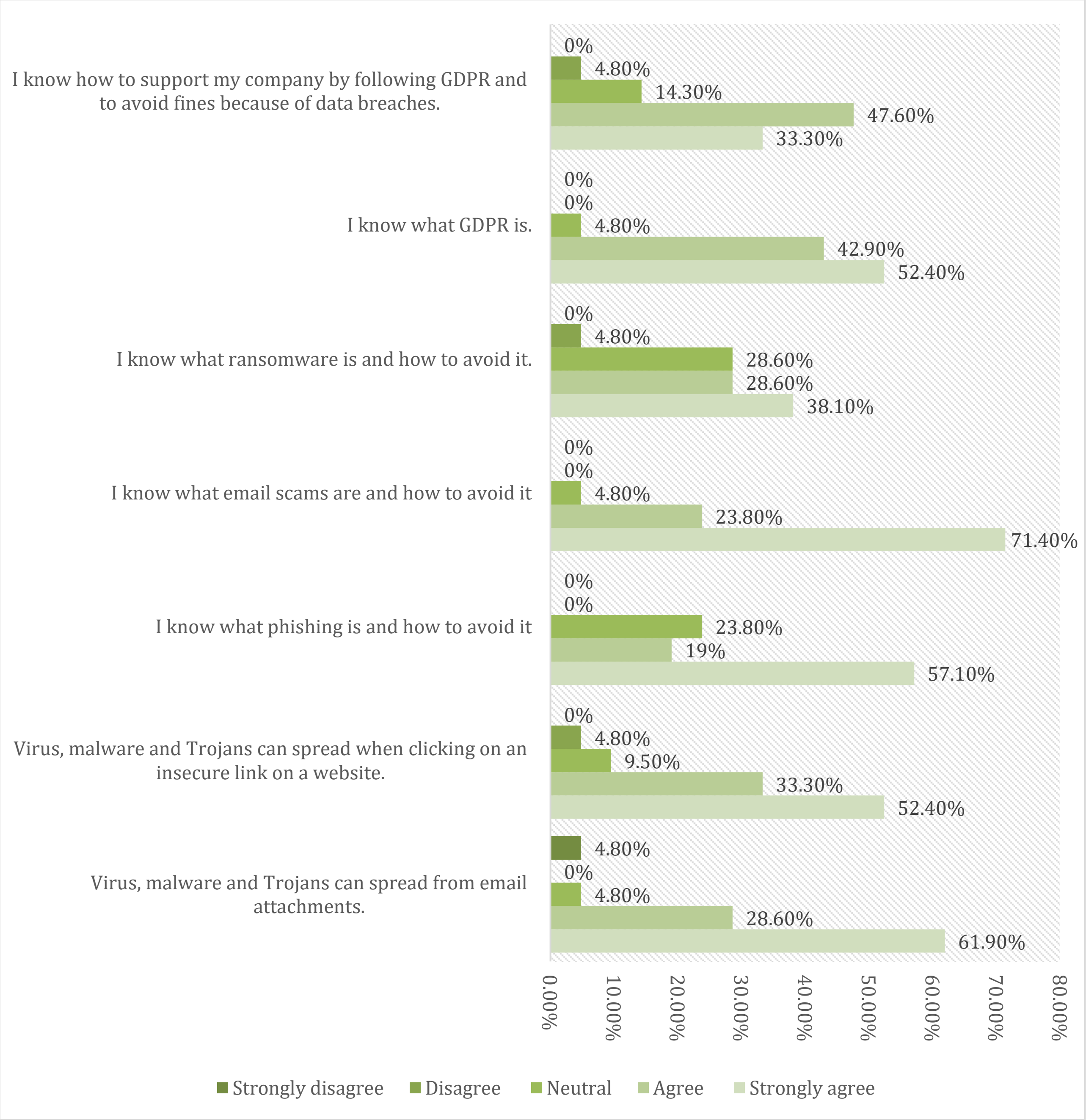

Figure 9: Diagram of questionnaire results for "Knowledge".

5.0 Discussion

In this chapter, we discuss the results of our survey in light of the findings of previous works.

By having a good culture for cybersecurity, SMEs can be more resilient towards attacks. This includes raising cybersecurity awareness in the organisation. The study of Li et al, (2018) says that when employees are aware of their company information security policy and procedures, they are more competent to manage cybersecurity tasks than those who are not aware of their company's cybersecurity policies.
This is in line with this study conducted where the results show that 62% of the respondents strongly agree that the company should provide cybersecurity guidelines as we can see in Figure 10.

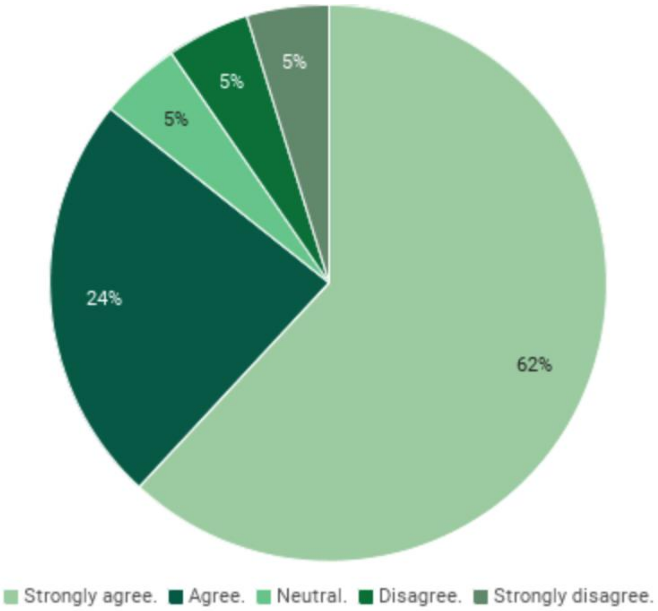

Figure 10: Pie chart of questionnaire result ("The company should provide cybersecurity guidelines.")

This is in line with the studies of NorSiS where they have a question of whether the workplace has rules for digital security or not, where 45% replied "yes", 8% "no", 33% "don't have a job" and 14% "don't know".

In the study by Renaud & Weir (2016) describing the cybersecurity risks in SME, a key solution in helping SMEs is to help them understand the main concept of cybersecurity. SMEs assets are usually under threat of cyberattacks such as data breach, destruction of data, and refusal of access to data, which probably affect several of the business activities negatively. Yet many signs indicate that SMEs underestimate cyber threats by not using efficient security measures.

The result from this study shows in Figure 11, that 52,4 % of the respondents strongly agree, as well as the 38,1% that agree that "the company should show how to comply with laws and regulations for security". By doing so, the concerning percentage of respondents who answered the question “How often does a cybersecurity incident occur in your company?”, as shown in Figure 12, would be lower than the result of 38% for 1-5 times per month.

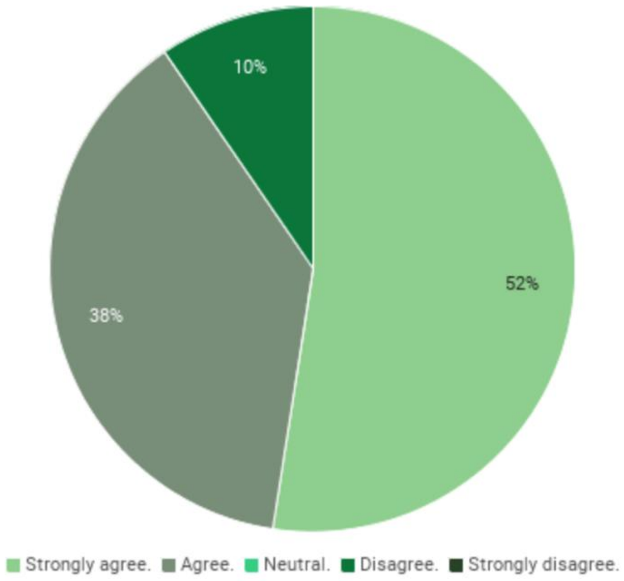

Figure 11: Pie chart of questionnaire result ("The company should show how to comply with laws and regulations for security.")

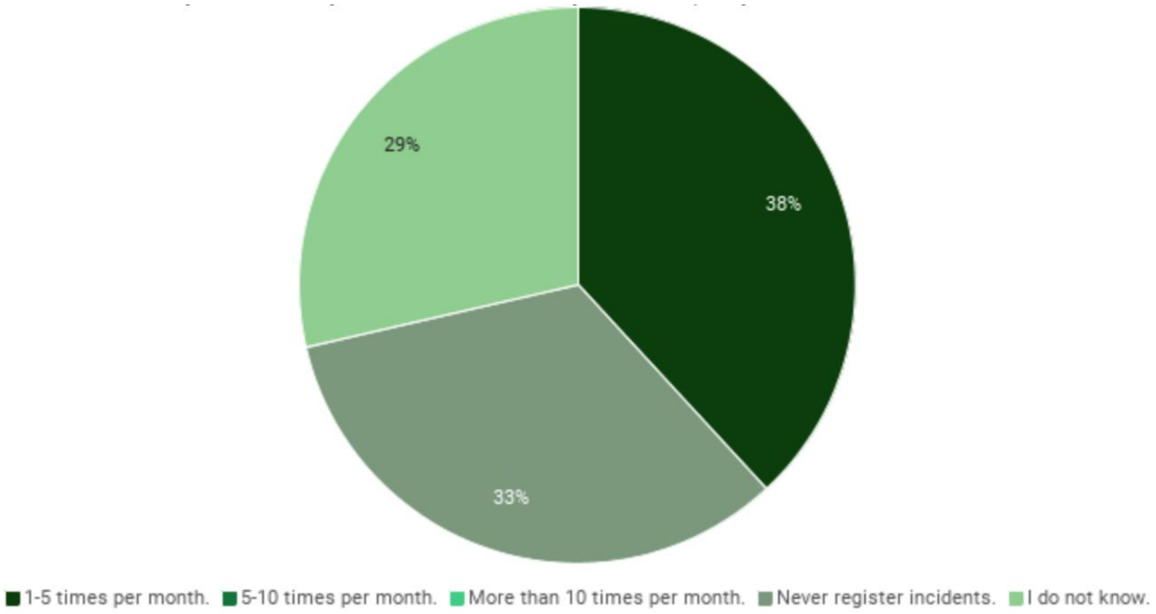

Figure 12: Pie chart of questionnaire result (“How often does a cybersecurity incident occur in your company?”)

In addition, when asked “How much of all business activities in your company are being used for security-related activities?”, as shown in Figure 13, 71% of the respondents answered, “low, less than 20% of all business activities.” This is in line with the studies of Ponsard & Grandclaudon, (2020) where the first step in SME cybersecurity is to raise awareness of cybersecurity, the fact that 71% of all respondents used less than 20% of their business activities on cybersecurity suggest that there is a need to raise awareness.

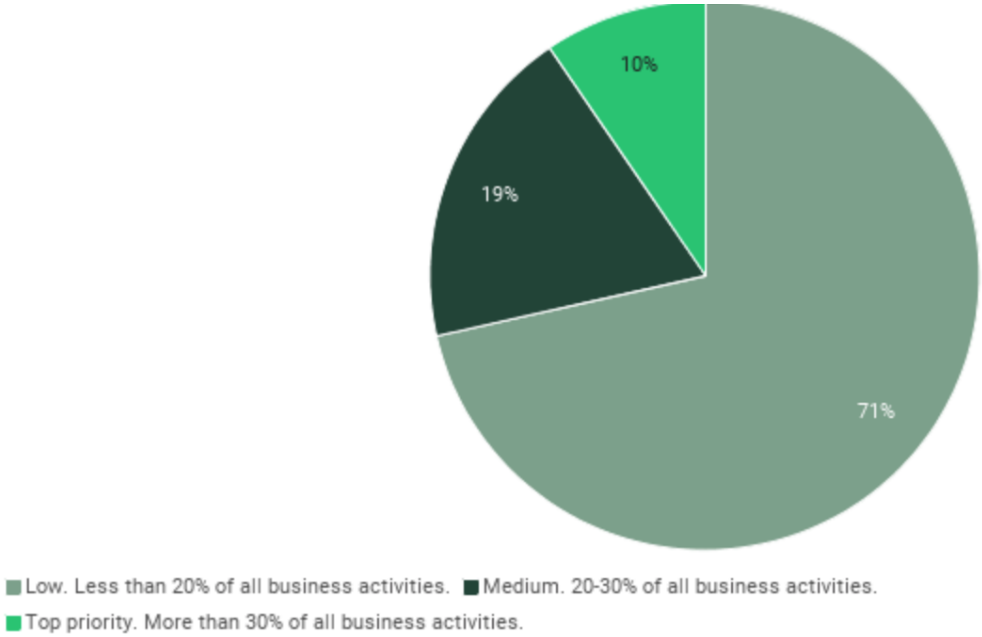

Figure 13: Pie chart of questionnaire result (“How much of all business activities in your company are being used for security-related activities?”)

Even if the SMEs have implemented security measures the employees have to follow them. As pointed out by Gcaza & Solms, (2017) users are considered to be the weakest link in the security chain - due to their insecure behaviour and lack of awareness. Their findings suggest that a cybersecurity culture should ideally be fostered at all levels, including individual, organisational, national and international levels. This means anyone in the organisation regardless of what position in the organisation the employee has.

Based on the results from the questionnaire presented in this study, we can see that employees generally are aware of different security risks such as phishing, using the same password multiple times, etc. However, when the respondents were asked “It is ok to connect a private USB into an office/company computer.” The answers were more spread out. By looking at Figure 14, a total of 39% of the respondents answered neutral, agree and strongly agree. By connecting private USB devices into company devices one can easily infect the whole company system with malicious content without the person involved even knowing what happened. This is something to take seriously by these SMEs in order to keep their company's information safe and secure.

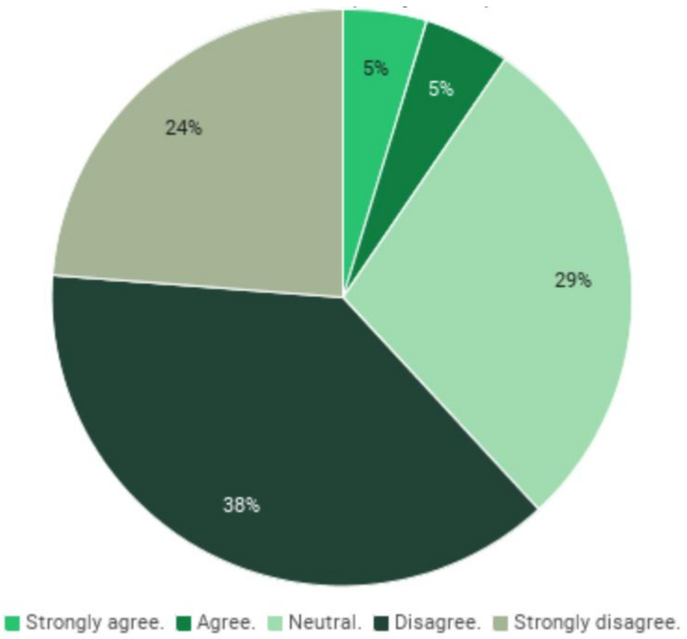

Figure 14: Pie chart of questionnaire result ("It is ok to connect a private USB into an office/company computer.")

The behaviour of the employees is important for SMEs cybersecurity goals. Bada et al. (2019) say in their study that changing behaviour requires more than providing information about risks and reactive behaviours. The study claims three components are needed to change behaviour, firstly they must be able to understand and apply the advice, they must be motivated and willing to do so and it requires a change of attitude and intention.

Parson et al. (2013) suggest that training should be contextualized and should use case studies to improve both pieces of knowledge of what is expected and also understanding of why this is important. He et al. (2019) says to prevent more data breaches to intellectual capital, organizations must provide regular cybersecurity awareness training for all personnel.

Based on the results of the questionnaire presented in this study, we can discuss the importance of general training of cybersecurity awareness among employees. When asked if "Virus, malware and Trojans can spread when clicking on an insecure link on a website." A total of 85% of the respondents answered strongly agree and agree as we can see in Figure 15. However, a total of 15% answered neutral and disagree. We believe that the ideal response for SMEs invested in cybersecurity and awareness would be close to 100% strongly agree.

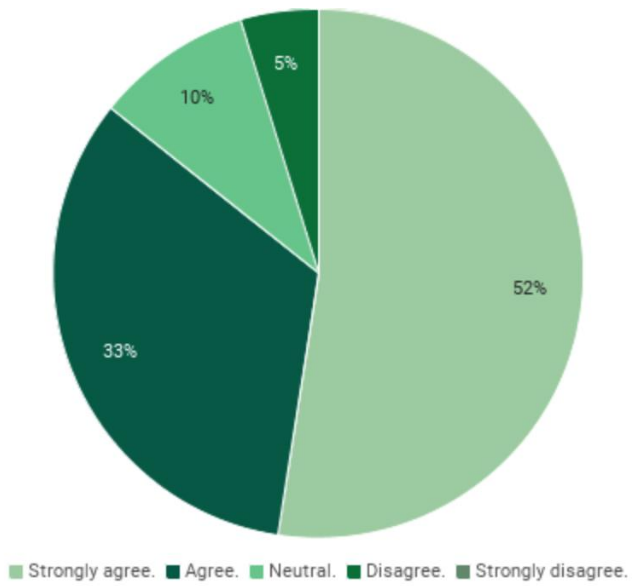

Figure 15: Pie chart of questionnaire result (“Virus, malware and Trojans can spread when clicking on an insecure link on a website.”)

In the questionnaire when the respondents were asked “I know what ransomware is and how to avoid it.” The results were spread out as we can see in Figure 16. We believe the ideal result for this question would be 100% strongly agree or at least more on the “agree” side. However, a total of 34% of the respondents answered neutral and disagree, which is concerning. Should any of these 34% of respondents be targeted for ransomware, it could lead to risks such as bankruptcy for SMEs, which is important to be aware of.

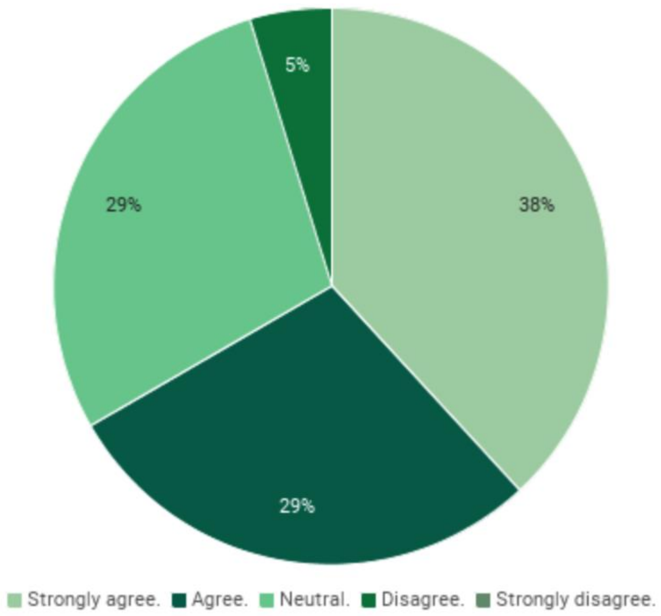

Figure 16: Pie chart of questionnaire result (“I know what ransomware is and how to avoid it.”)

Investing in employee training means recognizing their value and potential contribution to the success of the organisation. If companies do not change their belief about the importance of training as a means to recognize people's value, this can be an obstacle for the building of cybersecurity culture and risks failing from the start, (Corradini, 2020).

The knowledge in cybersecurity awareness is important to train and keep the employees updated. In the article of Zwilling et al. (2020) findings show that higher cybersecurity knowledge is connected to the level of cyber awareness, beyond the differences in the respondent's country or gender.

As we can see from the results of the questionnaire performed in this study, keeping employees up to date on security, with meetings or newsletters, seems to not be a high priority for all SMEs in this study. When asked, "The company has security newsletters, briefings or meetings about security." 14% of the respondents answered strongly disagree. In addition, 33% answered neutral. The results are presented in Figure 17.

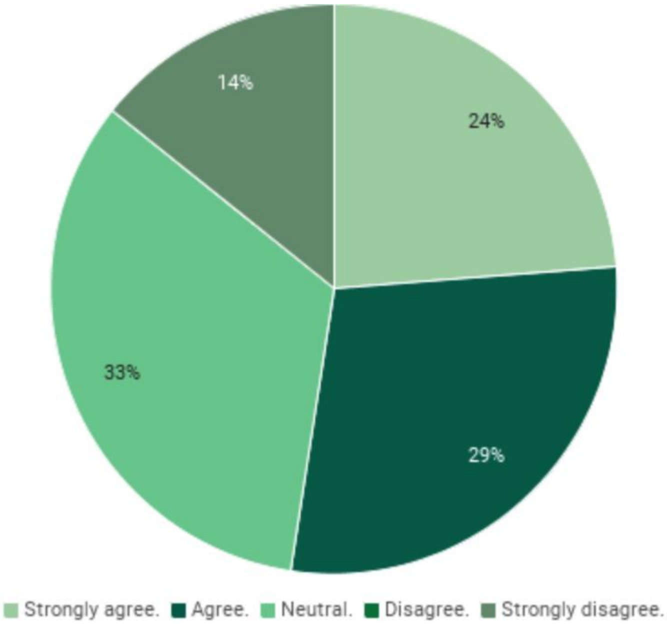

Figure 17: Pie chart of questionnaire result ("The company has security newsletters, briefings or meetings about security.")

Based on the results from the questionnaire conducted for this research, the respondents seem engaged in upholding GDPR. As we can see in Figure 18, when asked "I know how to support my company by following GDPR and to avoid fines because of data breaches." A total of 81% of the respondents strongly agree and agree. We believe this is very important and recognise that SMEs understand the importance of this as well.

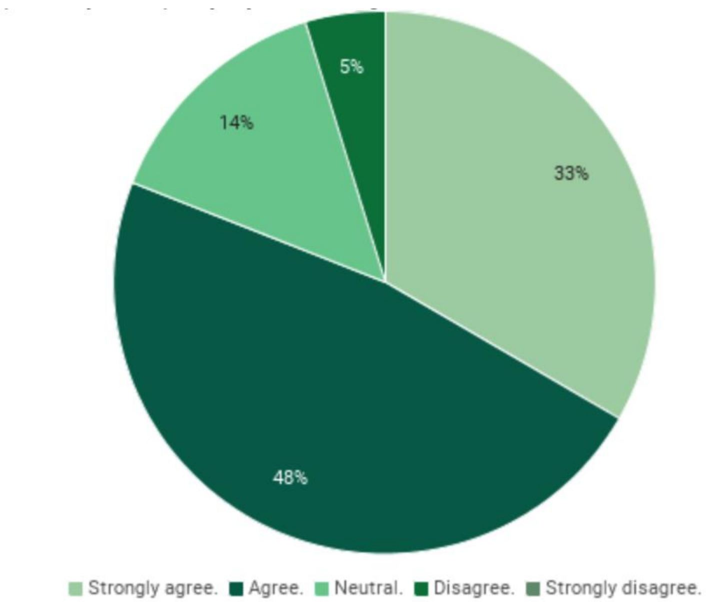

Figure 18: Pie chart of questionnaire result ("I know how to support my company by following GDPR and to avoid fines because of data breaches.")

Through the research done by Tirumala, Valluri & Babu, (2019), it is clear that the results from their survey show that employees fail to see their responsibility and security concerns.

As mentioned in 2.2 «Previous Research» of this thesis, the survey conducted by Tirumala, Valluri & Babu, (2019), with 4800 participants resulted in a few conclusions. Such as providing cyber restrictions and monitoring tools, a guide to install cyber restrictions and monitoring tools, mandatory two-factor authentication for employees, as well as clear guidelines for password management.
Based on the results, the conclusions should have already been in place and should be a standard for all organisations that may face any cybersecurity issues.

As mentioned in 2.2 «Previous Research» is a study done by Zwilling et al. (2020), where results show that the respondents are aware of the term «cybersecurity». However, only to a basic and insufficient extent. meaning they will only do measures such as strong passwords and installing antivirus software.
In addition, through the research by De Bruijn and Janssen (2017), as often said, humans are the weakest link. Meaning ignorance and limited understanding are at fault for the lack of planning and policies. In our questionnaire, on question number nine, 24% of the responses showed that they were either neutral or strongly agree that it is ok to share passwords with others. Question number 19 showed that as much as 38% agree or strongly agree that it is ok to have a personal device such as a phone, tablet computer at work. This shows that humans as the weakest link can put the organisation at risk by their behaviour.

By viewing these perspectives from the literature review together, one results in a deeper understanding of the cybersecurity awareness field. To summarize the discussion and study we have learned a deeper understanding of the cybersecurity awareness field and the categories “Meaning”, “Behaviour”, and “Knowledge”. In the general overview of the topic, the respondents were mostly full-time employees. The system at their workplace all respondents had an email system, but also the vast majority used website and blog systems followed by nearly half using social media systems. Interestingly 29% also didn’t know if there had been any cybersecurity incidents at their workplace which could mean a greater need for cybersecurity awareness focus.

In the category meaning it shows that employees think SME organisations should have rules and regulations and they think the organisation should follow them. In the behaviour category, we see that the employees are not fully invested to follow the recommended steps to increase cybersecurity awareness and that behaviour such as USB devices and sharing of passwords could put the organisation at a higher risk. In the knowledge category the employees claim to have a high understanding of the different topics. There should be more research on whether this is true, and from the literature, there seems to be little research on the "Knowledge" field.

6.0 Conclusion and Implications

In this chapter we conclude on our research, derive the implications from our study and suggest future research on the topic.

This study has reviewed the literature on cybersecurity awareness and conducted a survey with multiple SMEs. The study followed a qualitative research method with a mix of exploratory approach and collected data through a survey questionnaire. This thesis aimed at answering the research questions of RQ1: “What does cybersecurity situational awareness mean to an employee in a small to medium-sized organisation (SME)?” Including RQ2: “What types of behaviours do the SME employees perceive as factors that cause cyber incidents in SMEs?”.

Based on our questionnaire, the majority of respondents in our questionnaire were full-time employees and considered cybersecurity as a part of the daily IT job. The results show 61% of the respondents strongly agree that the company should provide cybersecurity guidelines. Yet still, 71% of the respondents answered that cybersecurity counts for “low, less than 20% of all business activities.” This seems to suggest that there is a need to raise awareness of cybersecurity to be included in all business activities. It also suggests that cybersecurity might not be the top priority of SMEs. Our study also suggests that humans as the weakest link can put the organisation at risk by their behaviour regarding passwords and personal devices at the workplace. This is also supported by 39% of the respondents who either agree, strongly agree or are neutral that it is ok to connect a private USB into an office/company computer. With the behaviours described above, it seems that the employee’s behaviour is not clear that they may pose a risk to organisational assets. In the “Knowledge” part of the questions in the survey, the respondents scored high in relation to their knowledge of viruses, malware, trojans, phishing, ransomware.

We believe this thesis can contribute to further research on the topic. However, the thesis also identified some gaps in the literature on the category “Knowledge”.
The implications of this study suggest the need for more focus on cybersecurity awareness among SMEs. The findings and results of the questionnaire that was conducted for this study may also be helpful for organisations, and perhaps to be utilised as a way of improving their employees’ behaviour and knowledge in regard to cybersecurity awareness training.

In conclusion, based on our literature review and the study conducted in the SMEs we have suggested further research on cybersecurity awareness to better protect data. Further research should also be on the focus pointed out in this thesis, the “Meaning, Behaviour and Knowledge” aspects. Especially the “Knowledge” dimension which we described earlier defines whether or not the employees have the knowledge of certain topics in cybersecurity, seem to have little previous research. Although the SME employees responded with high knowledge, more research can be done to investigate whether or not this actually is the case. Such an important topic should be more known as it may be crucial to find out whether the employees have the basic knowledge or not, as it can reduce the cybersecurity incidents in an SME. There could also be more research on how to increase the cybersecurity behaviour among SME employees and why it can lead to cybersecurity incidents.

7.0 References

Abd Rahim et al. (2015). *A systematic review of approaches to assessing cybersecurity awareness*. Available from: https://www.emerald.com/insight/content/doi/10.1108/k-12-2014-0283/full/html
Accessed on: 22.02.2021

Abawajy. (2012). *User preference of cyber security awareness delivery methods.* Available from: https://www.tandfonline.com/doi/full/10.1080/0144929X.2012.708787
Accessed on: 09.02.2021

Al-Mohannadi et.al. (2018). *Understanding Awareness of Cyber Security Threat among IT employees.* Available from: https://ieeexplore.ieee.org/abstract/document/8488196
Accessed on: 19.01.2021

Alshaikh. (2020). *Developing Cybersecurity Culture to influence employee behavior: A practice perspective*. Available from:
https://www.sciencedirect.com/science/article/pii/S0167404820302765
Accessed on: 25.01.2021

Andreadis & Kartsounidou, (2020). *The impact of splitting a long online questionnaire on data quality*. Available from: https://ojs.ub.uni-konstanz.de/srm/article/view/7294
Accessed on: 09.04.2021

Bada et al. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* Available from: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf
Accessed on: 15.02.2021

Coenraad, et.al. (2020). *Experiencing Cybersecurity One Game at a Time: A systematic review of Cybersecurity Digital Games.* Available from:
https://journals.sagepub.com/doi/full/10.1177/1046878120933312
Accessed on: 19.01.2021

Corradini. (2020). *Developing Cybersecurity Awareness*. Available from:
https://link.springer.com/chapter/10.1007/978-3-030-43999-6_6
Accessed on: 09.02.2021

Creswell, W. J. (2009). *Research Design – Qualitative, Quantitative, and Mixed Methods Approaches*.

De Bruijn, Janssen. (2017). *Building Cybersecurity awareness: The need for evidence-based framing strategies*. Available from:
https://www.sciencedirect.com/science/article/pii/S0740624X17300540
Accessed on: 21.01.2021

ENISA. (2020). *Threat Landscape*. Available from: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-the-year-in-review
Accessed on: 23.05.2021

European Commission. *SME Definition.* Available from:
https://ec.europa.eu/growth/smes/sme-definition_en
Accessed on: 28.02.2021

Franke & Brynielsson. (2014). *Cyber Situational Awareness - A systematic review of the literature.* Available From:
https://www.sciencedirect.com/science/article/pii/S0167404814001011
Accessed on: 10.02.2021

Gcaza & Solms. (2017). *Cybersecurity Culture: An ill-defined problem*. Available From:
https://link.springer.com/chapter/10.1007/978-3-319-58553-6_9
Accessed on: 17.02.2021

Hänsch & Benenson. (2014). *Specifying IT security awareness.*
Available from: https://ieeexplore.ieee.org/abstract/document/6974870
Accessed on: 17.02.2021

He et al. (2019). *Improving employees' intellectual capacity for cybersecurity through evidence-based malware training.* Available from:
https://www.emerald.com/insight/content/doi/10.1108/JIC-05-2019-0112/full/html
Accessed on: 18.02.2021

He & Zhang (2019). *Enterprise cybersecurity training and awareness programs: Recommendations for success.* Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257. Available from:
https://www.tandfonline.com/doi/full/10.1080/10919392.2019.1611528
Accessed on: 15.02.2021

Hyde (2000). *Recognising deductive processes in qualitative research.* Qualitative market research: An international journal.
Available from: https://doi.org/10.1108/13522750010322089
Accessed on: 23.03.2021

Kaplan et.al. (2015). Beyond cybersecurity: Protecting Your Digital Business. P.xiii.

Lee. (2017). *Cybersecurity awareness: Protecting data and patients.* Available from:
https://journals.lww.com/nursingmanagement/FullText/2017/04000/Cybersecurity_awareness__Protecting_data_and.6.aspx
Accessed on: 16.02.2021

Li et.al. (2018). *Investigating the impact of cybersecurity policy awareness on employees cybersecurity behaviour.* Available from:
https://www.sciencedirect.com/science/article/pii/S0268401218302093

Accessed on: 21.01.2021

Muhirwe & White. (2016). *Cybersecurity awareness and practice of next generation corporate technology users*. Available from: http://iacis.org/iis/2016/2_iis_2016_183-192.pdf
Accessed on: 14.02.2021

NIST SP 800-50, NIST SP-800-16. *Awareness.* Available from:
https://csrc.nist.gov/glossary/term/Awareness
Accessed on: 16.02.2021

NorSIS (2021). *The Norwegian Center for Information Security*. Available from:
https://norsis.no/english/
Accessed on: 01.04.2021

NorSIS (2021) 2. *Nordmenn og digital sikkerhetskultur 2020*. Available from:
https://norsis.no/wp-content/uploads/2020/10/Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf
Accessed on: 01.04.2021

The Confederation of Norwegian Enterprise (NHO). *Fakta om små og mellomstore bedrifter (SMB)*. Available from: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/
Accessed on: 28.02.2021

Organisation for Economic Co-operation and Development (OECD), (2015) *Digital security risk management*. Available from: http://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
Accessed on: 31.03.2021

Okoli. (2010). *A guide to conducting a systematic literature review of information system research.* Available from:
https://edisciplinas.usp.br/pluginfile.php/4126343/mod_resource/content/1/systematic%20literature%20reviews%20Okoli%2C%20Schabram%202010%20Sprouts.pdf
Accessed on: 22.02.2021

Parson et al. (2013). *Determining employee awareness using the human aspect of information security questionnaire (HAIS-Q)*. Available from:
https://www.sciencedirect.com/science/article/pii/S016740481300179X
Accessed on: 09.02.2021

Ponsard & Grandclaudon. (2020). *Guidelines and Tool Support for Building A Cybersecurity Awareness Program for SMEs.* Available from:
https://link.springer.com/chapter/10.1007/978-3-030-49443-8_16
Accessed on: 31.01.2021

Ponsard, Grandclaudon, Bal. (2019). *Survey and Lessons Learned on Raising SME awareness about Cybersecurity*. Available from: https://www.scitepress.org/Papers/2019/75743/75743.pdf

Accessed on: 31.01.2021

Rajivan & Cookie, (2017). *Impact of team collaboration on cybersecurity situational awareness.* Available from: https://link.springer.com/chapter/10.1007/978-3-319-61152-5_8
Accessed on: 16.02.2021

Renaud & Weir, (2016). *Cybersecurity and the unbearability of Uncertainty*. Available from: https://ieeexplore.ieee.org/document/7600224
Accessed on: 04.03.2021

Shaw et al. (2009). *The impact of information richness on information security awareness training effectiveness*. Available from: https://www.sciencedirect.com/science/article/pii/S0360131508001012
Accessed on: 18.02.2021

Shojaifar, and Fricker (2020). *SMEs confidentiality concerns for security information sharing.* Available from: https://link.springer.com/chapter/10.1007%2F978-3-030-57404-8_22
Accessed on: 21.03.2021

Tirumala, Valluri & Babu (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)*.
Available from:
https://ieeexplore.ieee.org/abstract/document/8821951?casa_token=9d5vGFKYzAsAAAAA:HFQ9u4tmtGty9Uqa31R27AtUt1Z8D-U2q-o0sa7qzPIKPzE8P94JtXzCtazDRvjecJcpGOCh
Accessed on 01.04.2021

Zani et al., (2018). *A review of security awareness approach ensuring communal learning.* Available from: https://aisel.aisnet.org/pacis2018/278/
Accessed on: 17.02.2021

Zwilling et al. (2020). *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*. The Journal of Computer Information Systems, 1-16.
Available from:
https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1712269?scroll=top&needAccess=true
Accessed on: 15.02.2021

8.0 Appendix

8.1 Appendix A: Questionnaire

General questions:

1. What is your position within the company?
    a. Full time employee
    b. Part time employee
    c. Partner
    d. Other

2. How does your company tackle cybersecurity aspects?
    a. The company has dedicated security team
    b. The company has one-two staffs that handle security
    c. A part of IT job
    d. Outsourced to the third party
    e. I do not know
    f. Other

3. How much of all business activities in your company are being used for security-related activities?

    [ ] Low. Less than 20% of all business activities.

    [ ] Medium. 20-30% of all business activities.

    [ ] Top priority. More than 30% of all business activities.

4. How often does a cybersecurity incident occur in your company?
    a. 1-5 times per month.
    b. 5-10 times per month.

c. More than 10 times per month.

d. Never register incidents.

e. I do not know.

5. What kind of online systems are used in your company? (Possible to select multiple answers)

[ ] Email for organisations and companies.

[ ] Website, blog.

[ ] Online bank accounts.

[ ] Personal information of customers stored electronically.

[ ] Social media accounts.

[ ] Online order, booking and payment.

[ ] Industrial control system.

[ ] Others....

The meaning of cybersecurity awareness. Select the answer that applies to you.

6. The company should provide guidance on cybersecurity.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

7. The company should show how to comply with laws and regulations for security.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

8. The company has security newsletters, briefings or meetings about security.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

Perceived behaviours that lead into cybersecurity incidents in your company

9. It is ok to share passwords with others.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

10. It is ok to open carelessly every email attachment.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

11. It is ok to easily trust an email that you believe looks legitimate.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

12. It is ok to connect private USB into an office/company computer.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

13. Updating computers/software is necessary to maintain security.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

14. Backups are necessary to maintain security.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

15. It is ok to visit illegitimate websites.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

16. It is ok to never change passwords.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

17. It is ok to use weak passwords (no numbers, uppercase, words etc)

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

18. It is ok to use the same password for multiple websites and social media.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

19. It is ok to use personal devices (phone, tablet, computer) at the office.

[ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

Knowledge of daily cybersecurity

20. Virus, malware and Trojans can spread from email attachments.
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

21. Virus, malware and Trojans can spread when clicking on an insecure link on a website.
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

22. I know what phishing is and how to avoid it
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

23. I know what email scams are and how to avoid it
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

24. I know what ransomware is and how to avoid it.
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

25. I know what GDPR is.
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

26. I know how to support my company by following GDPR and to avoid fines because of data breaches.
    [ ] Strongly agree. [ ] Agree. [ ] Neutral. [ ] Disagree. [ ] Strongly disagree.

8.2 Appendix B: Questionnaire Results

	Respondents	Per cent
General questions about cybersecurity 1-5		
1. What is your position within the company?		
Full time employee	17	81%
Part time employee	-	-
Partner	3	14%
Other	1	5%
2. How does your company tackle the cybersecurity aspect?		
The company has a dedicated security team	4	19%
The company has one-two staffs that handles security	6	29%
A part of IT job	11	52%
Outsourced to the third party	3	14%
I do not know	3	14%
Other	1	5%
3. How much of all business activities in your company are being used for security-related activities?		
Low. Less than 20% of all business activities.	15	71%
Medium. 20-30% of all business activities.	4	19%
Top priority. More than 30% of all business activities.	2	10%

4. How often does a cybersecurity incident occur in your company?		
1-5 times per month.	8	38%
5-10 times per month.	-	-
More than 10 times per month.	-	-
Never register incidents.	7	33%
I do not know.	6	29%
5. What kind of online systems are used in your company? (Possible to select multiple answers)		
Email for organisations and companies.	21	100%
Website, blog.	15	71%
Online bank accounts.	10	48%
Personal information of customers stored electronically.	9	43%
Social media accounts.	12	57%
Online order, booking and payment.	6	29%
Industrial control system.	4	19%
Other.	3	14%
Meaning of cybersecurity 6-8		
6. The company should provide guidance on cybersecurity.		
Strongly agree	13	61,9%
Agree	5	23,8%

Neutral	1	4,8%
Disagree	1	4,8%
Strongly disagree	1	4,8%
7. The company should show how to comply with laws and regulations for security.		
Strongly agree	11	52,4%
Agree	8	38,1%
Neutral	-	-
Disagree	2	9,5%
Strongly disagree	-	-
8. The company has security newsletters, briefings or meetings about security.		
Strongly agree	5	23,8%
Agree	6	28,6%
Neutral	7	33,3%
Disagree	-	-
Strongly disagree	3	14,3%
Behaviours of cybersecurity 9-19		
9. It is ok to share passwords with others.		
Strongly agree	1	4,8%
Agree	-	-

Neutral	4	19%
Disagree	3	14,3%
Strongly disagree	13	61,9%
10. It is ok to open carelessly every email attachment.		
Strongly agree	-	-
Agree	1	4,8%
Neutral	1	4,8%
Disagree	-	-
Strongly disagree	19	90,5%
11. It is ok to easily trust an email that you believe looks legitimate.		
Strongly agree	1	4,8%
Agree	-	-
Neutral	3	14,3%
Disagree	5	23,8%
Strongly disagree	12	57,1%
12. It is ok to connect private USB into an office/company computer.		
Strongly agree	1	4,8%
Agree	1	4,8%
Neutral	6	28,6%

Disagree	8	38,1%
Strongly disagree	5	23,8%
13. Updating computers/software is necessary to maintain security.		
Strongly agree	14	66,7%
Agree	5	23,8%
Neutral	2	9,5%
Disagree	-	-
Strongly disagree	-	-
14. Backups are necessary to maintain security.		
Strongly agree	16	76,2%
Agree	4	19%
Neutral	1	4,8%
Disagree	-	-
Strongly disagree	-	-
15. It is ok to visit illegitimate websites.		
Strongly agree	-	-
Agree	-	-
Neutral	1	4,8%
Disagree	8	38,1%

Strongly disagree	12	57,1%
16. It is ok to never change passwords.		
Strongly agree	-	-
Agree	1	4,8%
Neutral	4	19%
Disagree	3	14,3%
Strongly disagree	13	61,9%
17. It is ok to use weak passwords (no numbers, uppercase, words etc).		
Strongly agree	-	-
Agree	-	-
Neutral	-	-
Disagree	8	38,1%
Strongly disagree	13	61,9%
18. It is ok to use the same password for multiple websites and social media.		
Strongly agree	-	-
Agree	-	-
Neutral	-	-
Disagree	15	71,4%
Strongly disagree	6	28,6%

19. It is ok to use personal devices (phone, tablet, computer) at the office.		
Strongly agree	1	4,8%
Agree	7	33,3%
Neutral	8	38,1%
Disagree	2	9,5%
Strongly disagree	3	14,3%
Knowledge of cybersecurity 20-26		
20. Virus, malware and Trojans can spread from email attachments.		
Strongly agree	13	61,9%
Agree	6	28,6%
Neutral	1	4,8%
Disagree	-	-
Strongly disagree	1	4,8%
21. Virus, malware and Trojans can spread when clicking on an insecure link on a website.		
Strongly agree	11	52,4%
Agree	7	33,3%
Neutral	2	9,5%
Disagree	1	4,8%
Strongly disagree	-	-

22. I know what phishing is and how to avoid it		
Strongly agree	12	57,1%
Agree	4	19%
Neutral	5	23,8%
Disagree	-	-
Strongly disagree	-	-
23. I know what email scams are and how to avoid it		
Strongly agree	15	71,4%
Agree	5	23,8%
Neutral	1	4,8%
Disagree	-	-
Strongly disagree	-	-
24. I know what ransomware is and how to avoid it.		
Strongly agree	8	38,1%
Agree	6	28,6%
Neutral	6	28,6%
Disagree	1	4,8%
Strongly disagree	-	-
25. I know what GDPR is.		

Strongly agree	11	52,4%
Agree	9	42,9%
Neutral	1	4,8%
Disagree	-	-
Strongly disagree	-	-
26. I know how to support my company by following GDPR and to avoid fines because of data breaches.		
Strongly agree	7	33,3%
Agree	10	47,6%
Neutral	3	14,3%
Disagree	1	4,8%
Strongly disagree	-	-
Total	21	100%