Information Security Assessment of the Norwegian SMB-Sector: A Study of Culture, Leadership and Cost

Authors:

Salem Hamidi and Andreas Gaard

Supervisor:

Dr. Håkon Bjorheim Abrahamsen

Advisor:

Tord Fanøy Bårdsen

Submission Date:

14.06.2023

Study Programme:

Master of Science in Industrial Economics

University of Stavanger

Faculty of Science and Technology

Department of Security, Economics and Planning

University of Stavanger

FACULTY OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS

Study Programme: Industrial Economics	**The Spring Semester, 2023** **Open**

Authors:
Salem Hamidi and Andreas Gaard

Supervisor: Dr. Håkon Bjorheim Abrahamsen

External Supervisor: Tord Fanøy Bårdsen

Thesis Title: Information Security Assessment of the Norwegian SMB-Sector: A Study of Culture, Leadership and Cost

Credits (ECTS):
30

Keywords: Information Security, Security Culture, Security Awareness, Security Practices, Cost Estimation, Data Breaches, Cyber Insurance, Small and Medium-Sized Businesses	**Pages:** 79 **+ Appendix:** 15 Stavanger, 14/06/2023

Abstract

The aim of this study was to contribute to the understanding of information security practices and challenges in small and medium-sized businesses in Norway. The research focuses on organizational culture and leadership practices related to information security. Additionally, the study has been interested in mapping the number of security incidents, as well as their associated costs. The study collected a fresh set of data by conducting a survey of 236 small and medium-sized businesses across various industries and between the 11 Norwegian counties. The findings reveal that a significant number of Norwegian SMBs have experienced information security incidents over the past four years. While some incidents were severe and resulted in substantial costs, the median cost of incidents was found to be moderate and manageable for most businesses. However, it is emphasized that businesses should constantly raise their security levels to prepare for worst-case scenarios. Furthermore, the study highlights the role of cyber insurance in protecting businesses against data breaches. Approximately one out of every six participants reported that their organization had purchased cyber insurance and the findings show an increased likelihood to invest in such coverage for organizations that had experienced data breaches. This may indicate that the organizations recognize the importance of increasing security measures following a security incident. Interestingly, the research does not find a statistically significant relationship between the "Culture Security Level" and the probability or cost of incidents. The study acknowledges limitations in the methodology used to assess the "Culture Security Level" and highlights the need for further research. Based on the findings, it is concluded that the Norwegian SMB sector on average does not possess sufficient security measures to mitigate information security risk adequately. Overall, this thesis provides valuable insight into the information security landscape of Norwegian SMBs, highlights the challenges and offers recommendations for improving security practices.

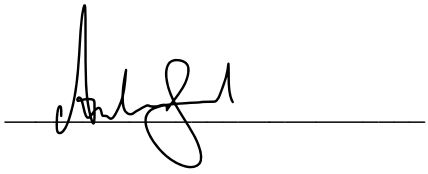
Preface

This master's thesis is the final product as part of a Master of Science degree in Industrial Economics written during the spring semester of 2023, by two students at the University of Stavanger, for the Department of Safety, Economics and Planning.

The purpose of this thesis has been to investigate how implementing different information security measures affects the overall information security in small and medium-sized businesses. The thesis has been especially interested in determining how leadership and culture within an organization contribute to reducing information security incidents, and the cost related to these incidents. We conducted a survey and performed quantitative analyses to gather information on this subject.

Stavanger, 14th June 2023

Salem Hamidi



Andreas Gaard

Acknowledgements

We would like to express our deepest gratitude and appreciation for the support, guidance and motivation we have received during the course of this whole master's degree.

First and foremost, we would like to extend our heartfelt gratitude to our thesis supervisor Dr. Håkon Bjorheim Abrahamsen, external advisor Tord Fanøy Bårdsen and Professor Jan Terje Kvaløy, whose exceptional guidance and expertise have been instrumental throughout the process of completing this master's thesis. We are eternally grateful for their constructive feedback, recommendation, insightful comments, unwavering support, understanding and patience exhibited during the course of this project. Without their valuable assistance, this accomplishment would not have been possible.

We would also like to express our gratitude to the participants from the small and medium-sized businesses who took the time to not only complete our survey but also responded with encouraging and motivating words and highlighted limitations.

Lastly, we would like to thank all our co-students, professors, friends, family members and everyone else who has continuously supported us throughout this journey.

Table of Contents

List of Figures

List of Tables

List of Equations

CHAPTER 1

Introduction

The purpose of this chapter is to provide the necessary information and give a clear understanding of the research study. It provides a brief overview of the history, current state and introduces the research topic and research questions this thesis will explore. Lastly, an outline of the remaining chapters.

1.1 Background

As a result of the increasing digitalization and widespread adoption of information- and communication technologies in society, information security has become a critical concern for organizations of all sizes, including small and medium-sized businesses (SMBs) (Bada & Nurse, 2019). Information security is defined as the protection of information and information systems from unauthorized access (NIST, 2023). The COVID-19 pandemic has forced organizations to accelerate their digital transformation due to restrictions which have led to an increased number of information security incidents (NorSIS, 2021). SMBs have therefore become more reliant on technology to conduct daily operations, which has exposed them to increased risks and security threats (Georgescu, 2021). With the increase in the number of incidents, it has become essential to implement not only technical measures but also develop cultural and organizational policies to prevent unauthorized access to systems, confidential information and sensitive data (NorSIS, 2021). According to the Digital Economy and Society Index (DESI) 2022 report, 77 percent of all SMBs in Norway have integrated a basic level of digital technology (European Commission, 2022).

SMB in Norway is defined as companies with less than 100 employees which is the definition that will be used in this research (Nærings- og handelsdepartementet, 2012). Small companies are defined as 1 - 20 employees, and medium-sized companies as 21 - 100 employees. SMBs play an important role in the economic growth and job creation in Norway, constitute 99 percent of all Norwegian companies, and stand for 44 percent of the country's value creation (Grimsby, Grünfeld, & Jakobsen, 2009).

Limited budget, resources and lack of personnel with security expertise make it difficult for these organizations to implement the necessary security measures (Mijnhardt, Baars, & Spruit, 2016). This makes these organizations more attractive targets for criminals seeking to exploit vulnerabilities. Most challenges and threats faced by SMBs related to information security can be attributed to different factors such as limited budget and resources, lack of cybersecurity expertise and inadequate security measures (Paulsen, 2016).

(Bada & Nurse, 2019; Mijnhardt, Baars, & Spruit, 2016; NorSIS, 2021) suggests there is a significant demand for more and further research on information security in SMBs. Different reports that have frequently been published over a long period on the information security of SMBs show several differences in their findings. According to Mørketallsundersøkelsen 2022 by Næringslivets Sikkerhetsråd, the average cost of a data breaches in Norwegian businesses is 43 000 NOK (Næringslivets Sikkerhetsråd, 2022), while the Cost of a Data Breach Report 2022 by IBM Security reports that the average cost of a data breach in Scandinavian businesses is around 25 MNOK (IBM Security, 2022).

1.2 Purpose

The purpose of this master´s thesis is to investigate the information security threats and challenges faced, the impact of these threats and measures implemented

to address them by SMBs in Norway. Additionally, to investigate the most common security threats and their associated probability and consequences. Furthermore, it seeks to explore the role of leadership and culture on information security in these organizations and the cost related to these breaches.

The findings in this study will contribute to the currently existing academic literature and discussion on information security challenges and threats and provide valuable insight into the status quo and specific challenges faced by SMBs. The insight gained through this research will provide SMBs with recommendations that can contribute to improving their information security resilience and protecting valuable assets. In addition, the report includes descriptive statistics and figures derived from the dataset as independent findings and supplementary information to the aforementioned topics.

This thesis is written in collaboration with Varde Hartmark, a Norwegian consulting company that specializes in technology and business management. The company have observed a significant increase in the number of requests for support regarding information security management from their clients.

1.3 Research Questions

Based on the reflections in the previous subchapters, the research questions for this thesis are:

RQ1: To which degree are Norwegian small and medium-sized businesses affected by information security incidents?

RQ2: Are small and medium-sized businesses sufficiently secure against information security incidents?

1.4 Report Outline

This report consists of seven chapters, and the organization of the remaining chapters in this report is as follows:

- **Chapter 2 – Literature Review**
  This chapter presents an overview of the relevant literature on each of the aforementioned topics. Additionally, it also provides a better understanding of the context, the current state of knowledge and contributes to highlighting gaps and areas where further research is needed.
- **Chapter 3 – Research Methodology**
  This chapter describes the research methodology used to conduct this study. It includes a description of the research design, survey design, data collection, data cleaning and regression methods, as well as privacy and ethical considerations considered during the study.
- **Chapter 4 – Summary Statistics**
  This chapter presents a descriptive statistical summary of the data gathered through the survey. The data is presented to provide an overview of the response to each of the questions from the questionnaire through figures and tables.
- **Chapter 5 – Results**
  This chapter presents the findings of the study and provides a clear understanding of the results in the context of the research questions.
- **Chapter 6 – Discussion**
  This chapter interprets and presents a critical evaluation of the results presented in Chapter 5 and information in relation to the research questions and purpose of the study. It also discusses the literature review, implications for further research and acknowledgment of any limitations of the study.
- **Chapter 7 – Conclusion**

This final chapter summarizes the main findings of the study and presents the conclusions and final thoughts. It also presents reflections on the findings and their implications and suggestions for future research.

CHAPTER 2

Literature Review

This chapter presents the existing academic literature relevant to the research topic. It aims to evaluate previous research and identify the gaps and limitations that exist in the current literature. This review will serve as a foundation for the research study and helps to put the research within the broader academic context and give a comprehensive understanding of the previous research conducted in the field (Fink, 2019).

2.1 Literature Review Method

There are many different guides and standardized methodologies for conducting a literature review, but according to (Okoli & Schabram, 2010) there are none that meet the specific needs of information system research. A literature review was conducted prior to this study, and the method selected for this review was a Systematic Literature Review (SLR) as described by (Okoli & Schabram, 2010). The SLR method provided a comprehensive overview of previous research, identifying gaps and suggestions for further research on this specific research topic (Peričić & Tanveer, 2019).

A variety of databases and search engines accessible to students at the University of Stavanger were used to find relevant literature. The databases used were Oria, Scopus, IEEE Xplore, ScienceDirect, Elsevier, JSTOR, Emerald and the Google Scholar search engine. These databases and the search engine gave access to an extensive collection of resources from diverse institutions and journals.

2.2 Threats and Challenges Faced by SMBs

SMBs face many threats and challenges when it comes to information security. The threats and attacks have increased for all types of organizations but have significantly increased towards SMBs, due to the lack of resources dedicated to information security measures (Bada & Nurse, 2019). SMBs often tend to lack the expertise and the necessary personnel to implement information security measures, which leaves them vulnerable to attack (van Haastrecht, Ozkan, Brinkhuis, & Spruit, 2021). They also tend to have employees with many different responsibilities rather than one employee with information security as their primary area of responsibility (Ponsard & Grandclaudon, 2020). Even though reports show an increase in incidents for SMBs, the management of these organizations assesses the risk of these threats as low and often underestimates the chances of them being targeted. Therefore, they are reluctant to implement or invest in security measures to reduce the risk of the probability of an attack (Benz & Chatterjee, 2020).

Information security encompasses not only technical aspects but also the human factor. Therefore, organizations cannot exclusively focus on technology to reduce the risk of threats (Bulgurcu, Cavusoglu, & Benbasat, 2010). Employees are often regarded as the organization's first line of defense, but also the weakest link when it comes to information security (Yildirim, Akalp, Aytac, & Bayram, 2011). According to (Li, et al., 2019) employees are not aware of the potential consequences that information security threats can pose to the organization. This lack of knowledge and awareness amounts to a large number of incidents caused by employees (Maalem, Rachid, Caulkins, Mohapatra, & Kumar, 2020).

2.2.1 Malware

Malware, short for malicious software is defined as any intrusive software developed by hackers with the purpose of stealing data and damaging computers or systems (Cisco Inc, 2023). Malware is reported to be the most frequent threat encountered by organizations (Mutalib, Zainol, & Halip, 2021). Through different methods, hackers manage to plant malware that can cause harm to organizations. The hackers are continuously evolving and becoming more sophisticated (Silva, López, Caraguay, & Hernández-Álvarez, 2019).

2.2.2 Phishing

Phishing is a method to deliver malware that has become one of the most common types used by hackers. By infecting emails with malicious malware and sending these to employees of organizations, hackers want to gain access to systems and confidential information and demand a ransom (Georgescu, 2021). The reason phishing is an effective method is because it targets the employees, which is the weakest link (Butler, 2007).

2.2.3 Ransomware

Ransomware is another threat that SMBs face and has increased after the COVID-19 pandemic (Georgescu, 2021). Ransomware incidents involve hackers accessing an organization's systems and encrypting their data. The hackers most commonly get access to the organization's systems through phishing emails and demand a ransom in exchange for giving back access to the organization's systems (Chesti, Humayun, Sama, & Jhanjhi, 2020).

According to (Georgescu, 2021) ransomware can be especially devastating for SMBs because of the lack of resources, and they may not have backups of their systems which makes it impossible to recover without paying the ransom. The

organizations do not only risk the loss of profit, but also the risk of damaging their reputations by getting sensitive information or confidential data published (Mutalib, Zainol, & Halip, 2021).

2.3 Education and Training

There are several previously conducted research studies that suggest the use of training programs contributes to increasing knowledge and awareness among employees (Bada & Nurse, 2019; Herold, 2005; Uchendu, Nurse, Bada, & Furnell, 2021). According to (Ghafir, et al., 2018) many employees forget the information after courses on security awareness. Therefore, it is important to develop training programs specific to the needs of the organizations, for the context of the organizations and relevant to its culture (Bada & Nurse, 2019).

According to (van Haastrecht, Ozkan, Brinkhuis, & Spruit, 2021) sharing information about security incidents that occur within an organization is essential to reduce the risk of future incidents and make the employees more aware and help to improve the overall information security. In a study (Li, et al., 2019) found that employees are more willing to take protective actions in relation to the organization's information security, if it is perceived to be vulnerable. This perceived vulnerability to potential threats also positively influences the motivation to comply with information security policies (Ifinedo, 2012).

By enhancing the security behavior of employees, organizations can create relevant and engaging training programs that can contribute to motivating employees to take information security seriously (He & Zhang, 2019).

2.4 Information Security Management

"Resilience is the ability of a system to sustain or restore its basic functionality following a risk source" (Aven & Thekdi, 2021). This applies to technical systems, but

also to businesses. Information security risk management is important to improve the resilience of businesses, and it is getting increasingly important as risk in today's business environment is changing fast.

There are various models developed to handle the management of security risk, such as the National Institute of Standard and Technology´s (NIST) Risk Management Framework, the COBIT 5 model from the International professional association ISACA and the ESRM cycle from (Petruzzi & Loyear, 2016). Even though the models are different, there are similarities among them. The ESRM model states that in security, risk management is important to identify and prioritize the assets that are to be protected, and to identify and prioritize the security risks threatening these assets. It is also important to treat these risks, this can be done in several ways. The risk can simply be accepted, the business can stop the risky activity, the business can transfer the risk to another party by buying insurance, or the business can reduce the probability and/or impact of the security risk (Petruzzi & Loyear, 2016). To perform these four steps effectively, both the management and the security practitioners need sufficient knowledge. The management team needs to identify their acceptable risk tolerance and take action to reduce their security risk to that acceptable level. Lastly, the ESRM cycle (Figure 1) states that continuous improvement is important, this includes incident response, root cause analysis and ongoing risk assessment (Petruzzi & Loyear, 2016).

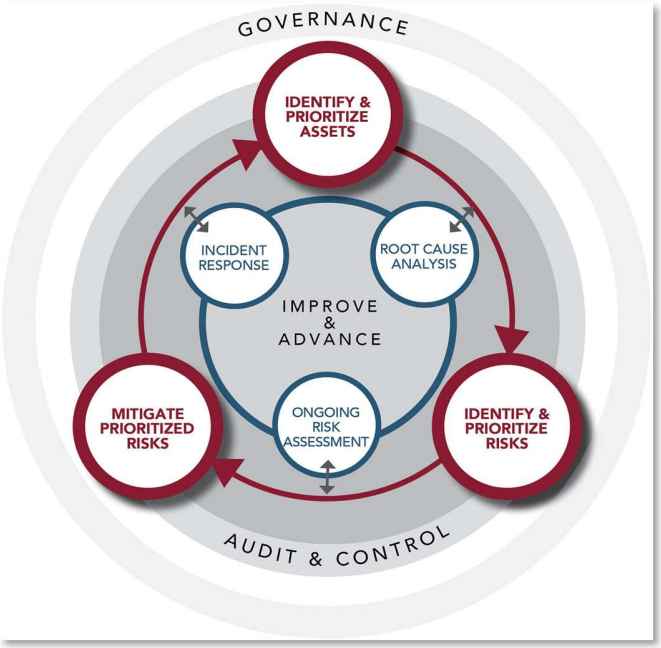


Figure 1: Enterprise Security Risk Management Tool (Security Risk Governance Group, 2023)

2.4.1 Information Security Framework

There are many different frameworks organizations can use when working with information security. ISO27001 is one of these frameworks and has emerged to become a global standard for information security, and is more generalized with a focus on recommendations and guidance rather than specific requirements (Mijnhardt, Baars, & Spruit, 2016; Syafrizal, Selamat, & Zakaria, 2020). This framework proposes guidelines and best practices for organizational information security which is divided into focus areas with specific control measures. and gives a complete overview of information security and how to reduce the risks of threats (International Organization for Standardization, 2022). SMBs often have limited resources, expertise, budget and time to implement these types of frameworks (Mijnhardt, Baars, & Spruit, 2016). Although the implementation of these frameworks remains difficult for SMBs, there are many SMBs that use the framework as a guide without getting certified (Valdevit, Mayer, & Barafort, 2009).

2.4.2 Cyber Insurance

Cyber insurance is a favorable way for organizations to transfer the financial risks related to network and computer incidents from the organization to a third party as a risk management strategy (Böhme & Schwartz, 2010; Tøndel, Meland, Omerovic, Gjære, & Solhaug, 2015). Technical implications cannot eliminate all risks related to cyber security (Franke, 2017). After cloud services and outsourcing of IT services have become more widespread, it has also become more difficult to manage risk through technical and organizational measures. The companies which provide IT services often have very limited liability in case of a data breach. Cyber insurance can be used to cover the gap between the contract limitations of the IT service provider and the total loss of the client (Franke, 2017). According to (Lemnitzer, 2021) cyber insurance is the most effective way to achieve cyber resilience. Insurance companies have strict requirements for companies who want to apply for cyber insurance, a typical absolute requirement for customers is to have an incident response plan. There are also other requirements depending on the industry in which the customer operates. The premium paid can be drastically reduced by adding different IT security implementations. An empirical study of the Swedish cyber insurance market from 2017 reports that the typical cyber insurance premium was 0.5 - 1.0 percent of the indemnity limit, meaning that a company has to pay 5 000 – 10 000 SEK per year for being insured up to 1 MSEK (Franke, 2017).

The insurance companies from the Swedish study are global actors, meaning that the premiums are likely to be quite similar in Norway (Franke, 2017). According to (Bahşi, Franke, & Friberg, 2020) there are only minor differences in pricing between cyber insurance in the Nordic countries. The same report also mentions that the Norwegian cyber insurance market is the least developed cyber insurance market in the Nordics regarding the number of companies being secured (Franke, 2017; Bahşi, Franke, & Friberg, 2020). During the Swedish study in 2017, cyber

insurance was mostly issued to bigger companies. The Norwegian insurance companies working with the SMB sector report that many of the potential customers don´t understand why they need cyber insurance since they have not experienced any incidents yet (Bahşi, Franke, & Friberg, 2020). A survey conducted by Ponemon Institute reported a 70 percent increase in the demand for cyber insurance after an organization experienced an incident (Ponemon Institute, 2013). This study will try to find out how common cyber insurance is in the SMB sector in Norway.

2.4.3 Information Security Operations

Information technology outsourcing is defined as handing over the management of IT assets, resources and activities to a third party, including information security, operations and maintenance (Rajaeian, Cater-Steel, & Lane, 2017). Since many SMBs have limited resources and expertise, these tasks are often outsourced to a managed service provider and can be a highly cost-effective method to get access to security measures and knowledge to reduce the risk related to information security (Froehlich, 2019).

2.5 Information Security Culture

(Da Veiga & Eloff, 2010) defines information security culture as "*The attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time*". Since employees are regarded as the weakest link when it comes to information security it is important for SMBs to develop a culture that promotes information security within the organizations and where incidents and breaches that occur are addressed (Öğütçü, Testik, & Chouseinoglou, 2016).

In many cases, the behavior of employees is the underlying cause of information security incidents (Herold, 2005). A report from IBM Security states that around 21

percent of all data breaches were caused by human errors, from for instance employees or contractors (IBM Security, 2022). An instrument called Information Security Culture Assessment (ISCA) is developed for this cause (Da Veiga & Eloff, 2010). The ISCA framework asks various questions to the employees in order to get an overview of the information security culture. There are 10 different categories of questions in the ISCA framework. Examples are changing management, information security leadership, training and awareness and privacy perception. The different answer options are "strongly agree, agree, unsure, disagree, strongly disagree", in this way the answers get a score from 1 - 5. By asking the employees these same questions over a period, it is possible to map the development of the information security culture.

It is likely to believe that the maturity of the companies' security culture is important for whether they suffer from data breaches, but studies also indicate that other measures can be taken to reduce the number of incidents such as classification schemes. There are various classification schemes such as those presented by (Herath, 2011). A classification scheme systematizes information based on its sensitivity and gives guidelines on how the information should be stored and handled, and who should have access to information with different classifications.

Information Security components should be implemented in an organization to change the information security behavior. The change in behavior might initially be forced due to the implemented components, but after a while, an information security culture will be created (Da Veiga & Eloff, 2010). This will create organizational values, assumptions, artifacts and creations. The organization will evolve a good basis for making intelligent decisions which might make them want to change the implemented components, or they might want to add new

components to strengthen the culture even further. This can be seen with the backward arrow from point C to point A (Figure 2).

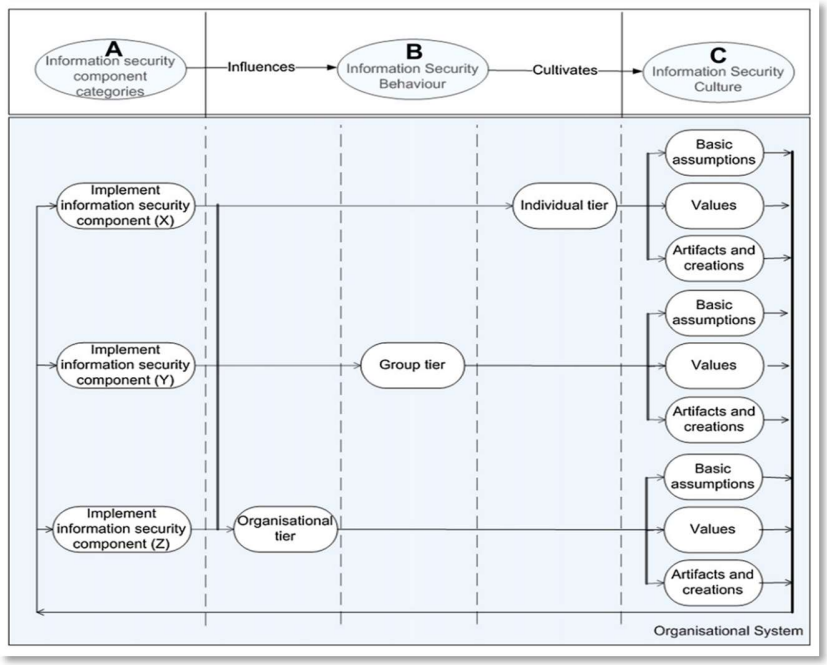


Figure 2: A Framework and Assessment Instrument for Information Security Culture (Da Veiga & Eloff, 2010)

The focus within a group can override the individual´s moral and mental efficiency, this is often referred to as group thinking. Making sure groups are making the right decisions when it comes to information security is important with good leadership. On an organizational level, the top management must decide on an overall strategy, policies and procedures to guide the organization in the desired direction (Da Veiga & Eloff, 2010).

According to (Uchendu, Nurse, Bada, & Furnell, 2021) on information security culture, the most crucial factors to achieve this is the leadership of the organization and the support from the management. Information security culture is developed by clearly defining policies, procedures and guidelines to make it easier for employees in different situations (Ioannou, Stavrou, & Bada, 2019).

2.6 Total Cost of Data Breach

It can be hard to identify the total cost of a data breach. Many companies hold sensitive information not only about their employees, but also about their business partners, patients and customers. If such information is leaked, it can lead to fines and legal action against the company (Da Veiga & Martins, 2015). A study by (Lee, Kauffman, & Sougstad, 2011) investigated how to profit-maximize the amount organizations invest in information security. There was a wide range of reasons why sensitive information had been leaked, such as accidents by employees, hacking and stolen or lost hardware. The study recommended a combination of both technical and non-technical solutions but concluded that it was neither possible, nor economically beneficial to try and mitigate all risks.

2.6.1 Value-at-Risk

Value-at-Risk (VaR) is defined as the maximum loss that could happen in an investment over a given period, with a given confidence level, and is commonly used by investors and commercial banks to quantify risk. It can be calculated by:

- Using statistical analysis on historical data.
- Assuming a normal distribution of return, based on the average return and standard deviation.
- Using the Monte Carlo Method to predict future investment prices (CFI Education Inc, 2023).

By using one of these three methods, it is possible to state that "A company can be X % sure that it will not lose more than $Y on the investment in a given timeframe".

2.6.2 Profit-at-Risk

By defining Profit-at-Risk (PaR) as the lowest acceptable level of profit within a given confidence level and time period, traditional VaR methods can be used for

making analyses (Lee, Kauffman, & Sougstad, 2011). An information security level can be defined as 0 < S < 1, where S = 1 is the maximum possible security level and S = 0 is no spending on information security at all. There will in most cases be too expensive to strive for S=1. The PaR model assumes that a company cannot price its products or services higher if the security level becomes higher, this means that the revenue R stays the same. Implementation costs are known costs to implement security measures. When implementation costs increase, security level S increases.

The average loss and the belonging probability are just slightly higher from S=0 versus S=1 (Figure 3). The probability distribution of the estimated losses λ(S) has a "longer tail" if the security level is low. This means that an extreme loss is more severe if the security level is low. PaR focuses on these extreme losses, which for a company is very important as an extreme loss potentially can lead to bankruptcy.

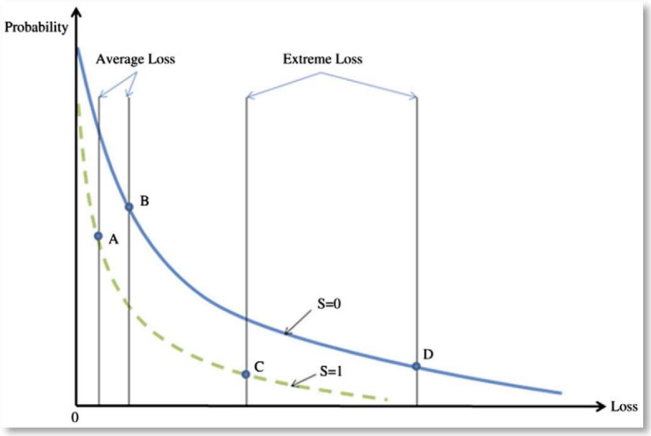


Figure 3: Probability Distribution of Financial Losses with S=0 and S=1 (Lee, Kauffman, & Sougstad, 2011)

By using historical data on the frequency and severity of data breaches within the company, or eventually, from companies within the same industry, it is possible to make a probability distribution of total losses, which again makes it possible to make a company-specific version of Figure 4. As seen from Figure 4, it is possible to find an inefficient protection interval, and an efficient protection interval. (Franke, 2017). In the efficient protection interval, there is a tradeoff between profit and risk. This method is often too comprehensive for most small and medium-sized businesses, but the key

takeaway from this is that the extreme losses are much more severe if the security level is low, and that there is a trade-off between Max profit and Max PaR.

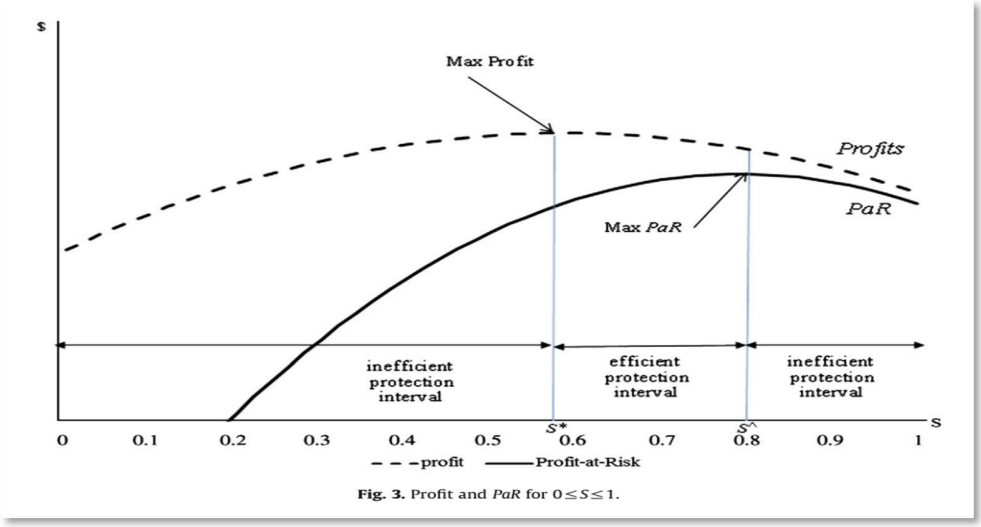


Figure 4: Profit-at-Risk Visualization (Lee, Kauffman, & Sougstad, 2011)

CHAPTER 3

Research Methodology

This chapter provides a thorough description of the processes and methods used to both collect and analyze the data. It provides an understanding of the methodology used in this study and enables for the assessment of the reliability and validity of the results. The research design, survey design, data collection, data cleaning, data analysis techniques, privacy and ethical consideration used in this study will be presented.

3.1 Research Design

The research design for this study was a cross-sectional survey that focused on the collection of data at a specific point in time, by administering a questionnaire to a large sample of SMBs in Norway (Schmidt & Brown, 2019). Quantitative methods were used to gather data from a large number of respondents that were subject to statistical treatments by using mathematical methods to analyze patterns, relationships and trends to either support or refute existing knowledge on this topic (Creswell & Creswell, 2018).

This study collected data on the topic of current information security practices, the number of information security incidents and the associated estimation of cost. Descriptive research was used to systematically describe the characteristics of this specific population and answer the research question, by using quantitative research methods to collect, analyze and interpret the data (Dulock, 1993). It was possible to describe the current state of the phenomenon of the aforementioned topics in the SMB sector. The data was gathered through a combination of both primary and secondary sources and was used to make estimates and generalizability of the findings (Leedy & Ormrod, 2012).

3.2 Survey Design

The primary source for obtaining data in this study was through conducting a survey, and a questionnaire was distributed to a large sample of SMBs in Norway. The questionnaire was based on several secondary sources and was used as inspiration for the design and formulation of questions to increase the quality of the questionnaire (Næringslivets Sikkerhetsråd, 2022; IBM Security, 2022). Although there were some questions added while other questions have been removed, adjusted and modified to better contribute to answering the research questions. The survey was administered by using an online survey platform called SurveyMonkey. To gather data and gain a better understanding of various challenges, different practices and opportunities within information security connected to the research questions, a fixed set of questions was formulated.

The questionnaire consisted of up to 24 questions (depending on selected options), and the time to complete the survey for each respondent was measured by MonkeySurvey, and the average time to complete was approximately 7 minutes. To reduce the number of participants abandoning the survey after beginning, the length and difficulty of the questions were tested by the supervisor, external advisor and industry professionals (with varying degrees of IT competence). Most of the questions were presented with a set of alternatives based on secondary sources, but also an option to elaborate and write additional information on some of the questions. There are also questions where the respondents were asked to cost estimate certain aspects related to information security incidents with the option to write in an input box.

The questionnaire is divided into five sections. The first selection is concerned with getting to know the respondent and the organizations, with questions regarding such as location, industry, revenue and number of employees. Lastly, matrix

questions were included; with rows representing different statements, the columns representing different answer options. The respondent had to select to which degree they agreed with the different statements. The statements had ordered answer options on a 5-point Likert scale from 1 = "strongly disagree" to 5 = "strongly agree".

The next section was concerned with leadership within the organization related to information security. These were mostly "yes" and "no" questions about whether the organization had cybersecurity insurance, implemented a framework for an information security management system, or a specific employee with information security as their primary area of responsibility.

The following section contained questions about information security culture within the organization. The questions were concerned with the frequency of how often information security policies and procedures were reviewed, information security training for employees, and reporting of deviations and unwanted incidents related to information security. All these questions had a pre-selected set of alternatives where some were "yes" and "no" questions, multiple-choice questions, and checkboxes.

The final section that was part of the standard path of the questionnaire contained questions about mapping the risks related to, and the number of information security incidents that had occurred. To map the perceived risk related to information security threats, a question was presented as a matrix question. Where the rows represented different threats, and the columns presented a Common Vulnerability Scoring System (CVSS) from "none" to "critical" for rating the severity of the security vulnerability. The next question was related to cost estimation of how much the respondent believed a data attack would cost on average for an affected organization, with an option to answer in

an input box. The last question was concerned with mapping which different types of information security incidents the organizations had been subject to. The question had a pre-selected set of answers in the form of checkboxes with the possibility of selecting multiple alternatives, and an option to elaborate in a text box. If the respondent had not been subject to an information security incident there was also an option to select "none of the above". If the respondent chose this option the survey was completed, but if the respondent had been subject to an information security incident they proceeded to another section.

This final part of the survey, which was explicitly for the respondents that had been subject to information security incidents, was concerned with the cost estimation related to these incidents. The questions in this section related to the respondents' cost estimation of various aspects that may have affected the total cost of the incident for the organization. These aspects include costs related to consultant services, loss of business, loss of data, reputation damage and loss of labor. To answer these questions the respondent had the option to write their answers in input boxes.

The survey was distributed in Norwegian, and there are a few reasons for that. Firstly, Norwegian is the official language of the country, and would therefore be more accessible and convenient for SMBs operating in Norway. Additionally, it was a strategic decision to reduce the possibility of misunderstanding or misinterpretation of the questions to ensure more accurate and reliable results. Finally, information security is a sensitive subject, and the use of the native language can contribute to establishing trust and credibility, which may have encouraged more SMBs to participate in the survey. The questionnaires, both in English and Norwegian can be found respectively in Appendix A and Appendix B.

3.3 Data Collection

According to (Thompson, 2012) sampling is defined as the process of selecting a subset of individuals from a larger population with the purpose of studying the whole population. Through surveying this subset, it was possible to collect data from a broad specter of SMBs in Norway and ensure representation from various sectors and locations.

A large population of companies from the SMB sector in Norway was obtained from Brønnøysund Register, which is a Norwegian government agency. The agency manages a public register of all organizations in Norway with additional information such as revenue, number of employees and contact information. The list was generated based on different criteria such as number of employees, location and industry. The organizations in the sample were selected with the criteria for SMBs in mind, and the location of the organization to include a diverse set of organizations from different counties in Norway.

The organizations received an invitation to participate in the study through a regular e-mail with information about the study, a link to the survey website, and instructions on how to complete the questionnaire. Before distributing the whole sample, it was conducted a test by e-mailing 100 randomly selected organizations. To increase credibility and trustworthiness the University of Stavanger student e-mail with the "@stud.uis.no"-domain was used for distribution. Since the e-mail contained a link to the survey website, there was a potential risk that the respondents believed the e-mail to be a phishing attempt and decided not to participate in the survey.

After completing the test, the rest of the organizations on the list received an e-mail with an invitation to participate in the research study. In total, 1272 potential participants received an invitation, where 254 responded. All the e-mails that

were sent were in Norwegian because of the same reasons the survey was in Norwegian as mentioned above. The data collection period started on February 14th and finished on April 15th of 2023. The distributed survey link allowed the receiver of the e-mail to take the survey on whatever device, wherever and whenever they preferred (until the survey was closed on April 15th).

3.4 Privacy and Ethical Considerations

The collection of data in this research study through the survey was conducted anonymously, and no personal data was gathered. Therefore, it was not necessary for an application to Sikt – Norwegian Agency for Shared Services in Education and Research (Sikt, 2023), previously called the Norwegian Center for Research Data (NSD). In the e-mail with the invitation sent to the organizations, all participants were informed that the survey was anonymous, and that the response would be treated confidentially.

3.5 Regression Analysis

Regression analysis is used as the primary statistical method for analyzing the data gathered through the survey. This method is used to examine the relationship between variables and make predictions. The two different types of regression methods used are linear regression and logistic regression.

3.5.1 Linear Regression

Linear regression is the simplest form of regression. It assumes a linear relationship between a dependent variable, and one or several independent variables, by estimating the effect of the independent variable on the dependent variable. The regression model finds the straight line that fits best and describes the relationship between the variables. Evaluating this relationship is done by using metrics such as P-values and R-squared. The P-value can range between 0 - 1. For

a 95% confidence level which is used as a basis in this thesis, a P-value < 0.05 gives statistically significant results. The R-squared is also in the range between 0 - 1 and states how much of the variance in the independent variable can be described by the independent variable(s) (James, Witten, Hastie, & Tibshirani, 2021).

3.5.2 Logistic Regression

In this thesis, an Excel Add-in named RegressIt was used to perform logistic regression. This specific type of regression model is commonly used when the dependent variable is binary. The general logistic regression model can be seen in Equation 1.

$$\hat{p} = \frac{e^{\beta_o + \beta_1 X}}{1 + e^{(\beta_o + \beta_1 x)}}$$

Equation 1: Logistic Regression Equation

By combining Equation 1 with a definition of "Odds Equation" and a logarithmic rule as seen in Equation 2, Equation 3 can be produced.

$$ODDS(A) = \frac{P(A)}{1 - P(A)}, \qquad \ln(e^a) = a$$

Equation 2: Odds Equation and a Logarithmic Rule

$$\ln\left(\frac{\hat{p}}{1 - \hat{p}}\right) = \beta_0 + \beta_1 X$$

Equation 3: Log-Odds Equation

Equation 3 is often referred to as the Log-Odds of outcome. The Log-Odds of the outcome equals a linear function of the X-variable. This shows that the logarithmic regression model has similarities with the linear regression model. The reason Logistic regression was used is that in contrast to linear regression, it always predicts the probability of outcome to be between 0 – 1 (Figure 5). The Graph to

the right in Figure 5 is known as a Sigmoid function, and this logistic regression line is described by Equation 1.

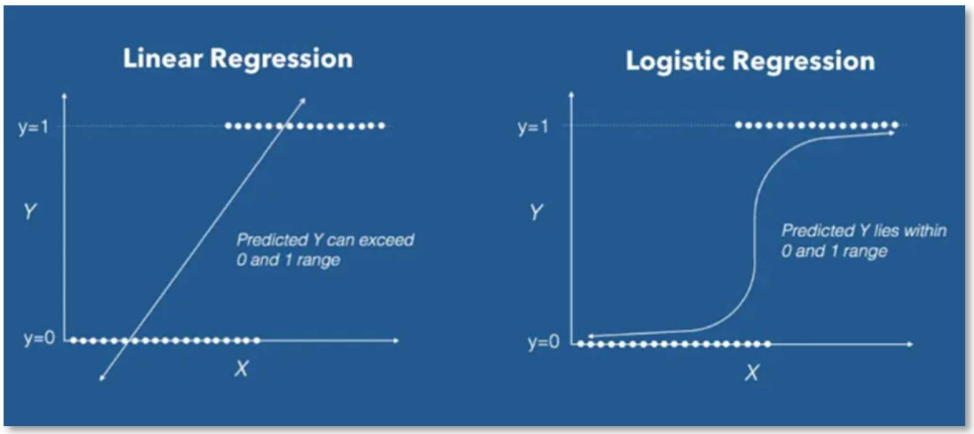


Figure 5: Linear Regression Versus Logistic Regression (Datascience, 2022)

Several regression models have been tested with different dependent and independent variables, to investigate if there are any patterns in which businesses suffer from data breaches, and how severe the consequences are. The different regression models are presented later in this thesis.

3.5.2.1 Logistic Regression Performance Metrics

For measuring the performance of the logistic regression models different indicators have been used. Odds-ratio is an important measurement to evaluate logistic regression models. The Odds-ratio is a variable that states how much the odds change with a one-unit increase in the independent variable while keeping the other independent variables constant. There are different ways of expressing Odds-ratio (Equation 4).

$$\frac{\frac{p_1}{1-p_1}}{\frac{p_2}{1-p_2}} = \frac{e^{\beta_0+\beta_1 x_{11}}}{e^{\beta_0+\beta_1 x_{12}}} = e^{\beta_1(x_{11}-x_{12})}$$

Equation 4: Different Ways of Expressing Odds-Ratio

A cutoff value was used for the model to predict if an observation is a failure (0) or a success (1). If a cutoff value of 0.5 is chosen the model treats observations with a predicted probability of 0.5 and higher as successes (a value of 1 on the binary 0 - 1 scale). If a true value of an observation is a success (1), and the model predicts it to be a success (1), the observation is correctly classified as a true positive. Sensitivity is a

measurement of the share of successes (1s) the model predicts to be successes (1s) with a specific cutoff value. If the true value of an observation is a failure (0), and the model predicts it to be a failure (0), the observation is a true negative. Specificity is a measurement of the share of failures (0s) the model predicts to be failures. If a value of an observation is a failure (0), but the model predicts it to be a success (1), the observation is misclassified, this is called a false positive. If the observed value is a success (1), but the model predicts it to be a failure (0) it is called a false negative (James, Witten, Hastie, & Tibshirani, 2021).

A ROC curve can be made with specificity on the X-axis, and 1 – sensitivity on the Y-axis. The ROC curve consists of many data points of different cut-off values forming the ROC curve, and an example of a ROC curve can be seen in Figure 6. The area under the curve tells how well the model predicts the outcome. The dotted line is a random classifier, and the area under the dotted line is 0.5. The theoretical maximum area under the ROC curve is 1, if the area under the ROC curve is greater than 0.5 it performs better than the random classifier.

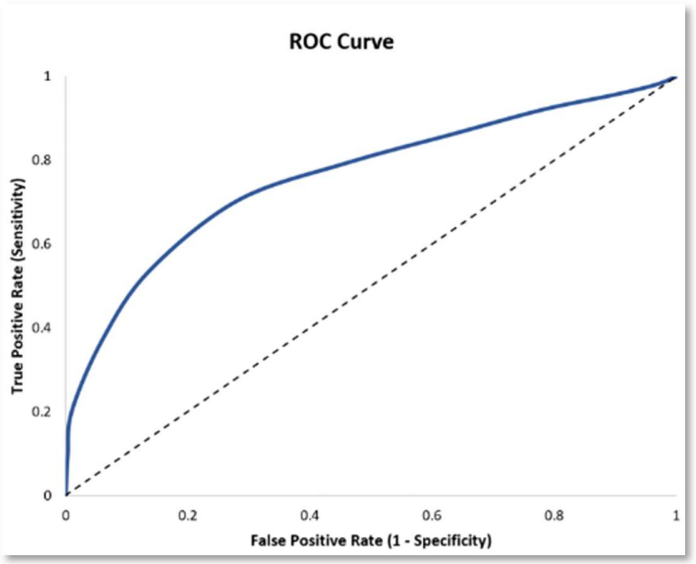


Figure 6: Example of a ROC Curve (Bobbitt, 2021)

CHAPTER 4

Summary Statistics

This chapter presents a summary of the collected data from each question from the questionnaire. It provides an overview of statistics and presents a visual representation of the central tendencies, variability and distribution of the data through tables, charts and figures to give a better understanding of the results.

4.1 General Respondent Information

The survey was distributed to 1274 organizations with a response rate of 19.9 percent (254 respondents) before cleaning the sample. Some of the responding companies had up to 2000 employees and were way bigger than the definition of SMB, these responses were removed. Some respondents were slightly bigger than the definition of SMB but were kept in order to increase the number of respondents close to 100 employees. By looking at the responses it could also be seen that some responding companies misunderstood the survey, or did not take it seriously, and these companies were also removed. The final response rate was 18.5 percent (236 respondents).

The 236 respondents were from 12 different industries, of which the majority of organizations were from the technology industry (21.2 percent), and construction and building operations (17.8 percent). Several requests had to be sent out to get a sufficient number of responses from organizations within other sectors like healthcare (3.0 percent), transport and storage (4.2 percent) and education (4.7 percent) (Figure 7). To get a realistic overview of the whole SMB sector in Norway the sample was gathered from all 11 administrative counties in Norway, with the majority of respondents located in Oslo (17.0 percent), Rogaland (14.0 percent) and Viken (15.7 percent) (Figure 7). Some regions are more densely populated

than others, therefore there were more respondents from the capital Oslo than from Nordland (3.4 percent).

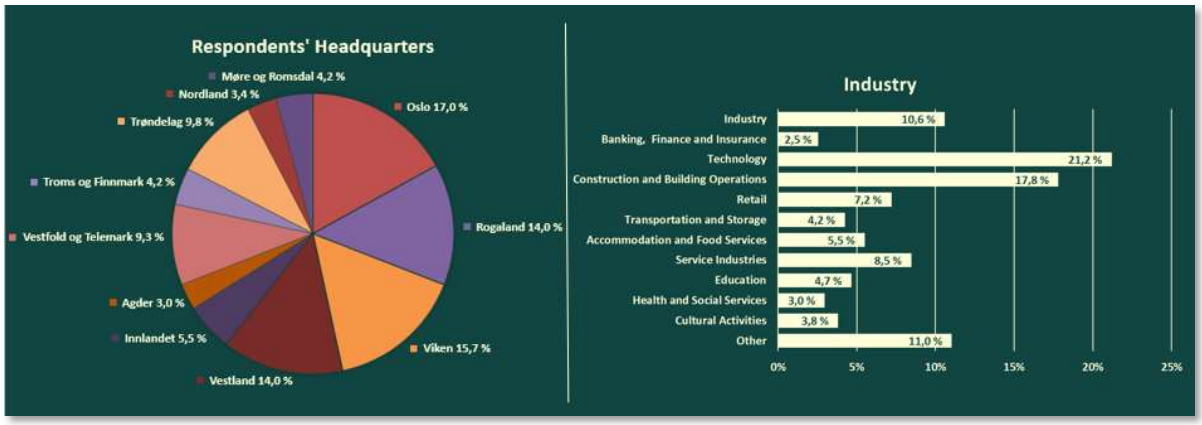


Figure 7: Headquarters' Location and Industry

Many of the questions in the questionnaire required the respondent to have some knowledge about the organization's information security and economics. In order to get as correct data as possible, the e-mail invitation asked the recipient of the email to preferably forward the e-mail to someone with this knowledge in the organization. The next figure displays the respondent's roles in the organization. The majority, with 71.6 percent of the respondents were the CEO of the companies. 11.9 percent and 7.2 percent of respondents respectively had an IT role or was a financial manager, while the remaining 9.3 percent had other roles (Figure 8).

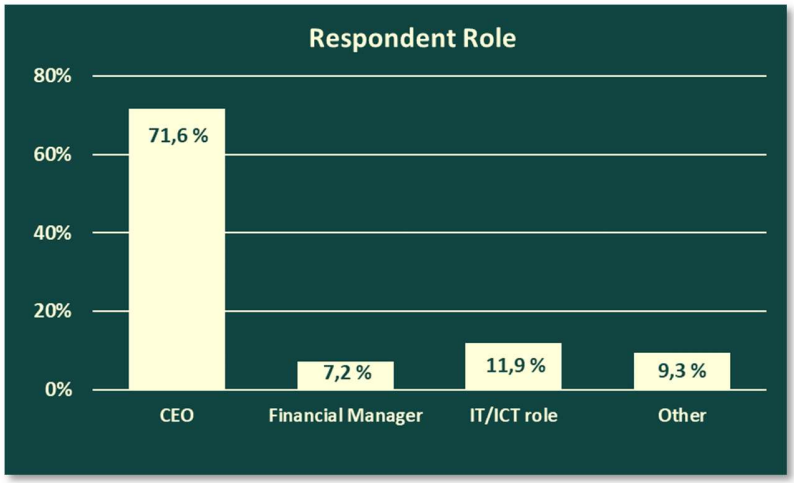


Figure 8: Respondent Role

The number of employees in the organizations in this study varied between 4 to 100 employees, and the average number of employees was 24. Another important factor to gather information about was the annual revenue of the organization, and the average annual revenue was 68.9 MNOK. In Figure 9 each of the dots represents a responding company´s number of employees on the X-axis, and yearly revenue on the Y-axis.

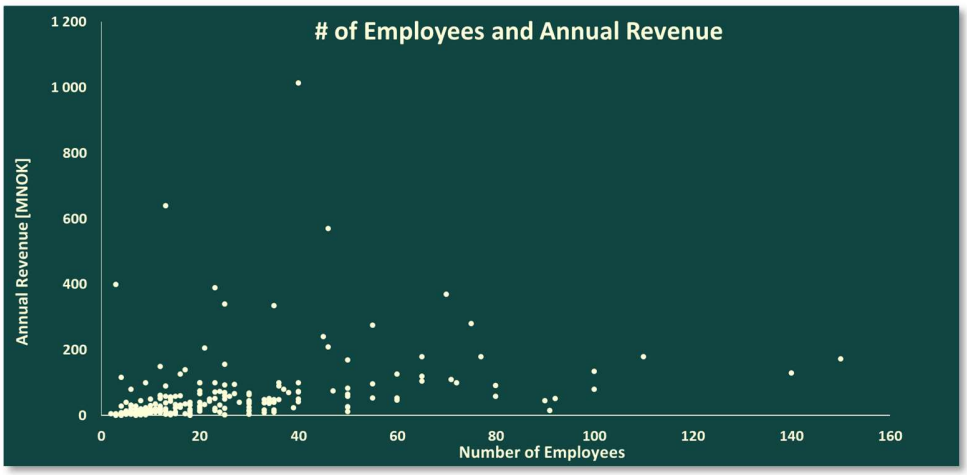


Figure 9: Number of Employees and Annual Revenue.

As previously mentioned, this thesis was written in collaboration with Varde Hartmark, which specializes in business consulting and mainly delivers services to private companies. The goal of this survey was to target private companies, and 96.9 percent of the participants in the survey were from the private sector (Figure 10). As previously mentioned, these public organizations were removed in the data-cleaning process.

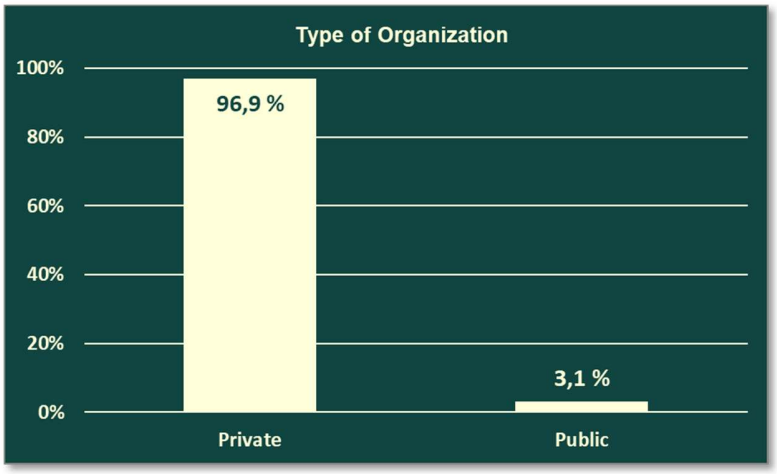


Figure 10: Type of Organization

4.2 General IT Information/Leadership

Information technology is for many companies something outside their main competence. Therefore, companies have the possibility of having IT operations either completely outsourced or partially outsourced to a third party, or internally organized. Figure 11 displays the respondent's organization of IT operations, 28.8 percent have it completely outsourced, 37.7 percent have it partially outsourced, 32.6 percent have it internally organized, while only 0.9 percent did not know the answer (Figure 11).

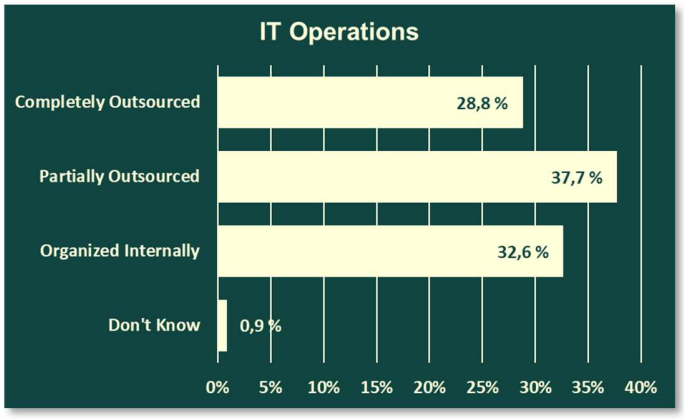


Figure 11: IT Operations

The majority of the organizations reported having an employee with information security just being a part of their responsibility (45.6 percent). Only 14.9 percent

had an employee where the main responsibility was information security, while 38.6 percent did not have an employee with information security as their main responsibility (Figure 12). From Figure 12 it is clear that most organizations (67.5 percent) do not use a framework in the work with information security, with only 17.5 percent using some form of framework.

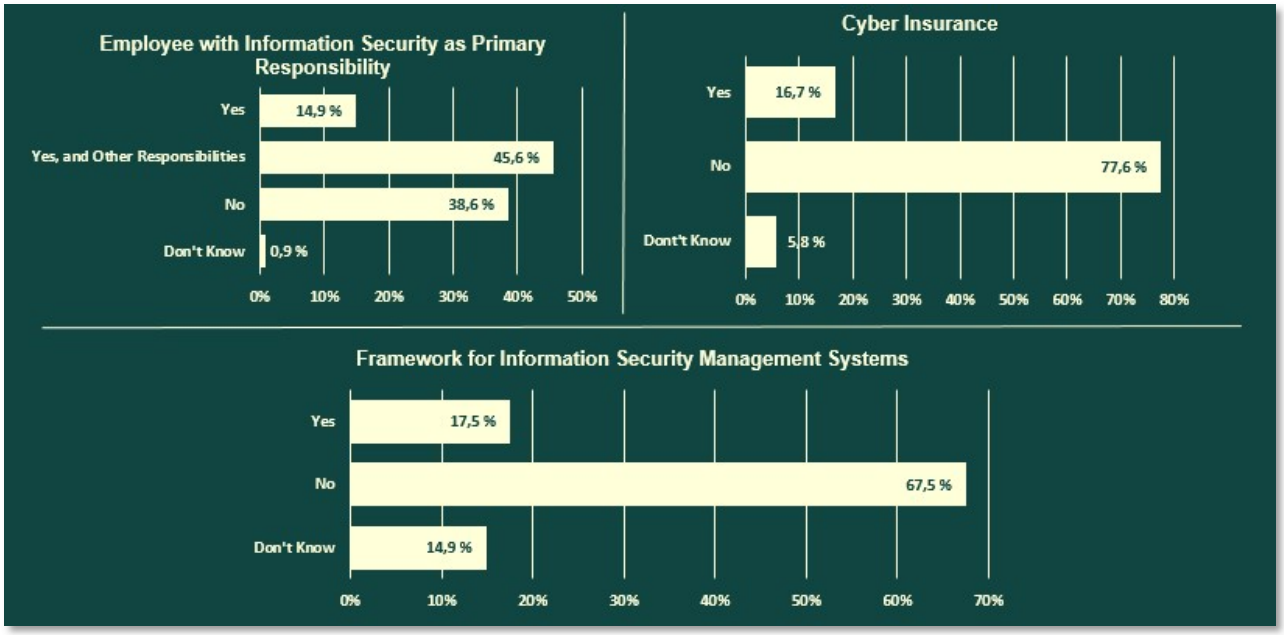


Figure 12: Main Role, Cyber Insurance, Framework

Out of the total, 16.7 percent of the participants had purchased cyber insurance, while the majority 77.6 percent had not purchased it. 5.8 percent of respondents did not know whether the organization had purchased cyber insurance or not (Figure 12).

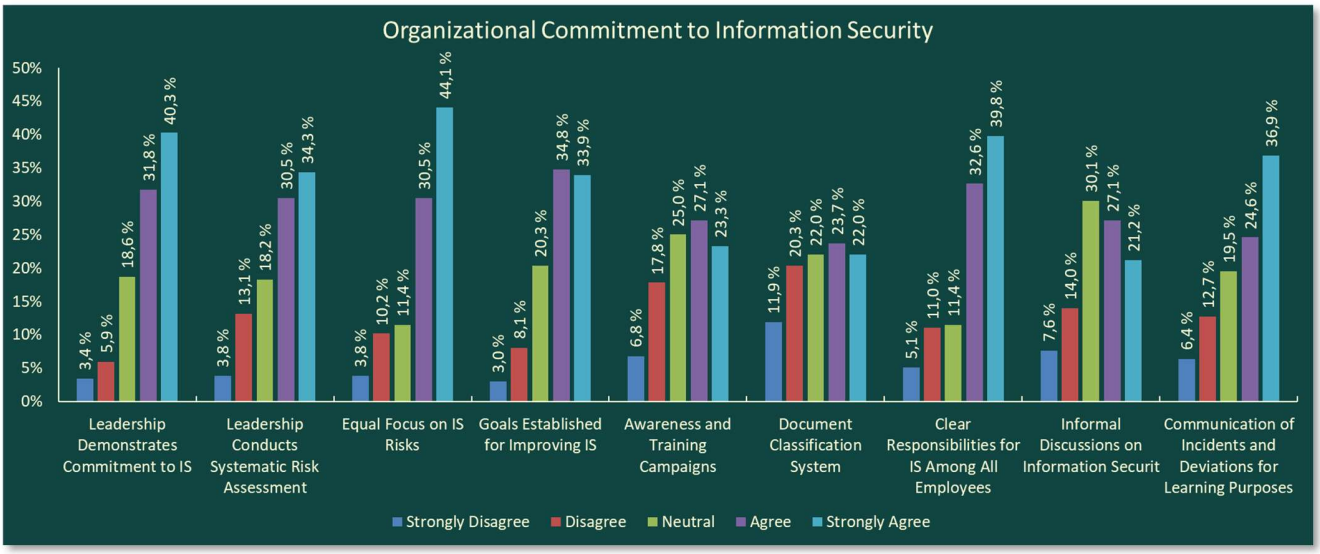


Figure 13: Organizational Commitment to Information Security Statements

When assessing the organization's commitment related to information security the respondent answered using a 5-point Likert scale from "strongly disagree" to "strongly agree". The majority of the respondents (40.3 percent) "strongly agreed" and 31.8 percent "agreed" that leadership demonstrates a commitment to information security, and 44.1 percent answered that there is equal focus on information security risks (Figure 13). On the other hand, 13.1 percent "disagree", and 3.8 percent "strongly disagree" that leadership conducts systematic risk assessment. Similarly, a significant portion of respondents, 17.8 percent "disagree" and 6.8 percent "strongly disagree" that awareness and training campaigns were carried out (Figure 13). The average weighted scores for the statements range from 3.24 to 4.01. The statement "clear responsibilities for information security among all employees" received the highest score 3.91, and "document classification system" received the lowest score 3.24.

4.3 Information Security Culture

Technology develops rapidly, which means that the cyber threat is constantly changing, and an organization has to adapt in order to protect itself from threats. A question was asked to find out the procedure for reviewing information security

procedures and guidelines. 35.5 percent reported the organization reviews it regularly, and 36.8 percent conduct ad hoc reviews, while 19.1 percent of the respondents did not have a systematic approach to it or do not have procedures and guidelines at all, and 4.6 percent stated the policies were outdated (Figure 14).

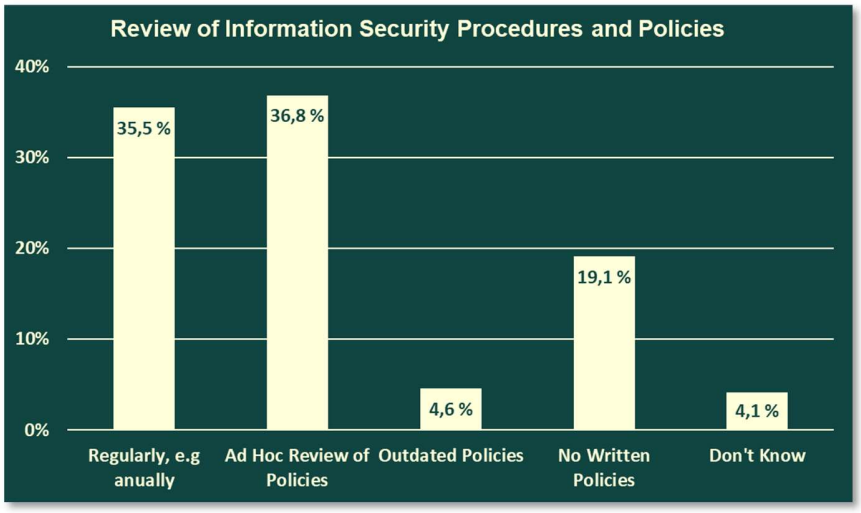


Figure 14: Review Policies

Knowing how to act as an individual in order to reduce the risk of information security incidents is not easy. Procedures and guidelines are worthless if the employees do not know how or about them. Figure 15 indicates that the majority of respondents receive one-on-one training (42.3 percent), followed by training related to password use and management (36.8 percent) and requirements for handling sensitive and confidential data (29.1 percent). Additionally, 21.4 percent of the respondents reported that employees in the organizations do not receive training in any of the items on the list (Figure 15).

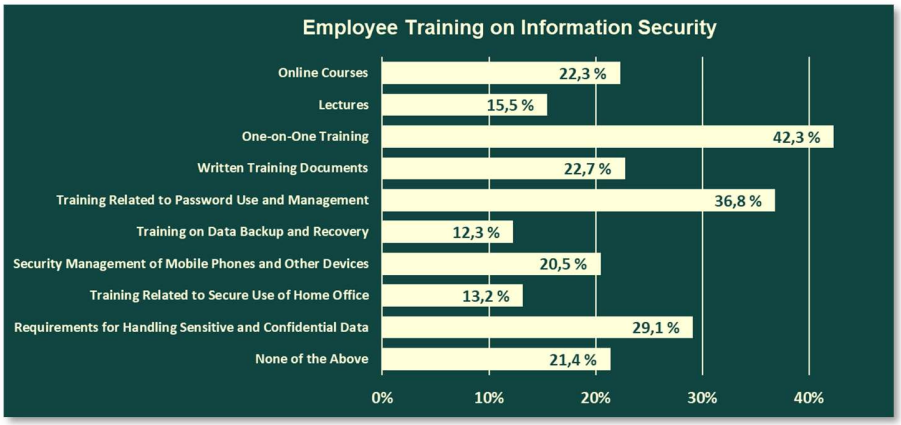


Figure 15: Employee Training

Regarding whether information about how employees can report deviations and unwanted incidents related to information security had been made available and communicated, 38.6 percent reported it was provided in writing, 34.1 percent orally and 26.4 percent did not make it available (Figure 16). When reporting or notifying about deviations and unwanted incidents, 49.1 percent report directly to the immediate supervisor. 20.5 percent report to the IT department and 18.2 percent used a digital notification system for reporting, while 9.1 percent of the respondents had no formalized way to report (Figure 16). In regard to whether the employees are kept up to date about ongoing threats, activity, deviations or incidents related to information security the majority (54.1 percent) answered that all employees are informed in the event of an incident. 21.8 percent reported only a limited group of employees are informed, and 20.5 percent of the respondents did not have a procedure to inform employees (Figure 16).

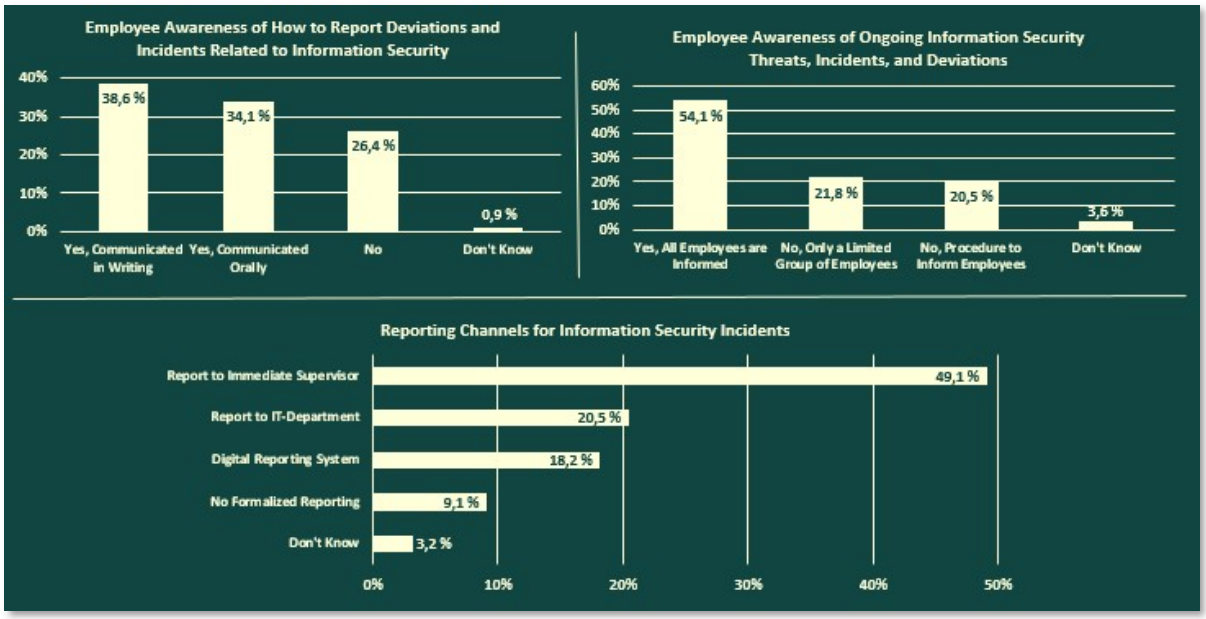


Figure 16: How to Report, Reporting Channels and Employees' Awareness of Ongoing Threats

4.4 Mapping Risks and Information Security Incidents

When assessing the risk and likelihood of different information security incidents, the participants responded using the Common Vulnerability Scoring System (CVSS) ranging from none to critical. The weighted average score for each of the incidents ranged from 2.81 to 3.11. The incident considered most likely to occur was a data breach, where 39.3 percent of the respondents rated it as moderate risk and 15.0 percent rating as high risk (Figure 17). The second most likely incident to occur was malware and viruses with 41.6 percent rating it as having moderate risk and 21.5 percent rating it as having high risk. Phishing and social engineering and Ransomware had an average rated score of 3.1 and 2.81 respectively. The incident assesses to have the least likelihood of occurring was unauthorized use and access to systems, with 39.7 percent rated it to have low risk, and 35.1 percent rated it to have moderate risk (Figure 17).

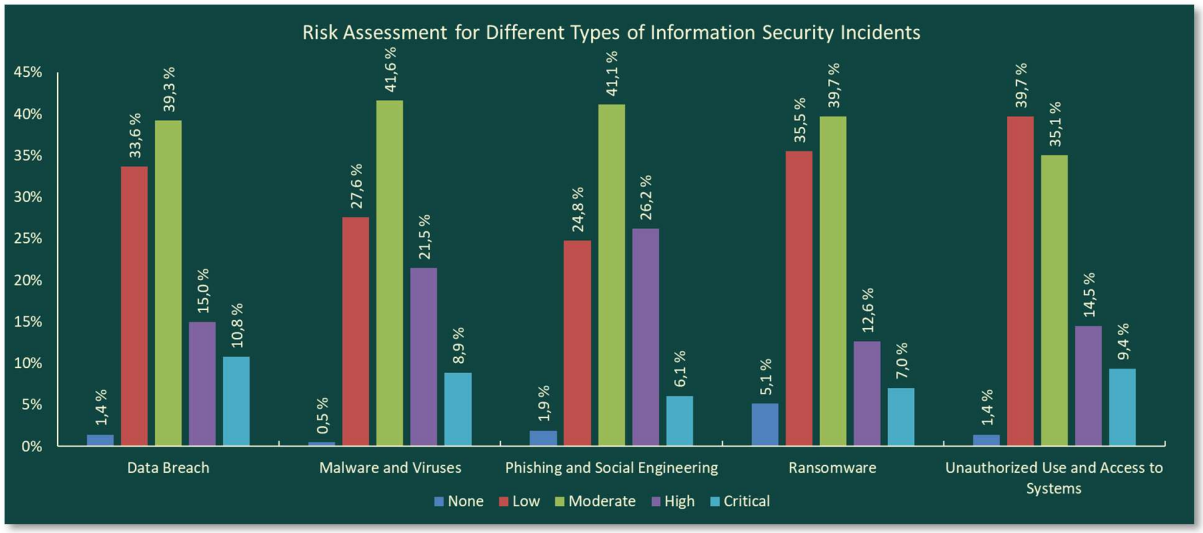


Figure 17: Risks Assessment

Out of all the respondents, 65.4 percent of the respondents reported that the organization had not been subject to information security incidents in the last four years (Figure 18). Among the organization that had experienced an information security incident, reported unintentional incident by an employee (14.0 percent) as the most common, followed by phishing-attack (8.4 percent), theft of ICT equipment (4.2 percent) and ransomware (4.2 percent). The other incidents such as loss of personal data, intentional incidents carried out by employees and affected by malicious software accounted for less than 3.0 percent of reported incidents (Figure 18).

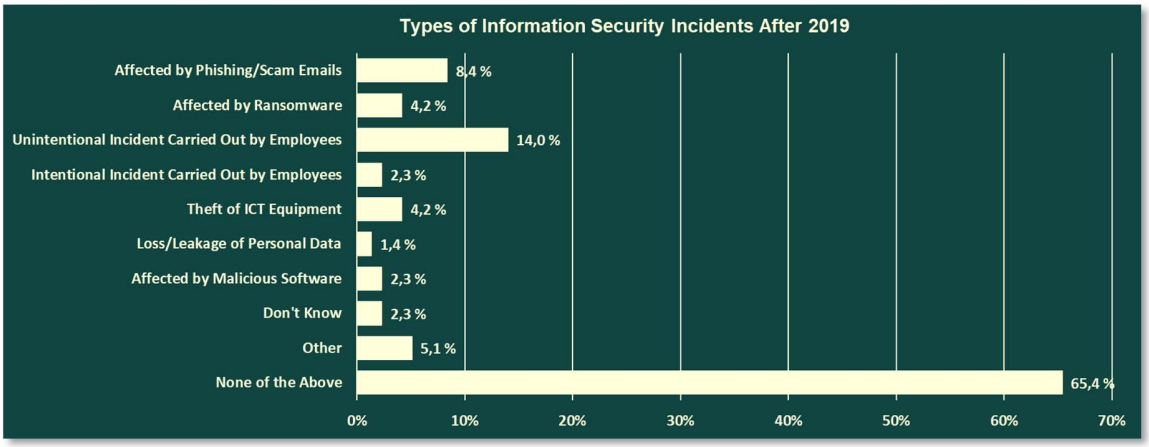


Figure 18: Information Security Incidents after January 2019

4.5 Cost Estimation of Information Security Incidents

As part of the standard path of the questionnaire, the respondents had to make a guess/ estimation of what they believed the average cost for any information security incident in the Norwegian SMB sector to be. The respondents estimated the average cost to be 2.65 million NOK, with the median guess/estimate being 500 000 NOK. In Figure 19 each of the dots represents the guess/estimation of the average cost of a data breach. The Y-axis is logarithmic due to the big spread between guesses. Each of the guesses is chronologically listed from smallest to largest along the X-axis. Some of the respondents answered "blank" on this question, which is why there are only approximately 180 respondents.

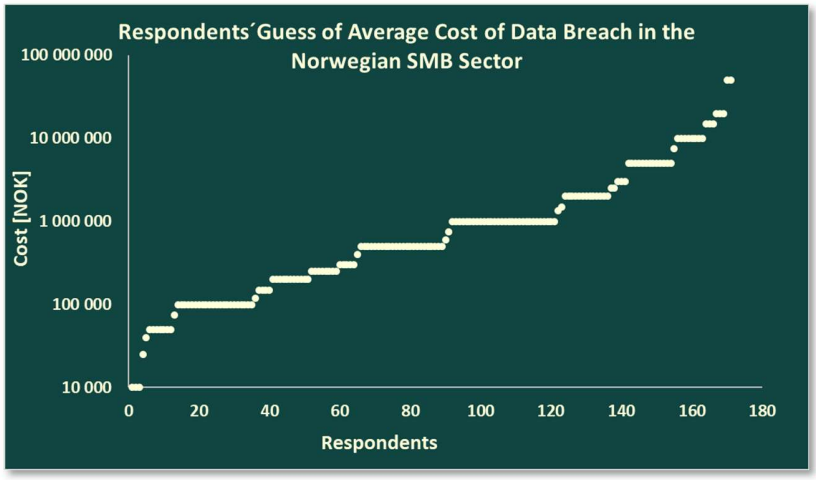


Figure 19: Respondents Guess / Estimation of The Average Cost of a Data Breach in the Norwegian SMB Sector

As part of the questionnaire depending on whether the respondent had been subject to a data breach, the respondent estimated the cost of different factors related to the specific incident. If the respondent had been subject to more than one data breach during the period, the most critical data breach was considered for the cost estimation questions. Figure 19 displays the estimated cost of factors that may impact the total cost of an information security incident such as consultant services, loss of business, loss of data, loss of reputation, or loss related to labor.

The most common cost, with 18 respondents reported consultant services as a cost related to the incident. The cost of consultancy also happens to be the costliest of the five categories with an average cost of 1.42 MNOK (Table 1). There are big differences in the average and median costs, and three out of the five cost categories actually have a median cost of 0 NOK.

	Total Cost	Consultants Cost	Lost Business	Lost Data	Lost reputation	Loss of Workforce
Average	4 311 436	1 422 225	930 610	380 526	642 632	935 443
Median	135 000	10 000	0	0	0	15 000
Max	50 000 000	30 000 000	15 000 000	5 000 000	10 000 000	10 000 000

Table 1: Cost Estimation of Data Breaches

Out of the 236 respondents, 70 participants had been subject to a data breach, where nine of these respondents had been subject two times, and two respondents had suffered three times. The costliest incidents had a total cost of 50 MNOK. Out of all the data breaches, 12 had a total cost higher than 1 MNOK, 18 had a cost lower than 100 000 NOK, and the rest of the data breaches had a cost between 100 000 NOK and 1 MNOK (Table 2)

Number of Respondents	236
Total companies Exposed to Incident	70
Total # Incidents	83
Companies Exposed 2 Times	9
Companies Exposed 3 Times	2
Most Costly Incidents	
Total Hacked	50 000 000
Ransomware	50 000 000
Accidental Event of Employee	22 095 000
Theft of IT-Equipment	11 000 000
Malicious Software	6 950 000
Accidental Event of Employee	5 000 000
Number of Incidents Cost > 1 000 000	12
Number of Incidents Cost < 100 000	18

Table 2: Overview of Data Breaches

4.6 Margin of Error

All surveys have a margin of error, due to statistical uncertainty. A 95% confidence interval is calculated for each question by using Equation 5. With 236 responses there is a 95% probability that the correct answer is within +/- 1.53 percent to +/- 6.59 percent of the results from the survey, depending on the percentage result on each question.

$$\left[p - 1.96\frac{\sqrt{f(1-p)}}{\sqrt{n}}, p + 1.96\frac{\sqrt{p(1-p)}}{\sqrt{n}}\right]$$

n = number of responses
f = the frequency of the answer
p = probability of the answer

Equation 5: 95 % Confidence Interval

CHAPTER 5

Results

The purpose of this chapter is to present in-dept analysis of the responses from the survey, as well as combining findings from the different questions in the survey in order to answer the research questions.

5.1 Differences Between Industries

Firstly, it was interesting to look at the differences between industries when it comes to average yearly turnover and the average number of employees in each industry. The respondents were given 9 statements regarding information security culture and leadership. They rated their company on a Likert scale from strongly disagree – strongly agree, which was converted to a score from 1 - 5. The total possible score can vary from 9 – 45, and this score will in this thesis be referred to as "Culture Security Score" (Table 3). A company with a high "Culture Security Score" is assumed to have a high "Culture Security Level", which is to some degree comparable with the "Information Security Level" presented in the Methodology chapter.

Industry	Average Yearly Turnover (NOK)	Average Number of Employees	Culture Security Score
Health and Social Services	22 807 018	34	83 %
Technology	35 618 408	22	82 %
Bank / Finance / Insurance	505 440 000	37	79 %
Other	90 617 017	29	78 %
Service Industry	35 993 871	25	76 %
Transportation and Storage	90 329 000	30	76 %
Education	31 370 000	28	74 %
Retail	140 647 059	27	73 %
Industry	103 825 000	35	69 %
Accommodation and Food Services	26 953 846	21	68 %
Cultural Activities	41 222 222	31	67 %
Construction and Building Operations	76 451 645	24	66 %

Table 3: Differences between Industries

The top three scoring industries are Health and Social Services (83 percent), Technology (82 percent) and Banking/Finance/Insurance (79 percent) as shown in Table 3. Banking/Finance/Insurance handle large sums of money and follows strict information security regulations such as the Norwegian IT regulation (Finansdepartementet, 2022). Companies within health and social services handle personal information about patients, which is also strictly regulated (Normen, 2022). The technology industry which in general is familiar with computer science, might have more knowledge about the threats regarding cyber-attacks, and therefore know how important it is to prioritize it. While the three lowest-scoring industries all have relatively low yearly turnover and usually do not handle critical information about customers. It is important to mention that some of the industries have few respondents and that coincidences can therefore play a significant role in these findings.

Furthermore, it was interesting to look at the differences between the number of data breaches and the cost of data breaches in the different industries (Table 4). As mentioned above some industries have few respondents, the two industries with the most respondents are therefore compared: The technology sector has a significantly higher "Culture Security Score" than the construction and building operations sector. The technology sector also has a lower yearly turnover and fewer employees. Despite these differences, the result from this survey indicates that the probability of an attack in the technology sector is 50 percent higher than in the construction and building operations sector, over a 4-year period. Both the average and the median cost of the incidents are also higher in the Technology sector (Table 4).

Industry	Average Cost	Median Cost	Companies Subject to Data Breaches	Number of Data Breaches
Bank / Finance / Insurance	3 425 000	3 425 000	67 %	4
Education	75 000	75 000	55 %	6
Retail	27 500	25 000	47 %	8
Cultural Activities	36 500	36 500	44 %	4
Transportation and Storage	11 341 000	170 000	40 %	4
Technology	1 162 333	700 000	36 %	18
Industry	16 661 000	11 000 000	36 %	9
Other	2 395 000	230 000	35 %	9
Accommodation and Food Services	10 000	10 000	31 %	4
Health and Social Services	30 000	30 000	29 %	2
Service Industry	325 333	425 000	25 %	5
Construction and Building Operations	746 667	210 000	24 %	10

Table 4: Differences in Cost and Incidents in Industries.

It looks like some industries are more vulnerable to attacks than other industries. The reasons behind these differences can be because of the volume of data the industry handle and the value of this data (Verizon, 2023). The technology sector is known to have valuable data, which is attractive to hackers. The information handled by the Construction and building operations sector on the other hand is not considered as high-risk, even though there is an increasing trend due to a growing use of the Internet of Things (Verizon, 2023)

5.2 Number of Employees and Yearly Turnover

A logistic regression analysis is made where the relationship between the size of companies (number of employees and yearly turnover) and the probability of information security incidents is investigated.

The dependent variable is binary. Companies that have suffered from a data breach get a value of 1, and companies that have not suffered from a data breach get a value of 0. There are two independent variables: The number of Employees, and Yearly Turnover. Since the respondents were asked if they had

suffered from a data breach over a 4-year period the results also indicate probabilities for data breaches over a 4-year period.

Two different regression models are tested with "Number of employees" and "Yearly Turnover". The P-value for "Number of employees" was 0.059 and the P-value for "Yearly Turnover" was 0.06, meaning that both of the independent variables were slightly above the requirement of 0.05 for being statistically significant on a 95 % confidence level. However, when the two independent variables were tested in the same regression model, the P-values were 0.185 for "Employees" and 0.177 for "Yearly Turnover". This shows that there is quite a strong correlation between the two independent variables. Even though the results are not statistically significant, they are still valuable to present and discuss. The coefficients are plotted in the regression equation and presented in Equation 6.

$$\hat{p} = \frac{e^{-0.737+0.006715n_{employees}+0.001631n_{turnover}}}{1 + e^{-0.737+0.006715n_{employees}+0.00161n_{turnover}}}$$

Coefficients:
Constant: -0.737
Employees: 0.006715
Yearly Turnover [MNOK]: 0.00161

Equation 6: Regression Equation

The regression equation is plotted in two Sigmoid graphs. Figure 20 shows the probability of a data breach with rising yearly turnover for a company. There is a clear positive relationship between yearly turnover and the probability of data breaches. The upper and lower 95 % confidence interval is plotted as dotted lines. This means that according to the model, it is a 95% probability that the true value falls between the two dotted lines. These lines are created by calculating the confidence interval on 13 equally spaced values on the X-axis and drawing a smoothed line between the data points. Since the survey has very few observations of companies with yearly turnover > 500 MNOK, the uncertainties are much greater in the upper interval. It is also worth mentioning that the upper

dotted line never exceeds 1.0, simply because the probability of a data breach cannot be greater than 1.0 (Figure 20).

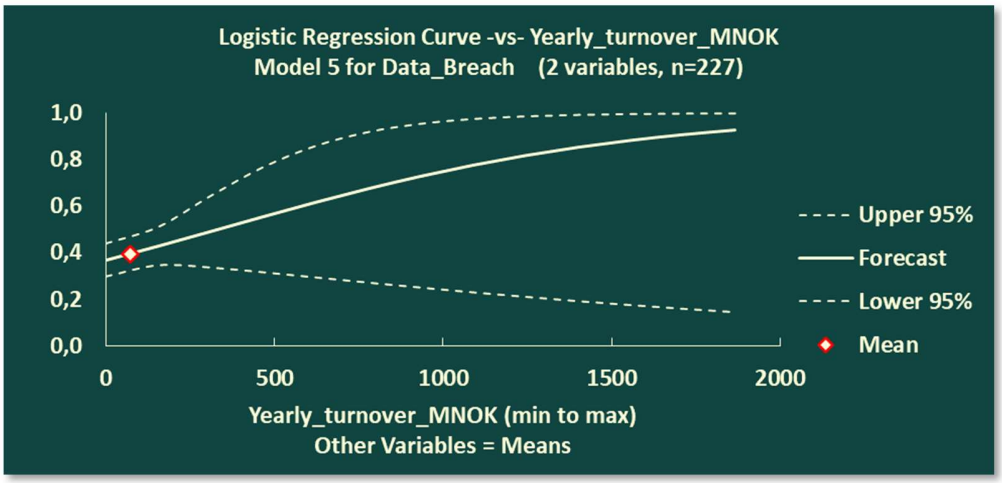


Figure 20: Relationship between "Yearly Turnover" of a Company and the Probability for a Data Breach

Figure 21 shows the probability of a data breach with the rising number of employees. In this particular calculation, the respondents who had between 100 – 400 employees were also added. This was done in order to compare the SMB sector with companies that are slightly bigger. Due to few observations over 100 employees, the uncertainties are greater in the upper interval. Since this thesis only focuses on the SMB sector, most of the responding companies had less than 50, which makes the confidence level relatively narrow below 50 employees.

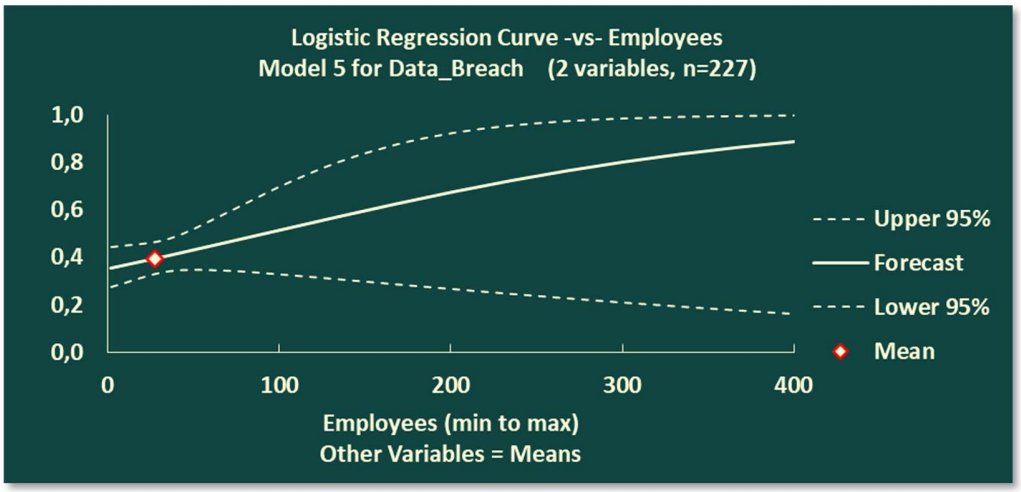


Figure 21: Relationship between "Number of Employees" and the Probability of a Data Breach

The solid white line in Figure 22 represents a ROC curve. The area under the ROC curve is 0.54, which means that the model is slightly better than a random classifier to predict outcomes. The area under the dotted line is 0.50, and the dotted line represents a random classifier (Figure 22).

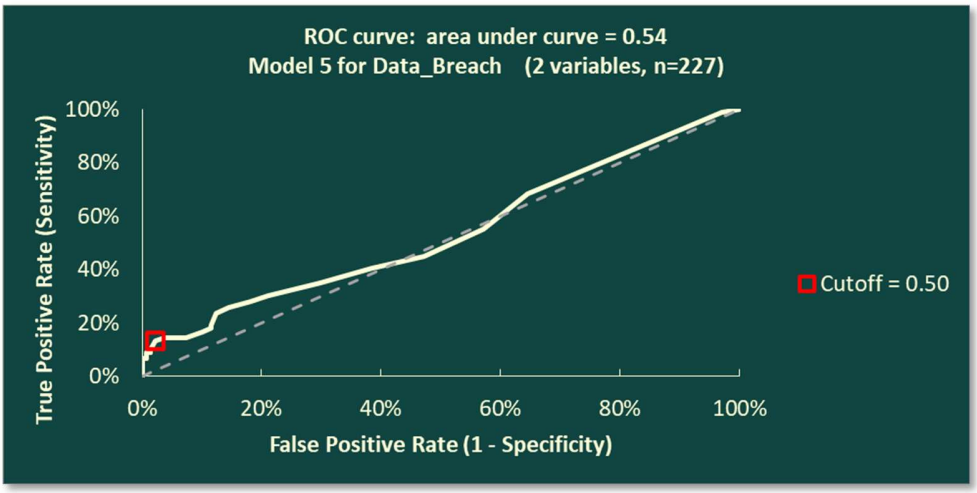


Figure 22: ROC Curve with Cutoff Value of 0.5

The cutoff value is set to 0.5. This means that if the model predicts the probability of a data breach for a specific company to be 0.5 or higher, the model classifies the company as a 1, on the binary 0 - 1 scale. The model predicts most of the smallest responding companies to have a probability of data breach in the interval between 0.3 and 0.4, which means that they are classified as a 0 on the binary 0 - 1 scale. With a cut-off value of 0.5, the model only predicts 15 companies to have suffered from a data breach, which is very low. However, out of the 15 predicted companies, 12 of the companies have actually suffered from a data breach. All the different outcomes of the model can be seen in the classification table below. At a cutoff value of 0.50, the model predicts 64.8 percent correct, with a true positive rate of 13.5 percent and a true negative rate of 97.8 percent (Table 5).

Cutoff value for prediction of Yes: 0,50 RMSE = 0,481

Actual:	Predicted: # No	Predicted: # Yes	Total
# No	135	3	138
# Yes	77	12	89
Total	212	15	227
Percent correct =	64,8%	True positive rate =	13,5%

Actual:	Predicted: % No	Predicted: % Yes	Total
% No	59 %	1 %	61 %
% Yes	34 %	5 %	39 %
Total	93 %	7 %	100 %
True negative rate =	97,8%		

Table 5: Classification Table for the Logistic Regression Model

These results indicate that the two predictors have limited ability to predict outcomes and that the variation cannot be explained completely by the two predictors. There might be some important explanatory variables that are not found in this thesis. Another possibility is that apart from the number of employees and yearly turnover, it might actually be quite random which companies are exposed to data breaches.

Odds-ratio is another important measurement to evaluate the logistic regression model. It gives information about how the odds for a data breach change with one unit change in one of the independent variables ("number of employees" or "Yearly Turnover") while keeping the other independent variable constant.

The Odds ratio for a company with constant yearly turnover and a rising number of employees was calculated with the use of the Logistic regression equation (Equation 1) and the equation for Odds-ratio (Equation 4) presented in Chapter 3. Since the SMB sector is defined as businesses with up to 100 employees, intervals of 10 employees were chosen. In the same way, the Odds-ratio for a company with a constant number of employees and rising turnover was calculated. The yearly turnover for the responding companies was up to 2000 MNOK, intervals of 100 MNOK were therefore chosen. The Odds-ratios are presented in Table 6. It is important to mention that this is the percentage increase in the odds, not the percentage change in the probability of a data breach.

Increase in # Employees	Odds Ratio	% Increase in Odds	Increase in Turnover [MNOK]	Odds Ratio	% Increase in Odds
10	1,07	7 %	100	1,18	18 %
20	1,14	14 %	200	1,39	39 %
30	1,22	22 %	300	1,63	64 %
40	1,31	31 %	400	1,92	92 %
50	1,40	40 %	500	2,26	126 %
60	1,50	50 %	600	2,66	166 %
70	1,60	60 %	700	3,13	213 %
80	1,71	71 %	800	3,69	269 %
90	1,83	83 %	900	4,34	334 %

Table 6: Odds-ratio by Increase in Number of Employees and Turnover.

To better understand the concept of the Odds-ratio and the table above, it is explained by an example of a fictitious company A. Company A has 20 employees and 80 MNOK yearly turnover. The probability of a data breach over a 4-year period for the company is calculated with the regression equation:

$$\hat{p} = \frac{e^{-0.737+0.006715*20_{employees}+0.001631*80_{turnover}}}{1 + e^{-0.737+0.00671 *20_{employees}+0.001631*80_{turnover}}} = 0.384$$

The odds for a data breach for company A is:

$$\frac{P(A)}{1-P(A)} = \frac{0.384}{1-0.384} = 0.624$$

If the yearly turnover for company A rises from 80 MNOK to 280 MNOK (while still being 20 employees) the odds can simply be multiplied by 1.39 (Table 6) which gives an odd of 0.864. Now that the odd is known, it is easy to calculate the new probability of 0.464, as seen from the calculation below.

$$\frac{P(A)}{1-P(A)} = 0.864 \rightarrow P(A) = 0.464$$

5.3 "Culture Security Level" and Probability of Data Breaches

The relationship between "Culture Security Level" and the probability of an information security incident is investigated with logistic regression analysis.

The companies are asked if they have been subject to an information security incident (yes/no). This answer is transformed into a binary 0 - 1 variable, which is the dependent variable in a logistic regression analysis. The total "Culture Security Score" (9 - 45) is used as the independent variable. The results of the regression analysis can be seen in Figure 23. The results indicate that there is a slight decrease in the probability of data breaches with rising security scores. The model estimates that a company with a very low "Culture Security Score" has a 48 percent chance of having a data breach over a 4-year period, while a company with a high "Culture Security Score" has a 39 percent chance. Few of the responding companies had a "Culture Security Score" below 20, this makes the spread between the upper 95% and the lower 95% confidence interval quite big for lower scores (Figure 23).

Figure 23: Regression Results

The P value to "Culture Security Score" is 0.541 which means that the results from this regression analysis are far from statistically significant. There can be several reasons why the model fails to find a statistically significant result:

- The survey fails to ask the right questions to give a realistic "Culture Security Score".
- The companies that have experienced an information security incident have taken information security more seriously after the incident and therefore get a quite high score.

- The statements are rated by an insider in the company, often the CEO. It is his/her subjective opinion. The subjective opinion might differ from the actual "Culture Security Level" in the company.
- There might not be a relationship between which companies in the Norwegian SMB sector that are subject to a data breach, and their focus on information security culture.

A regression model of the relationship between each individual question and the probability of an information security incident is also tested. Only 1 out of the 9 questions were close to significant. The statement: "All employees know who has the main responsibility for information security" had a P-value of 0.068 which is very close to being statistically significant on a 95% confidence level (Figure 24).

The regression results indicate that companies that answered, "Strongly Agree" (5 points) on the statement had a lower probability of experiencing a data breach than companies that had an answer corresponding to 4 points or lower (Figure 24). Since nine regression analyses were performed it is however likely that one of them is close to being statistically significant simply by chance.

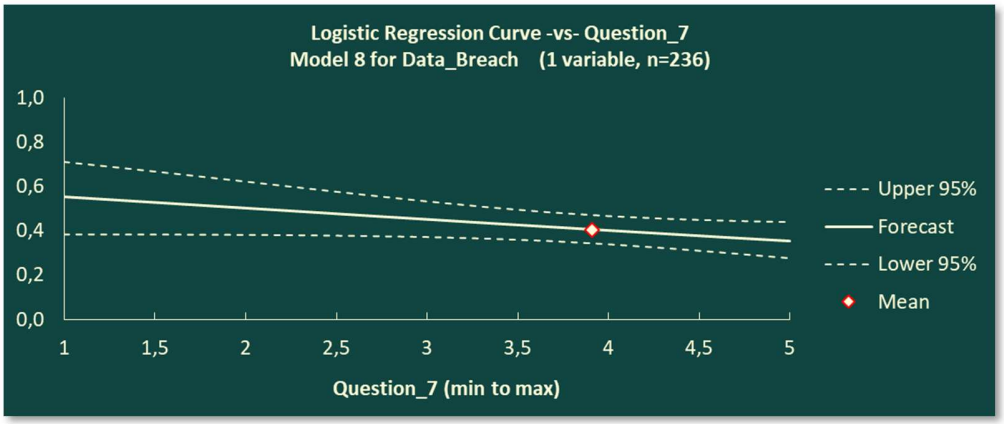


Figure 24: Relationship between Statement 7 and Probability of a Data Breach

5.3.1 "Culture Security Level" and Cost of Data Breaches

A study from 2011 states that the estimated losses have longer tails if the security level is low (Lee, Kauffman, & Sougstad, 2011). It would therefore be interesting to

see if there is a similar relationship to be found in this thesis. It is important to mention that this thesis did not investigate the actual security level of the companies, but the respondents gave their subjective opinion about the company's "Culture Security Level" by rating themselves on several statements.

The cost of data breaches in this study ranges from 1000 NOK to 50 MNOK, with the median cost being 135 000 NOK. The big differences between the costliest data breaches and the median cost indicate that the distribution of data breach losses has a long right tail.

Since this dependent variable is not binary, a linear regression analysis is made to investigate the relationship between "Culture Security Level" and the cost of information security incidents. The dependent variable is the cost of an information security incident, and the independent variable is the "Culture Security Score". The regression results can be seen in Table 7. With a P-value of 0.933 for "Total Score", this study finds no relationship between the companies' "Culture Security Score" and the cost of information security incidents. The relationship between the cost of information security incidents and each individual statement is also analyzed, but none of the statements gives valuable information.

R-Squared	0.001
P-Value of Intercept	0.522
P-Value of "Culture Security Score"	0.933

Table 7: Regression Results

As previously mentioned, there are quite a few weaknesses with how the "Culture Security Score" is found. The results therefore cannot conclude that there is no relationship between the actual security level and cost of data breaches in the Norwegian SMB sector.

5.4 Increased Focus on Cyber Security After an Incident

There are results that indicate that companies that have experienced an information security incident have increased their focus on information security afterward. The "Culture Security Score" for different categories can be seen in Table 8.

	No Incident	Incident Cost < 100 000	Incident Cost 100 000 - 1 000 000	Incident Cost > 1 000 000
Average Score	32	32.7	35.5	35.6
Average Percent of Max Score	71%	73%	78%	79%

Table 8: Increase in Culture Score with Increasing Cost of Data Breach

The results seen in Table 8 indicate that the focus on information security rises after an incident, however, the differences are small. Another difference can be seen by looking at which companies have cyber insurance. 18 percent of companies in the survey had cyber insurance. Amongst the companies which had been subject to a data breach, 26 percent of the companies had cyber insurance. It is therefore likely that companies that have experienced data breaches have bought cyber insurance afterward in order to reduce the consequences of a potential future attack. As written in the literature review, insurance companies have strict requirements for companies that want to apply for cyber insurance. It is therefore likely that the companies that have applied for insurance after a data breach have been forced to raise their security level due to the cyber insurance requirements.

5.5 Criticality of Data Breaches

To investigate how critical the data breaches are, Equation 7 is tested for each of the companies that have suffered from a data breach. This equation is defined by the authors of this thesis.

$$\frac{Cost\ of\ Data\ breach}{Yearly\ Revenue} = Data\ Breach\ Criticality$$

Equation 7: Data Breach Criticality

The differences in the criticality of the data breaches are quite big. The average data breach criticality is 23.3 percent which is severe. The difference between the average and the median data breach criticality is very big, this is because some of the data breaches are extremely costly. The most critical data breach actually cost more than 400 percent of the company´s yearly turnover.

	Data Breach Criticality	Top 4 Costly Incidents
Average	23,3%	409 %
Median	0,363%	321 %
Max	409 %	60 %
Min	0,001%	23 %

Table 9: Data Breach Criticality Results

The ability to handle a big cost of a data breach varies between industries and individual companies. This depends on many factors such as the profit margin, solidity, liquidity and the financial structure of the company. Due to confidentiality reasons, the respondents in the survey were not asked about details in their accountings. To say something about how well Norwegian companies on average can handle the economic consequences of data breaches, the average profit margin of Norwegian companies was used, which in 2021 was approximately 7.5 percent (Holst, 2022).

It is very interesting to see how much data breaches cost compared to the profit of the companies because that gives information about whether they are capable of handling the expenses or not. By taking the data breach criticality in Table 10 and dividing it by the average profit margin (7.5 percent), it is possible to get information about how much the data breaches cost compared to the yearly average profit.

	Data Breach Criticality / Average Profit Margin (7.5)
Average	311 %
Median	4,8 %
Max	5451 %
Min	0,007%

Table 10: Data Breach Criticality / Average Profit Margin

For a company with a profit margin of 7.5 percent, the cost of an average data breach will be over 300 percent of their yearly profit. For many companies such a loss could lead to the company going bankrupt. The median cost of a data breach is smaller, the cost of the median data breach will account for 5 percent of the yearly profit for a company with a 7.5 percent profit margin. Such a loss is still significant, but it is likely that most companies will manage to handle it quite well.

The big difference between the average and median cost of data breaches shows that there are a few very big data breaches. In this study the most critical data breach cost the organization 409 percent of the yearly revenue, which for a company with a 7.5 percent profit margin would be over 5450 percent of the profit margin. Most companies would require external financial support from owners or banks to avoid bankruptcy if being subject to such a loss.

The most extreme losses are very critical, and companies should be prepared for them. One way to do that is to raise the security level, which reduces the extreme losses (Lee, Kauffman, & Sougstad, 2011). Companies could also consider cyber insurance, to transfer the risk to a third party. As previously mentioned, the insurance companies have strict requirements.

CHAPTER 6

Discussion

The main purpose of this thesis was to provide more information and data on the topic of information security in Norwegian SMBs. This chapter will discuss and interpret the findings presented in chapter 4 and chapter 5. Additionally, it will explore the limitations and weaknesses of this study, as well as implications of the findings and recommendations for future research.

6.1 Examining the Descriptive Statistics

There were a number of interesting findings presented in the summary statistics of the survey in relation to the research questions worthy of mentioning. Most of the findings support the information found through the literature review and results of other studies conducted on the same topic.

First and foremost, the findings indicate that only 17.5 percent of the respondents use a framework in their work with information security management. Other reports indicate this number to be significantly higher (51 percent) (Næringslivets Sikkerhetsråd, 2022). As previously mentioned, there is a possibility that the respondents misunderstand or misinterpret the questions. According to (Valdevit, Mayer, & Barafort, 2009) the larger companies tend to use information security management frameworks, while smaller companies often do not due to lack of resources. Since the average number of employees in the organizations was 24 employees this may explain these findings.

As (Ponsard & Grandclaudon, 2020) suggests employees in SMBs often tend to have multiple roles, and not a person specifically dedicated to information security. This seems to correlate with the findings in the study, as 45.6 percent

report that the organization has an employee with information security as one of their responsibilities. While only 14.9 percent report an employee with information security as their primary responsibility.

This data from this study indicates it is not that common for Norwegian SMBs to have cyber insurance, and most of the respondents report that they do not have cyber insurance (77.6 percent). This supports the claim made in a Swedish study that cyber insurance is mostly issued to bigger companies (Franke, 2017), and that organizations do not understand why they need cyber insurance (Bahşi, Franke, & Friberg, 2020).

The organizational commitment to information security according to these findings seems to be quite high, where the respondents mostly "strongly agree" with the statements about the organization's commitment on a 5-point Likert scale. This correlates with the findings of (Öğütçü, Testik, & Chouseinoglou, 2016) which underline the importance of developing a culture that promotes information security. (Uchendu, Nurse, Bada, & Furnell, 2021) states that the most important factor when it comes to information security culture is the leadership, and specifically the support from the leadership. The data from this study can also indicate that the leadership in the Norwegian SMBs have started to understand the importance of the management role in developing a sufficient organizational commitment to information security.

The majority of the respondents reports some form of employee training in information security, which according to (Bada & Nurse, 2019) is important to increase knowledge and awareness. On the other hand, 21.4 percent reported none of the training methods listed as answer options in the questionnaire. The reason for these findings may be because of the limitations of the answer options, but supports the fact that employees forget information after training courses

(Ghafir, et al., 2018), and the need for organization to develop specific training programs for the needs and context of the organization (Bada & Nurse, 2019; He & Zhang, 2019).

(van Haastrecht, Ozkan, Brinkhuis, & Spruit, 2021) reports that the sharing of information security incidents within an organization is crucial for reducing the risk of future incidents. The data in this study shows that 54.1 percent of the respondents report that after an incident all employees are informed about ongoing threats, incidents, or deviations.

Furthermore, when it comes to risk assessment of the different types of information security threats most of the respondents evaluate the risk of the different types of threats as either low or moderate. This correlates with the findings of (Li, et al., 2019) that states that employees are not aware of the potential consequence that information security threats can pose. Additionally, (Benz & Chatterjee, 2020) report that the management of the SMBs assess the threats as low, and do not think they will be targeted. Since the majority of the respondents were the CEO (71.6 percent) of the company these findings support those claims. The respondents guess/ estimates of the average cost of a data breach in the SMB sector was 2.65 MNOK, while the actual average cost of the data breaches from the responding companies was 4.31 MNOK. This is also an indication that that the management of the responding companies underestimate the consequences of data breaches.

Lastly, there are a significant number of organizations that have been subject to one or more information security incidents. According to (Yildirim, Akalp, Aytac, & Bayram, 2011) the weakest link in regard to information security is the employees. The data in this study supports that claim and the type of information security incident most frequently reported in this study was an unintentional

incident carried out by an employee (14.0 percent). Another finding was that 8.4 percent were affected by a phishing attack, and (Butler, 2007) argues that the main reason phishing is an effective method is because it targets the weakest link which is the employees.

6.2 Discussion of the Analysis and Results

The most important regression results are presented and discussed in chapter 5. However, the relationship between most of the questions in the survey and the probability and consequences for data breaches were tested. For instance, it was tested to see if how the IT Operations were organized had a relationship with the probability and consequence of data breaches. Similarly, the other questions from the survey were tested. Amongst all the different questions asked in the survey no clear relationship was found. This indicates that apart from the size of companies (Number of Employees and Turnover), and which industry the company belongs to, it seems to be quite random which companies are subject to data breaches, and what the consequences of the data breaches are.

It is likely that this randomness is due to weaknesses in the way the survey is conducted. As mentioned earlier it is likely that the responding companies that have suffered from a data breach have raised their focus on information security after the incident. This is a potential reason for why there are no relationships to be found between the different questions asked and the probability and consequences of data breaches.

6.3 Limitations

Although this research project has provided valuable information, it is practically impossible to completely remove all limitations. This study is not an exception and has several limitations. In order to understand the findings in this research it is important to acknowledge and be aware of these limitations. There are many

different aspects that may potentially impact the results when researching a sensitive subject like information security.

The potential for self-report bias was of the major limitations in this research. Since the participants were asked to self-report on information security in relation to the organizational, cultural, and cost estimation in the data collected process, the results may have been subject to social desirability bias, or other forms of response bias. The participants may overreport the positive aspects or underreport the negative (their weaknesses). Another factor that may have affected the data is the participants who misunderstood or misinterpreted some of the questions on the survey, or provided false answers, which may have led to inaccurate findings.

Another important limitation to be considered is related to the potential for representative bias and self-selection bias in the survey. Although participants were selected from a diverse group representing different industries, geological locations and numbers of employees, it may still not be fully representative. Since participants self-select to take the survey, the individuals who are more interested in the topic, or have experienced an information security incident may be more willing to participate in the survey. Another factor that may affect the representative bias is the fact that the study was only conducted on still operational organizations in the SMB sector. As previously mentioned in the literature review many companies that experience information security incidents go out of business. It is therefore natural to speculate that the number of incidents and the cost of these are higher than found in this study.

Although the survey was designed to map the current information security practices and cover a wide range of topics, the survey questions may have had limited scope, and not captured all relevant factors. There were various considerations to make when designing the survey, such as keeping the survey

length manageable, which limited the number of questions and the depth and detail of the participant responses.

6.4 Further Research

Since the survey was sent out to functioning companies, it does not gather any information about companies that have gone bankrupt due to data breaches. It would have been interesting to find official lists of companies that recently have gone bankrupt and invite the former CEO to attend a survey. In this way it would be possible to get information about how many bankruptcies occur due to data breaches.

As previously mentioned, there are several potential weaknesses regarding the "Culture Security Score". Seen in retrospect it would have been smart to ask companies that have been subject to a data breach to rate their "Culture Security Score" before and after the data breach. By implementing these changes in further research this can potentially lead to statistically significant results.

To get sufficient amount of data the participants were asked if they had experienced any data breaches over a 4-year period. The four last years include the corona pandemic, which in many ways was different from normal. According to a report from NorSiS there were more data breaches during the Corona pandemic, compared to the years before the pandemic (NorSIS, 2021). It is likely that the past four years will be different from the next four years. For further research it can be interesting to see if there are any major differences in the results if the time period of the Covid-19 pandemic is not included in the survey.

CHAPTER 7

Conclusion

The main purpose of this thesis was to provide new information and contribute to the research on the topic of information security in small and medium-sized businesses in Norway. Aiming to gain insight into the culture and leadership practices in relation to information security, and the cost related to incidents. The findings in this research were interesting when compared and considered to the existing literature reviewed.

According to the findings in this thesis, a significant share of Norwegian small and medium-sized businesses has experienced one or more unwanted incidents related to information security the last four years. The costliest data breaches in this study are extremely severe, that is in line with previous research on the topic. The median cost of the incidents is quite moderate and should be manageable for most businesses. Businesses should be prepared for the worst-case scenario; this can be done by raising the security level. The findings in this study do however not find any statistically significant relationship between "Culture Security Level" and the probability or cost of incidents. This thesis mentions several weaknesses with the methods of finding the "Culture Security Level". Due to these weaknesses, it cannot be drawn a conclusion stating that there is no relationship.

Another way for companies to protect themselves against data breaches is by buying insurance. One out of six companies in this study have bought cyber insurance. An interesting finding is that a bigger share of the businesses that have been subject to a data breach have insurance. This indicates that companies that have experienced a data breach act afterwards, in order to minimize the consequences if they were to be attacked again. The "Culture Security Score" of businesses that have experienced a data breach is higher than the "Culture

Security Score" for the organizations that have not suffered from a data breach. This indicates that businesses raise their "Culture Security Level" after they experience the importance of being protected against data breaches.

The result from the survey indicates that there are big differences between industries. There are some industries which have few respondents, which makes coincidences play a significant role. The two industries with the most respondents are the technology sector and the construction and building operations sector. Even though the respondents from the technology sector on average had less employees and lower annual revenue the sector still had 50 percent more data breaches compared to the construction and building operations sector.

The thesis finds a positive relationship between the probability for data breaches and number of employees and yearly turnover for Norwegian companies in the SMB sector. This means that businesses with a high yearly turnover have a higher probability of data breaches.

The first research question is: "To which degree are Norwegian small and medium-sized businesses affected by information security incidents?". By looking at the numbers from this study there have been 83 data breaches over a 4-year period, across 236 responding companies. The consequences of the data breaches are big, with several incidents with a cost of more than 10 MNOK. The result from this thesis therefore indicates that the Norwegian SMB sector is highly affected by information security incidents.

The second research question is: "Are the small and medium-sized businesses sufficiently secure against information security incidents?". If a company is sufficiently secure against information security incidents, depends on the risk they are willing to take. A company with a low-security level spends less on cyber

security but has a higher probability of a data breach, and the expected consequences are higher compared to a company with a higher security level.

The results from the survey show that the average "Culture Security Score" is around 75 percent. It is not necessarily a goal to strive for a higher security level, it depends on the company's willingness to be exposed to risk. It is important that each individual company has a strategy that takes this into consideration.

The result from the survey indicates that the responding companies that have suffered from a data breach have raised their "Culture Security Level", and that they have bought cyber insurance after the incident. This indicates that companies find out that they are not sufficiently secured against data breaches, first after a data breach has happened. The respondents' guess of the average cost of a data breach was approximately half of the actual costs of the data breaches in this thesis. Since the actual consequences are more severe than their beliefs, it can be argued that they are not sufficiently secured against data breaches.

With the above-mentioned arguments, this thesis concludes that on average the Norwegian SMB sector is not sufficiently secured against information security incidents. However, there are individual differences between companies, and it ultimately depends on the company´s desired risk profile.

References

Aven, T., & Thekdi, S. (2021). *Risk Science: An Introduction.* Taylor & Francis Group. doi:10.4324/9781003156864

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393-410. doi:10.1108/ICS-07-2018-0080

Bahşi, H., Franke, U., & Friberg, E. L. (2020). The cyber-insurance market in Norway. *Information and Computer Security, 28*(1), 54-67. doi:10.1108/ICS-01-2019-0012

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531-540. doi:10.1016/j.bushor.2020.03.010

Bobbitt, Z. (2021, August 9). *Statology*. Retrieved May 3, 2023, from How to Interpret a ROC Curve (With Examples): https://www.statology.org/interpret-roc-curve/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library, 25*(5), 517-533. doi:10.1108/02640470710829514

Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: towards a unifying framework. *Workshop on the Economics in Information Security (WEIS)*.

CFI Education Inc. (2023, May 7). *Value at Risk (VaR): A measurement technique that estimates the risk of an investment*. Retrieved from Corporate Finance Institute: https://corporatefinanceinstitute.com/resources/risk-management/value-at-risk-var/

Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020). Evolution, Mitigation, and Prevention of Ransomware. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, 1-6. doi:10.1109/ICCIS49240.2020.9257708

Cisco Inc. (2023). *What is malware?* Retrieved April 5, 2023, from Cisco: https://www.cisco.com/site/us/en/products/security/what-is-malware.html

Creswell, J. W., & Creswell, J. D. (2018). *Research design : qualitative, quantitative & mixed methods approaches* (5th ed.). SAGE Publications, Inc.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi:10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *The Computer Law and Security Review, 31*(2), 243-256. doi:10.1016/j.clsr.2015.01.005

Datascience. (2022, 12 21). *Linear regression vs logistic regression – Detailed analysis with examples.* Retrieved April 25, 2023, from Datasciencedojo: https://datasciencedojo.com/blog/linear-regression-vs-logistic-regression/

Dulock, H. L. (1993). Research Design: Descriptive Research. *Journal of Pediatric Oncology Nursing, 10*(4), 154-157. doi:10.1177/104345429301000406

European Commission. (2022). *Digital Economy and Society Index 2022 Norway.* Brussels: European Union.

Finansdepartementet. (2022, 03 01). *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT).* Retrieved from Lovdata: https://lovdata.no/dokument/SF/forskrift/2003-05-21-630

Fink, A. (2019). *Conducting Research Literature Reviews: From the Internet to Paper* (5th ed.). Los Angeles: Sage publications Inc.

Franke, U. (2017). The cyber insurance market in Sweden. *Computer & Security, 68*, 130-144. doi:10.1016/j.cose.2017.04.010

Froehlich, A. (2019, 07 01). *What are pros and cons of IT security?* Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/answer/What-are-the-pros-and-cons-of-outsourcing-IT-security

Georgescu, T. M. (2021). A Study on How the Pandemic Changed the Cybersecurity Landscape. *Informatica Economica, 25*(1), 42-60. doi:10.24818/issn14531305/25.1.2021.04

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing, 74*(10), 4886-5002. doi:10.1007/s11227-018-2337-2

Grimsby, G., Grünfeld, L. A., & Jakobsen, E. W. (2009). *99% SMB - Grunnfjell og vekstmotorer i norsk næringsliv.* Oslo: MENON Business Economics. Retrieved from https://www.menon.no/wp-content/uploads/26menonpubl13200999smb.pdf

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*(4), 249-257. doi:10.1080/10919392.2019.1611528

Herath, K. M. (2011). *Building a privacy program : a practitioner's guide.* Portsmouth: International Association of Privacy Professionals (IAPP).

Herold, R. (2005). *Managing an Information Security and Privacy awareness and Training Program* (1 ed.). New York: Auerbach Publications. doi:10.1201/9781003040231

Holst, L. A. (2022, November 23). *Norsk næringsliv har aldri tjent mer penger!* Retrieved May 13, 2023, from Dun&Breadstreet: https://www.dnb.com/no/kunnskap/artikler/norsk-naeringsliv-har-aldri-tjent-mer-penger.html

IBM Security. (2022). *Cost of a Data Breach: Report 2022.* New York: IBM Corporation. Retrieved from https://www.ibm.com/downloads/cas/3R8N1DZJ

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

International Organization for Standardization. (2022). *ISO/IEC 27001 Information security management systems*. Retrieved May 9, 2023, from ISO: https://www.iso.org/standard/27001

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, (pp. 1-4). Oxford. doi:10.1109/CyberSecPODS.2019.8885240.

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2021). *An Introduction to Statistical Learning with Applications in R* (2nd ed.). New york: Springer.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems, 51*(4), 904-920. doi:10.1016/j.dss.2011.02.009

Leedy, P. D., & Ormrod, J. E. (2012). *Practical Research: Planning and Design* (10th ed.). Boston: Pearson Educational.

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy, 6*(2), 118-136. doi:10.1080/23738871.2021.1880609

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems, 56*(2), 106-115. doi:10.1080/08874417.2016.1117369

Mutalib, M. M., Zainol, Z., & Halip, M. H. (2021). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* (pp. 1-6). Kedah: IEEE. doi:10.1109/ICRAIE52900.2021.9703991

Maalem, L., Rachid, A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Springer Singapore, 3*(1), 1-18. doi:10.1186/s42400-020-00050-w

NIST. (2023). *Computer Security Resource Center*. Retrieved March 22, 2023, from National Institute of Standards and Technology: https://csrc.nist.gov/glossary/term/infosec?fbclid=IwAR1cmsqXCadf6VUu0zGaPJgmVkSrNbX_pKBMlkhj3TAGLkoHh1PgkeXKT1U

Normen. (2022, November 21). *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.* Retrieved from Direktoreate for e-helse: https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

NorSIS. (2021). *Trusler og trender 2021.* Gjøvik: NorSIS. Retrieved from https://norsis.no/content/uploads/2022/05/NorSIS_Trusler_Trender_2021_Digital.pdf

Nærings- og handelsdepartementet. (2012). *Små bedrifter – store verdier: Regjeringens strategi for små og mellomstore bedrifter.* Regjeringen. Retrieved from https://www.regjeringen.no/globalassets/upload/nhd/vedlegg/rapporter_2012/102377_nhd_smb_web.pdf

Næringslivets Sikkerhetsråd. (2022). *Mørketallsundersøkelsen 2022.* Oslo: Næringslivets Sikkerhetsråd.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Social Science Research Network, 10*(26).

Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer Journal, 49*(8), 92-97. doi:10.1109/MC.2016.223.

Peričić, T. P., & Tanveer, S. (2019, July 23). *Why systematic reviews matter: A brief history, overview and practical guide for authors*. Retrieved from Elsevier: https://www.elsevier.com/connect/authors-update/why-systematic-reviews-matter

Petruzzi, J., & Loyear, R. (2016). Improving organisational resilience through enterprise security risk management. *Journal of Business Continuity & Emergency Planning, 10*(1), 44-56.

Ponemon Institute. (2013). *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age.* Ponemon Institute.

Ponsard, C., & Grandclaudon, J. (2020). Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs. In P. Mori, S. Furnell, & O. Camp, *Information Systems Security and Privacy* (Vol. 1221). Springer, Cham. doi:10.1007/978-3-030-49443-8_16

Rajaeian, M. M., Cater-Steel, A., & Lane, M. (2017). A systematic literature review and critical assessment of model-driven decision support for IT outsourcing. *Decision Support Systems, 102*, 42-56. doi:10.1016/j.dss.2017.07.002

Schmidt, N. A., & Brown, J. (2019). *Evidence-based practice for nurses: Appraisal and application of research* (4th ed.). Burlington: Jones & Bartlett Learning.

Security Risk Governance Group. (2023, 05 22). *Enterprise Security Risk Management*. Retrieved from ESRM: https://esrm.info/enterprise-security-risk-management/

Sikt. (2023). *Carrying out a project without processing personal data*. Retrieved May 8, 2023, from Sikt: https://sikt.no/en/gjennomfore-et-prosjekt-uten-behandle-personopplysninger

Silva, J. A., López, L. I., Caraguay, Á. L., & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks - Detection and Prevention Parameters. *Remote Sensing, 11*(10). doi:10.3390/rs11101168

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. *International Journal of Communication Networks and Information Security (IJCNIS) , 12*(3), 417-432.

Thompson, S. K. (2012). *Sampling* (3ed ed.). Hoboken: John Wiley & Sons, Inc.

Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). *Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research.* Oslo: SINTEF. Retrieved from http://hdl.handle.net/11250/2379189

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future. *Computers & Security, 109*. doi:10.1016/j.cose.2021.102387

Valdevit, T., Mayer, N., & Barafort, B. (2009). Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings. In R. V. O'Connor, N. Baddoo, J. C. Gallego, R. R. Muslera, K. Smolander, & R. Messnarz, *Software Process Improvement* (Vol. 42, pp. 201-212). Berlin: Springer. doi:10.1007/978-3-642-04133-4_17

van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. *Applied Sciences, 11*(15). doi:10.3390/app11156909

Verizon. (2023). *2022 Data Breach Investigation Report (DBIR).* New York: Verizon.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 31*(4), 360-365. doi:https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

Appendix Section

Please appendix. see attached files for the appendix's is listed here with name and description:

Appendix A: Survey Questionnaire English Edition

Information Security – Questionnaire

This survey aims to assess information security practices within small and medium-sized businesses (SMBs) and is conducted by two master's students in Industrial Economics at the University of Stavanger. The survey takes an average of 7 minutes to complete, and we appreciate your participation to the best of your ability. All data will be collected anonymously and treated confidentially.

Section 1:

1. What is the role in organization do you have as the respondent of this survey?

- CEO
- Financial Manager
- IT/ICT Role
- Other (Please Specify)

2. Is the organization public or private?

- Private
- Public

3. In which county does the organization have its headquarters?

- Oslo
- Rogaland
- Viken
- Vestland
- Innlandet
- Agder
- Vestfold og Telemark
- Troms og Finnmark
- Trøndelag
- Nordland
- Møre og Romsdal

4. In which industry does the organization operate?

- Industry
- Banking, Finance and Insurance
- Technology
- Construction and Building Operations
- Retail
- Transportation and Storage
- Accommodation and Food Services
- Service Industries
- Education
- Health and Social Services
- Cultural Activities

Other (Please Specify)

5. Is the IT-operations in the organization outsourced?

- Completely Outsourced
- Partially Outsourced
- Organized Internally
- Don't Know

6. Approximately how many employees were there in the organization on January 1, 2023?
(Number of people employed in the organization, regardless of position or employment percentage)

7. Approximately how much did the organization generate in revenue in 2022
If the financial statements for 2022 are not completed, you can provide the revenue for 2021.
The answer should be in NOK. You can round to the nearest 100.000

8. How much do you agree with the following statements?

	Strongly Disagree	Disagree	Unsure	Agree	Strongly Agree
The management demonstrates leadership	•	•	•	•	•

and commitment to information security					
The management has conducted a systematic risk assessment related to information security.	•	•	•	•	•
The management views risks related to information security on par with other risk factors.	•	•	•	•	•
The organization has objectives related to improving information security.	•	•	•	•	•
The organization conducts awareness and training campaigns.	•	•	•	•	•
The organization has a document classification system.	•	•	•	•	•
It is clear to all employees who is responsible for information security.	•	•	•	•	•
Information security is informally discussed among employees.	•	•	•	•	•
Incidents and deviations related to information security are communicated openly internally for learning purposes.	•	•	•	•	•

2. Information Security Management

9. Does the organization have an employee with primary responsibility for information security?

- Yes
- Yes and Other Responsibilities
- No
- Don't Know

10. Has the organization purchased cyber insurance?

- Yes
- No
- Don't Know

11. Does the organization use established frameworks such as ISO/IEC 27001 in its work on information security?

ISO/IEC 27001: Information security management systems - one of the world's most recognized standards for data security. The standard takes a holistic approach to IT security and describes best practices for protecting data.

- Yes
- No
- Don't Know

3. Information Security Culture

We have some questions here regarding the culture in the organization.

12. How often does the organization review information security policies and procedures?

- Systematically at regular intervals, e.g., Annually
- Policies reviewed Ad Hoc
- Outdated Policies
- No Written Policies
- Don't know

13. What introduction/training in information security do employees receive? (You can choose multiple options)

- ☐ Online Courses
- ☐ Lectures

- ☐ One-on-One Training
- ☐ Written Training Documents
- ☐ Training Related to Password Use and Management
- ☐ Training on Data Backup and Recovery
- ☐ Security Management of Mobile Phones and Other Devices
- ☐ Training Related to Secure Use of Home Office
- ☐ Requirements for Handling Sensitive and Confidential Data
- ☐ None of the Above

14. Has information been communicated and made available to employees on how to report deviations and unwanted incidents related to information security?

- Yes, Communicated in Written
- Yes, Communicated Verbally
- No
- Don't Know

15. How can employees notify and report deviations and unwanted incidents related to information security?

- Report to the Immediate Supervisor
- Report to IT-Department
- Digital Reporting System
- No Formalized Reporting
- Don't Know

16. Are employees informed about ongoing activity/threats, deviations, and incidents related to information security?

- Yes, All Employees are Informed
- No, Only a Limited group of Employees
- No, Precedure to Inform Employees
- Don't Know

4. Mapping Risks and Information Security Incidents

17. Assess the company's risk related to the various incidents:

	None	**Low**	**Moderate**	**High**	**Critical**
Data Breach	•	•	•	•	•
Malware and Viruses	•	•	•	•	•
Phishing and Social Engineering	•	•	•	•	•

Ransomware	•	•	•	•	•
Unauthorized Use and Access to Systems	•	•	•	•	•

18. How much do you think a data breach costs on average for a small and medium-sized business (SMB)? Answer in NOK.

19. Has the organization been affected by any of these incidents since January 1, 2019? (You can choose multiple options)

- ☐ Affected by Phishing/Scam Emails
- ☐ Affected by Ransomware
- ☐ Unintentional Incidents Carried Out by Employees
- ☐ Intentional Incidents Carried Out by Employees
- ☐ Theft of ICT Equipment
- ☐ Loss/Leakage of Personal Data
- ☐ Affected by Malicious Software
- ☐ Don't Know
- ☐ None of the Above

☐ Other (Please Specify)

5. Cost Associated with Data Breaches

If it is difficult to answer with actual amounts, you can provide an approximate amount. If you don't have actual/estimated amounts, you can choose not to answer.

20. Cost Associated with Consulting Services

When answering this question, think about the most severe security incident during the period. Approximately how much did the organization spend on consulting services related to the attack? Answer in NOK.

21. Cost of Lost Business

When answering this question, think about the most severe security incident during the period. During a hacker attack, a company is often prevented from continuing its business operations for a period. The company may be unable to provide services during that time, and they may, for example, lose the opportunity to bid on a major contract. What is the estimated cost resulting from lost business? Answer in NOK.

22. Cost of Data Loss

When answering this question, think about the most severe security incident during the period. During an unwanted security incident, data is often lost, such as technical drawings, accounting data, trade secrets, or physical IT equipment. What is the estimated cost of data loss? Answer in NOK.

23. Cost of Reputation Loss

When answering this question, think about the most severe security incident during the period. If company A has been subjected to hacking, it can lead to company B being skeptical about doing business with company A because they do not trust that company A can protect critical information. What is the estimated cost resulting from reputation loss? Answer in NOK.

24. Cost of Lost Workforce

When answering this question, think about the most severe security incident during the period. An example could be a consulting firm that usually charges 1000 NOK per hour, but due to a data breach, they are prevented from performing consulting work. If a company has 10 consultants who are unable to work for 5 days, they will lose 10 * 1000 NOK/hour * 8 hours * 5 days = 400,000 NOK. What is the estimated cost resulting from lost workforce? Answer in NOK.

Appendix B: Survey Questionnaire Norwegian Edition

Informasjonssikkerhet – Spørreundersøkelse

Denne undersøkelsen ønsker å kartlegge informasjonssikkerhet tilknyttet små og mellomstore bedrifter (SMB), og gjennomføres av to masterstudenter innen Industriell Økonomi ved Universitetet i Stavanger. Undersøkelsen tar i gjennomsnitt 7 minutter og vi setter pris på om du svarer etter beste evne. All data hentes inn anonymt og behandles konfidensielt.

1. Hvilken rolle i virksomheten har du som svarer på spørreundersøkelsen?

- Daglig leder
- Økonomiansvarlig
- IT/IKT-rolle
- Annet (vennligst spesifiser)

2. Er virksomheten privat eller offentlig?

- Privat
- Offentlig

3. I hvilket fylke har virksomheten sitt hovedkontor?

- Oslo
- Rogaland
- Viken
- Vestland
- Innlandet
- Agder
- Vestfold og Telemark
- Troms og Finnmark
- Trøndelag
- Nordland
- Møre og Romsdal

4. I hvilken bransje opererer virksomheten?

- Industri
- Bank, Finans og Forsikring
- Teknologi
- Bygg- og Anleggsvirksomhet
- Varehandel
- Transport og Lagring
- Overnattings- og Serveringsvirksomhet
- Tjenesteytende Næring
- Undervisning
- Helse og Sosial
- Kulturell Virksomhet

Annet (vennligst spesifiser)

5. Er IT-driften i virksomheten outsourcet?

- Helt outsorucet
- Delvis outsourcet
- Organisert internt
- Vet ikke

6. Omtrent hvor mange ansatte var det i virksomheten 1. Januar 2023?
(Antall personer som var ansatt i virksomheten, uavhengig av stillingstype eller stillingsprosent)

7. Omtrent hvor mye omsatte virksomheten for i 2022?
Hvis regnskapet for 2022 ikke er fullført kan en oppgi omsetningen for 2021.
Svaret angis i NOK. Rund gjerne av til nærmeste 100 000.

8. Hvor enig er du i følgende påstander?

	Helt uenig	Delvis enig	Nøytral	Delvis enig	Helt enig
Ledelsen demonstrerer lederskap og en forpliktelse for arbeidet for informasjonssikkerhet	•	•	•	•	•
Ledelsen har gjennomført en systematisk risikovurdering knyttet til informasjonssikkerhet	•	•	•	•	•
Ledelsen i virksomheten ser på risiko knyttet til	•	•	•	•	•

informasjonssikkerhet på lik linje med andre risikofaktorer					
Virksomheten har målsetninger knyttet til forbedring av informasjonssikkerhet	•	•	•	•	•
Virksomheten utfører bevissthet- og opplæringskampanjer	•	•	•	•	•
Virksomheten har et system for klassifisering av dokumenter	•	•	•	•	•
Det er tydelig for alle ansatte hvem som har ansvaret for informasjonssikkerheten	•	•	•	•	•
Informasjonssikkerhet diskuteres uformelt blant ansatte	•	•	•	•	•
Hendelser og avvik knyttet til informasjonssikkerhet kommuniseres åpent internt for læringsformål	•	•	•	•	•

2. Ledelse knyttet til informasjonssikkerhet

9. Har virksomheten en ansatt med hovedansvar for informasjonssikkerhet?

- Ja
- Ja, men har også andre ansvarsoppgaver
- Nei
- Vet ikke

10. Har virksomheten tegnet cyberforsikring?

- Ja
- Nei
- Vet ikke

11. Benytter virksomheten seg av kjente rammeverk som f.eks. ISO/IEC 27001 i arbeidet med
informasjonssikkerhet? ISO/IEC 27001: Ledelsessystemer for informasjonssikkerhet - en av verdens mest anerkjente standarder for datasikkerhet. Standarden har en helhetlig tilnærming til IT-sikkerhet og beskriver beste praksis for å beskytte data.

- Ja
- Nei
- Vet ikke

3. Kultur knyttet til informasjonssikkerhet

Vi stiller her noen spørsmål som går på kulturen i virksomheten

12. Hvor ofte gjennomgår virksomheten informasjonssikkerhetsretningslinjer og -prosedyrer?

- Dette gjøres systematisk med jevne mellomrom, f.eks. årlig
- Dette gjennomgås og oppdateres etter behov, men har ikke noe systematikk i det.
- Det har blitt gjennomgått en gang, men har ikke oppdatert det siden
- Virksomheten har ingen skriftlige retningslinjer og prosedyrer knyttet til informasjonssikkerhet
- Vet ikke

13. Hvilken innføring/opplæring innen informasjonssikkerhet får ansatte?
(Her kan du velge flere alternativer)

- ☐ Nettkurs
- ☐ Foredrag
- ☐ En-til-en opplæring
- ☐ Skriftlige opplæringsdokumenter
- ☐ Opplæring knyttet til passordbruk og -håndtering
- ☐ Opplæring om sikkerhetskopiering og gjenoppretting av data
- ☐ Sikkerhetshåndtering av mobiltelefoner og andre enheter

- ☐ Opplæring knyttet til sikker bruk av hjemmekontor
- ☐ Innføring i krav til håndtering av sensitiv og konfidensiell data
- ☐ Ingen av de ovennevnte

14. Er det kommunisert og tilgjengeliggjort informasjon til ansatte om hvordan de kan rapportere avvik og uønskede hendelser knyttet til informasjonssikkerhet?

- Ja, skriftlig kommunisert
- Ja, muntlig kommunisert
- Nei
- Vet ikke

15. Hvordan kan ansatte varsle om- og rapportere avvik og uønskede hendelser knyttet til informasjonssikkerhet?

- Ansatte varsler til nærmeste leder
- Ansatte varsler til IT-ansvarlig/IT-avdeling
- Ansatte rapporterer i et digitalt varslingssystem
- Virksomheten har ingen formalisert måte å rapportere
- Vet ikke

16. Får ansatte vite om pågående aktivitet/trusler, avvik og hendelser knyttet til informasjonssikkerhet?

- Ja, alle ansatte blir informert ved informasjonssikkerhetshendelser
- Nei, kun en begrenset gruppe ansatte som er direkte involvert i håndteringen av hendelsen blir informert
- Nei, virksomheten har ikke prosedyrer for å informere alle ansatte om informasjonssikkerhetshendelser
- Vet ikke

4. Kartlegging av risiko og informasjonssikkerhetsbrudd

17. Vurder virksomhetens risiko knyttet til de ulike hendelsene:

	Ingen	**Lav**	**Moderat**	**Høy**	**Alvorlig/Kritisk**
Datainnbrudd	•	•	•	•	•
Malware og Virus	•	•	•	•	•
Phishing og sosial manipulasjon	•	•	•	•	•

Ransomware	•	•	•	•	•
Uautorisert bruk og tilgang til systemer, enheter eller tjenester	•	•	•	•	•

18. Hvor mye tror du et dataangrep på små og mellomstore bedrifter (SMB) i gjennomsnitt koster for den rammede bedriften? Svar angis i NOK

19. Har virksomheten blitt utsatt for noen av disse hendelsene siden 01.01.2019? (Her kan du velge flere alternativer)

- ☐ Rammet av phishing-angrep/svindel-epost som faktisk har hatt konsekvenser for virksomheten
- ☐ Rammet av løsepengevirus
- ☐ Utilsiktet hendelse foretatt av ansatte, for eksempel uønsket sletting/endring/lekkasje
- ☐ Tilsiktet hendelse foretatt av ansatte, for eksempel sletting/endring/lekkasje
- ☐ Annet (vennligst spesifiser)
- ☐ Tyveri av IKT-utstyr, for eksempel datamaskiner, mobiltelefoner og harddisker
- ☐ Tap/lekkasje av persondata
- ☐ Rammet av skadelig programvare annet enn løsepengevirus
- ☐ Vet ikke
- ☐ Ingen av de ovennevnte

5. Kostnad knyttet til dataangrep
Til slutt ønsker vi å kartlegge den økonomiske konsekvensen av dataangrep.

Hvis det er vanskelig å svare med faktiske beløp, kan du estimere et omtrentlig beløp. Hvis du verken har faktiske/estimerte beløp kan du la være å svare

20. Kostnad knyttet til konsulenttjenester
Når du skal besvare dette spørsmålet, tenk på den mest alvorlige sikkerhetshendelsen i

perioden. Omtrent hvor stor utgift hadde virksomheten i konsulenttjenester i forbindelse med angrepet? Svaret angis i NOK

21. Kostnad av tapt forretning

Når du skal besvare dette spørsmålet, tenk på den mest alvorlige sikkerhetshendelsen i perioden. Under et hackerangrep vil en ofte blir hindret i å fortsette forretningsvirksomhet i en periode. Virksomheten kan bli forhindret i å levere tjenester i perioden, og virksomheten kan f.eks. miste muligheten til å by på en stor kontrakt. Hva er estimert kostnad som følge av tapt forretning? Svaret angis i NOK

22. Kostnad av tapt data

Når du skal besvare dette spørsmålet, tenk på den mest alvorlige sikkerhetshendelsen i perioden. Under en uønsket sikkerhetshendelse vil ofte data gå tapt, eksempler kan være tekniske tegninger, regnskapsdata, forretningshemmeligheter eller fysisk IT-utstyr. Hva er estimert kostnad av tapt data? Svaret angis i NOK

23. Kostnad som følge av tapt omdømme

Når du skal besvare dette spørsmålet, tenk på den mest alvorlige sikkerhetshendelsen i perioden. At en virksomhet A har blitt utsatt for hacking, kan føre til at virksomhet B blir skeptiske til å gjøre forretning med virksomhet A fordi de ikke stoler på at virksomhet A klarer beskytte
kritisk informasjon. Hva er estimert kostnad som følge av omdømmetap? Svaret angis i NOK

24. Kostnad av tapt arbeidskraft

Når du skal besvare dette spørsmålet, tenk på den mest alvorlige sikkerhetshendelsen i perioden. Et eksempel kan være et konsulentfirma som vanligvis fakturerer 1000kr/time, men på grunn av dataangrep blir de hindret fra utføre konsulentarbeid. Et firma med 10 konsulenter som hindres å jobbe i 5 dager vil da tape 10stk * 1000kr/t * 8t * 5 dager = 400 000kr
Hva er estimert kostnad som følge av tapt arbeidskraft? Svaret angis i NOK