

# **Outsourcing and its Influence on Cybersecurity in SMEs: An Exploratory Study in Norwegian Context**

JARLE NORDBY JOHNSEN & CHRISTIAN KITTILSEN

SUPERVISOR

Devinder Thapa

**University of Agder, 2022**

Faculty of Social Sciences

Department of Information Systems



# ABSTRACT

Outsourcing IT services to a third party is a trend that is becoming more common, and the majority of those who do not, are considering it. By outsourcing these services, companies do not have to take care of IT themselves and can expect that the provider ensures safety in the solutions. But exactly how cybersecurity is influenced by this in Norwegian small and medium-sized companies is the purpose of this qualitative study. A purposive sampling method was used to recruit participants who had first-hand experience with outsourcing and the potential to provide us with the insight we sought. Semi-structured interviews were conducted with personnel responsible for managing IT in companies with less than 250 employees. Data from the interviews were transcribed and analyzed by using the qualitative data analysis software NVivo 12 Pro. The study found several different ways in which outsourcing influences cybersecurity. The most prominent security benefits that were identified were quality improvement and increased capacity. Loss of data control, communication issues, dependency and supply chain attacks were the main security challenges found in the study. To address these difficulties, mitigation measures such as control competency, contract with SLA, and a focus on business continuity were discovered.

The findings of this study can be used by organizations that consider an outsourcing strategy to be better prepared and make correct choices at an early stage. In addition, it gives companies that already outsource a valuable insight into which measures others have applied to mitigate known challenges.

**Keywords: Outsourcing, Small and medium-sized enterprises, Managed service provider, Challenges, Benefits, Mitigation techniques**



# PREFACE

We are two students taking a master's degree in cybersecurity - security management and this paper is our thesis. Cybersecurity is a field that continues to evolve at a fast pace which makes it very interesting. The topic for this thesis will be outsourcing of IT services and how it influences the cybersecurity in Norwegian small and medium-sized businesses. We chose to look at this topic due to how relevant it is today. An increasing number of organizations are outsourcing their IT needs, but we suspected that this is not done without complications. As students in cybersecurity, we were curious about how this influences the security in the organizations and how the customers and providers deal with this issue.

While attending "Sikkerhetsdagen 2021" in Grimstad, we heard a lot of debates regarding cyber defense, and one statement caught our attention:

*It looks like we are headed for a more joint system for cyber defense in organizations rather than having IT security departments in each one. This is to be able to increase, but also more easily share the knowledge and experience (Kampenes, 2021, Translated by author).*

Such a statement from Inge Kampenes, who is the head of the Norwegian armed forces cyber defense, intrigued our interest and we wanted to learn more about how a joint system would influence organizations. Gaining more understanding on how companies are influenced would be beneficial for companies that consider outsourcing and we seek to provide this.



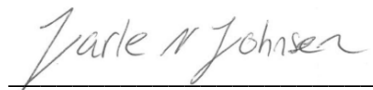
# ACKNOWLEDGEMENTS

We would like to thank the people who have dedicated their time and effort to assist us in completing this thesis.

Firstly, we thank our supervisor Devinder Thapa for his guidance on conducting qualitative research, academic writing, and general support throughout the project.

We would also like to thank our lecturer Marko Ilmari Niemimaa for his help in writing the literature review.

Lastly, we would like to thank the individuals and organizations that participated in our interviews. Without all of you our thesis would not have been possible.



Jarle Nordby Johnsen



Christian Kittilsen





# Table of Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>1</b>
1.1	Research questions .....	2
1.2	Research approach.....	3
1.3	Thesis structure .....	3
<b>2</b>	<b>THEORETICAL BACKGROUND</b> .....	<b>5</b>
2.1	Background .....	5
2.2	Systematic literature review .....	6
2.2.1	Method .....	6
2.2.2	Results.....	12
2.2.3	Conclusions.....	19
2.2.4	Gaps .....	21
<b>3</b>	<b>METHODOLOGY</b> .....	<b>22</b>
3.1	Philosophical paradigm .....	22
3.2	Research design.....	22
3.3	Data collection.....	23
3.4	Data analysis .....	24
3.5	Validity and reliability .....	26
3.6	Ethical considerations .....	27
<b>4</b>	<b>FINDINGS</b> .....	<b>28</b>
4.1	Security benefits of outsourcing.....	29
4.1.1	Quality improvement .....	29
4.1.2	Capacity enhancement .....	30
4.2	Security challenges of outsourcing .....	31
4.2.1	Loss of data control.....	31
4.2.2	Communication issues .....	32
4.2.3	Dependency.....	33
4.2.4	Supply chain attacks .....	33
4.3	Mitigation techniques for security issues .....	34
4.3.1	Control improvement .....	34
4.3.2	Vendor selection .....	36
4.3.3	Business continuity .....	37
<b>5</b>	<b>DISCUSSION</b> .....	<b>39</b>
5.1	What security benefits are associated with outsourcing IT services? .....	39

5.2	What security challenges are associated with outsourcing IT services?.....	40
5.3	In what ways can SMEs mitigate these challenges? .....	42
5.4	Limitations .....	44
<b>6</b>	<b>CONCLUSION</b> .....	<b>46</b>
	<b>REFERENCES</b> .....	<b>48</b>
	<b>APPENDIX</b> .....	<b>53</b>
	Appendix A - Email.....	53
	Appendix B - Interview guide .....	54
	Appendix C - NVivo.....	55
	Appendix D - Consent form .....	56

## **List of figures**

Figure 1	Systematic literature review process (Okoli & Schabram, 2010) .....	7
Figure 2	Literature review results .....	20
Figure 3	Themes and codes.....	26
Figure 4	Overview of findings .....	28
Figure 5	Literature and findings comparison.....	44

## **List of tables**

Table 1	Articles in literature review .....	11
Table 2	Interview respondents.....	24
Table 3	Thematic analysis process (inspired by Braun & Clarke, 2006) .....	25
Table 4	Challenges and mitigating measures .....	34
Table 5	Summary of findings .....	38



# 1 INTRODUCTION

In recent years, cybercrime has been on the rise as reported by many sources. Cybersecurity Venture expects global cybercrime costs to grow by 15 percent per year over the next five years reaching 10,5 trillion USD annually by 2025 (Morgan, 2020). The FBI's Internet Crime Report (2021) states that phishing related attacks have increased by more than twelve times since 2017. Looking at available information specifically related to Norway, the NorSIS report on threats and trends in 2021 also warns about an increase in ransomware and other digital threats (NorSIS, 2021). With these numbers in mind, it is clear that organizations must be aware of cyber threats and prepare for cyber incidents. There are several examples of recent cyberattacks against Norwegian corporations, such as in December 2021 when the food company Nortura (Nortura, 2021) and the media concern Amedia (Amedia, 2021) were both targeted.

Additionally, the COVID-19 crisis has given cybercriminals new opportunities to exploit businesses and individuals online. Interpol (2020), Europol (2020) and Verizon (2021) all report on increased cybercriminal activities as a result of the pandemic and people working from home. Employees now require remote access to company resources in order to do their jobs and attackers are utilizing this to compromise systems, gain access to information and disrupt services. As reported in Trellix 2022 Threat Predictions, the evolving threat landscape and ongoing global pandemic makes it more important than ever for businesses to keep updated on cybersecurity trends so that they can be proactive and actionable in protecting their data (Trellix, 2022). The developing trends in phishing, ransomware, malware, and Distributed Denial of Service (DDoS) attacks are therefore particularly challenging and worrying for businesses.

Despite this, the top management in small and medium-sized enterprises (SME) tend to think that their company is safe from cyberattacks because attackers are more likely to target larger enterprises (Bisson, 2021; Bullguard, 2020). Another survey uncovered that 20% of SME owners believe they have zero vulnerabilities (Bullguard, 2020). As a result of this, many SMEs are reluctant to implement security measures (Renaud and Weir, 2016).

However, contrary to the belief that they are not targets, research has proved otherwise. According to a 2019 study conducted by Ponemon Institute, "*cyber threats against SMEs are becoming more targeted*" (Ponemon Institute, 2019, p. 4). The study reports that 66% of SMEs experienced a cyberattack in the past year and that there was a significant increase in data breaches in SMEs over the past

three years (Ponemon Institute, 2019). These numbers are from an international study which included Norway.

In comparison to larger companies, SMEs typically have less resources and expertise to deal with the threats and less opportunity to overcome the issues. This is the reason many of them choose to outsource the task to a Managed Service Provider (MSP). As many as 83% of companies with an in-house security team are considering outsourcing to an MSP in 2021 (Syntax, 2021). This is a cost-effective way to harness cyber expertise and the MSPs have first-hand experience of what the latest threats are in a fast-changing environment (Hendy, 2021). Outsourcing to an MSP can have both positive and negative sides and it might have an effect on the cybersecurity in the organization. How outsourcing influences cybersecurity and what measures can be taken to mitigate the negative sides will be the focus of this study.

## **1.1 Research questions**

There is a lot of available research on how outsourcing can be beneficial and the challenges that it can present, but these are mostly international papers focused on larger organizations. Norway is one of the leading countries in Europe in terms of digitalization and it is therefore important to study this topic in a Norwegian context (Regjeringen, 2021). Additionally, security does not seem to be the focus of many studies and proposals for what can be done to mitigate security risks should be further researched, as will be described in the literature review. That is why this study asks the following research question:

**How does outsourcing IT services influence the cybersecurity in Norwegian SMEs?**

By including some sub questions, it is easier to investigate specific parts of the topic and find information that can be used to answer the main research question. These questions are narrower and break the work into more tangible parts. The sub questions in this study are:

**RQ1: What security benefits are associated with outsourcing IT services?**

**RQ2: What security challenges are associated with outsourcing IT services?**

**RQ3: In what ways can SMEs mitigate these challenges?**

## **1.2 Research approach**

This exploratory study implements a qualitative approach in order to reach our research objectives. A purposive sampling method was used to find suitable subjects and relevant data was collected through semi-structured interviews. An interview guide with open ended questions was created to assist in the interviews. To analyze the data, a thematic analysis with an inductive approach was conducted. A qualitative data analysis software was used to code the data in accordance with the descriptive coding method.

## **1.3 Thesis structure**

This thesis is divided into a total of six chapters. To provide an overview of the thesis structure, the remaining chapters and their contents are briefly introduced.

### ***Chapter 2 - Theoretical background***

This section primarily consists of two parts. Firstly, some background information that is necessary to understand the thesis is presented, and secondly, a review of already existing literature on the thesis topic is provided. The method that was used to conduct the literature review will be explained in detail, followed by its results and conclusions.

### ***Chapter 3 - Methodology***

In this section, the research approach that was used to conduct the research is addressed. This includes the philosophical paradigm, research design, data collection and data analysis. The process of the data collection and analysis is also presented. Additionally, how we ensured the validity and reliability of the study and what ethical considerations were taken into account are explained.

### ***Chapter 4 - Findings***

Here, we address our findings from the research. Themes that were identified through the interviews are presented together with quotes from participants.

### ***Chapter 5 - Discussion***

In this section, we discuss the findings in relation to what previous research has found. What our research agrees with, what it disagrees with and what gaps it fills are addressed. Also, we present and discuss some findings that were too underrepresented, but that we think are worth mentioning.

### ***Chapter 6 - Conclusion***

The conclusions that are drawn from the findings section are presented in this section. The research questions are revisited and suggestions for further research are proposed.



## **2 THEORETICAL BACKGROUND**

It is necessary to establish some theoretical background to be able to understand the context of the study. This chapter provides an overview of the background and previous research related to the thesis topic. A literature review was performed to ascertain the state of the art in the area of outsourcing and its impact on cybersecurity in SMEs. How this review was conducted will be explained, and its results and conclusions will be presented. Additionally, gaps in the literature will be identified.

### **2.1 Background**

This study includes some important terms that are central to the thesis topic. It is therefore necessary to explain these to enable the reader to fully understand the study.

#### *Small and Medium-sized Enterprises*

SME (Small and Medium-sized Enterprises) is a collective term for companies that have a number of employees under a certain limit. It has different definitions ranging from companies with 0-1000 employees (Gartner, n.d.A), 0-250 employees (European commission, n.d.) and 0-100 employees (NHO, n.d.). This study is focused on Norwegian mid-sized organizations and uses the European Commission's definition of companies with less than 250 employees.

#### *Managed Service Provider*

MSP (Managed Service Provider) is a specialized company that offers IT services and support to other companies. They can deliver services like networks, applications, infrastructure, and security, and supply their customers with support and administration (Gartner, n.d.B). MSPs can scale to whatever their client needs. MSPs that deliver security are often referred to as MSSPs (Managed Security Service Provider), but in this report, it will be included in the MSP term.

## ***Outsourcing***

Outsourcing is the business practice of farming out services or job functions to a third party. Companies may choose to outsource everything regarding IT or just some parts of it, depending on their needs. It is possible to outsource to an onshore company (in the same country), nearshore (neighbor country within same time zone) or offshore (more distant country) (Overby, 2017). Conventional outsourcing has involved using an MSP. Today, however, many providers offer cloud solutions to outsourcing, called cloud sourcing. In this study, the general term outsourcing refers to both conventional outsourcing and cloud sourcing.

## ***Cloud sourcing***

Cloud sourcing is the act where a company pays a third-party cloud hosting provider to deliver support and IT services. This is similar to conventional outsourcing but the cost for cloud computing services is more often based on a per-use model instead of a monthly or yearly fee (Knapp, 2018). The advantage of cloud sourcing compared to outsourcing is the ability to scale fast, and that customer demands can be realized faster than in the traditional way where you have to relate to an MSP (Fleutiaux, 2017). The data, services and applications are available on virtual platforms that the users can access anytime, anywhere (Sarangam, 2021). The providers and users of cloud sourcing are sometimes referred to as CSP (Cloud Service Provider) and CSU (Cloud Service User).

## **2.2 Systematic literature review**

A literature review was conducted prior to this study. The purpose of the review was to build a knowledge base for our further research. To make sure that enough reliable literature was found we decided to follow a specific method with well described steps.

### ***2.2.1 Method***

The preferred method for this review was a systematic literature review (SLR). An SLR can be beneficial as they deliver a clear and comprehensive overview of what evidence is available on a specific topic. They can also help identify gaps in earlier research suggesting what should be researched further to better understand the field (Peričić & Tanveer, 2019).

This systematic literature review is following a method developed by Okoli and Schabram (2010). This method was chosen as it is specifically designed for conducting SLRs in Information Systems (IS) research. While creating the guide, Okoli and Schabram used several different articles and guides involving both how to conduct an SLR and how to conduct reviews in IS. The method consists of eight different steps that are all essential to make sure the review is scientifically rigorous. The different steps are shown in figure 1 and will be described in detail.

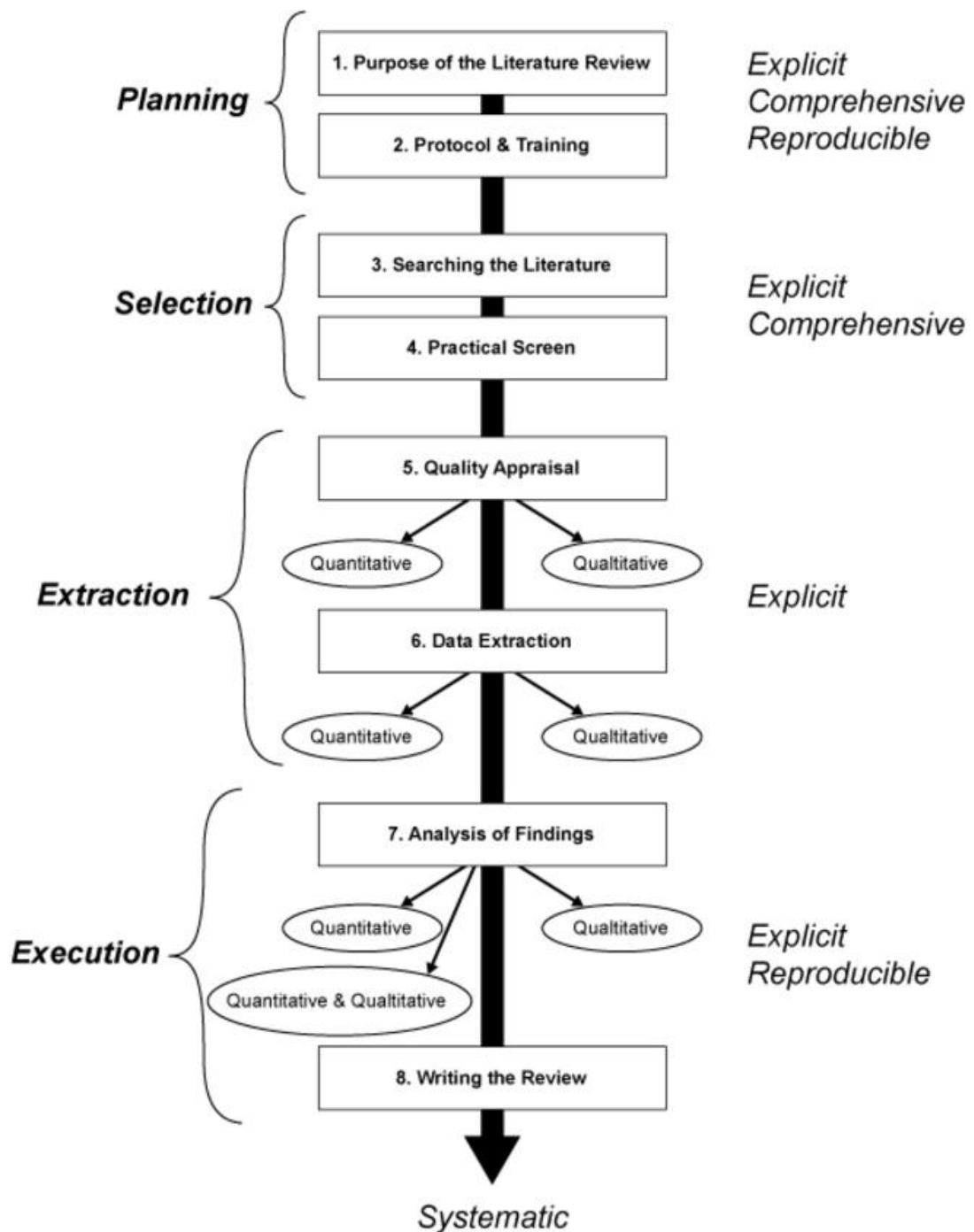


Figure 1 Systematic literature review process (Okoli & Schabram, 2010)

## **Purpose**

The systematic literature review provided an analytical approach to review relevant literature. As this was a literature review for an academic thesis, its main purpose was to investigate what earlier research had concluded regarding the thesis subject and to identify gaps that require further research. This way, the review also served the purpose of increasing our knowledge and understanding of our particular subject matter. In this thesis, the review assisted in gaining insight into what benefits outsourcing can bring for SMEs, what challenges they face and how they can potentially mitigate these issues. This insight was valuable when creating the interview guide and helped us know what to look for while further researching the topic.

## **Protocol**

As the review was conducted by two researchers, it was important that both researchers followed the same procedure. Therefore, a set of guidelines was created so that we were consistent and in agreement about how to conduct the review. The guidelines included instructions on how to conduct the search for literature, practical screen, quality appraisal and data extraction, the details of which are described in the following sections.

## **Search**

During the search process, certain queries, search engines, databases, journals, and criteria were used in order to find relevant literature. These were chosen to ensure that the search was comprehensive and relevant to the research questions.

The queries that were used covered the areas of the study well. They allowed us to find literature about outsourcing benefits, risks, and measures in SMEs, and made sure that they were relevant for the research questions. The queries that were used in the search process are as follows:

- Outsourcing IT in SME
- Outsourcing benefits / SME
- Outsourcing risks/challenges / SME
- Security issues with outsourcing SME
- Cybersecurity in SME
- Outsourcing cybersecurity
- Security challenges for SME

- Mitigate outsourcing security risks
- Cloud computing
- Cloud outsourcing

The databases and journals that we used to search for the literature were ProQuest, Scopus, and Senior Scholars' Basket of Journals, as well as the search engine Google Scholar. The databases and search engine were chosen as they provide large libraries of sources from many different research institutions and journals, which ensures comprehensiveness of the search. Google Scholar in particular produced a lot of results. The Senior Scholars' Basket of Journals were also specifically chosen as they are the top journals in the field of information systems, and relevant articles found in these journals are expected to be valid and of high quality.

Some initial criteria were used in the search process so that only literature relevant to the research questions were considered. For literature to be eligible for consideration, they needed to cover at least one of the following criteria:

- Identify security benefits with outsourcing either in SMEs or in general
- Identify security risks or challenges with outsourcing either in SMEs or in general
- Identify mitigating measures to deal with the risks or challenges
- Discuss cybersecurity considerations in SMEs
- Answer one of the specific research questions

### **Practical screen**

The search resulted in a large number of articles. Therefore, a practical screen was carried out to decide which of these articles were relevant enough to be considered for the review. To be able to judge whether to include or exclude articles, some criteria were formed. These were as follows:

- Article type: Only valid research articles, papers, PhD/Master theses or book chapters. Editorials, research opinions and commentaries will be excluded
- Publication date: Only literature published after 2005. Articles prior to this year can only be used if the contents are still relevant regardless of publication date
- Publication language: Only literature published in Norwegian or English
- Publication source: Only literature published by or from academic journals, research institutions or books

- Citation: Preferably literature that has been cited by others

### **Quality appraisal**

Once it had been decided what articles to include based on the practical screen criteria, they had to be examined more closely to assess their quality. To this end, we developed a set of questions to determine if the quality of the articles were sufficient. Articles with inadequate quality were excluded from the review. The questions were as follows:

- Does the literature pass all criteria for practical screening?
- Does the literature address a clearly focused question?
- Does the researcher use a valid method for research?
- Does the researcher provide evidence to support their arguments and conclusions?
- Does the research have any bearing on the research questions of this study?

### **Data extraction**

At this stage, we had compiled a complete list of articles to include in the review and could proceed to extract the relevant data. Any information that was applicable to the research was deemed relevant. The extraction was conducted by thoroughly reading the articles and systematically extracting the applicable information.

### **Synthesis of studies**

During the synthesis, we analyzed the extracted information and identified commonalities and patterns. The purpose of this was to make sense of the vast amount of information collected from the review.

### **Writing the review**

Lastly, we wrote the actual review. The literature results and conclusions are reported in the following sections. Table 1 shows an overview of the articles used to write the literature review.

Table 1 Articles used in literature review

Article	Keywords	Theme		
		Benefits	Challenges	Mitigations
Ackermann et al., 2012	Malicious insiders, multi-tenancy, availability issues		■	
Almutairi & Riddle, 2018	Increased knowledge and experience, loss of data control, loss of technical skills	■	■	
Bachlechner et al., 2014	Audits, legal issues		■	
Beaumont, 2006	SLA			■
Cezar et al., 2013	Double moral hazard, several MSPs, SLA		■	■
Chow et al., 2009	Loss of data control, malicious insiders, multi-tenancy, due diligence, audits, availability issues, trust issues		■	
CSA, 2020	Malicious and negligent insiders, multi-tenancy		■	■
di Vimercati et al., 2012	Loss of data control		■	
Dickmann et al., 2010	SLA			■
Dodds, 2021	Ability to scale, greater compliance, better efficiency	■		
Catteddu & Hogben., 2009	Increased quality, loss of governance, malicious insiders, multi-tenancy, incomplete deletion, availability risks, legal issues, security awareness	■	■	
Feng et al., 2020	Increased quality, loss of data control	■	■	
Fenn et al., 2002	Increased expertise	■		
Goo et al., 2008	SLA			■
Green & Green, 2014	Multi-tenancy, legal issues		■	
Ashraf & Jawad, 2018	Loss of data control, multi-tenancy, availability issues, legal issues		■	
Karyda et al., 2006	Loss of data control, legal issues, loss of technical skills, security policies, several MSPs, security awareness		■	■
Kaur & Singh, 2015	Loss of data control, availability issues, due diligence, audits, legal issues		■	
Khalil et al., 2014	Malicious insiders, multi-tenancy, audits, availability issues		■	
Khan et al., 2012	Malicious insiders, multi-tenancy, availability issues, loss of technical skills		■	
Khorshed et al., 2012	Malicious insiders, multi-tenancy		■	
Kumar et al., 2015	Malicious insiders, availability issues		■	
Lee et al., 2013	Double moral hazard		■	
Nero, 2018	Access to technical knowledge	■		

Pang & Tanriverdi, 2022	Fewer security incidents	■		
Ristenpart et al., 2009	Multi-tenancy		■	
Rowe, 2007	Increased experience, malicious insiders, loss of technical skills, trust issues, liability	■	■	■
Tafti, 2005	SLA			■
Wulf et al., 2019	Malicious insiders, multi-tenancy, audits, availability issues, legal issues, security awareness, trust issues, several CSPs, SLA		■	■
Xiao & Xiao, 2012	Loss of data control, malicious insiders, multi-tenancy, availability		■	

### 2.2.2 Results

The literature shows many different positive and negative sides of outsourcing. As this study focuses on how cybersecurity is influenced by outsourcing and not how it generally influences a company, the review focused on studies in which security was the main topic. This resulted in findings regarding the benefits and challenges to security when outsourcing, as well as possible mitigations to the raised issues.

#### Security benefits of outsourcing

The literature includes few security benefits of outsourcing, but we have found some ways in which companies' security is positively influenced by this practice. These are divided into various categories, however, one thing they all have in common is that they impact the security quality.

#### *Service quality*

The main reason that companies choose to outsource their IT services, which is the most obvious, is how it increases the quality of the services. Research has shown that it improves quality in several ways and since the MSP are specialized in a specific IT area, they will have greater knowledge and experience. This enables them to deliver better solutions more effectively (Almutairi & Riddle, 2018). The experienced staff will spend all their time monitoring networks and being updated on latest vulnerabilities, new hacker tools and new security patches and updates (Rowe, 2007). Fenn et al. (2002) came to the same conclusion and added that it is easier to gain a greater level of expertise by outsourcing than obtaining this in-house.



### *Multiple and similar clients*

An MSP often focuses on a specific industry or on providing a particular service which might lead to them having more similar clients. The organizations that use this MSP will benefit as the MSP uses knowledge gained from other clients. Considering this, MSPs that serve multiple client firms in the same industry contribute to improved security quality (Feng et al., 2020).

### *Cloud solutions*

As mentioned, access to patches and updates is a big benefit of outsourcing. Updates via the cloud can be rolled out more rapidly to the platform that the customers use compared to in a traditional client-based system that rely on the patching model. Large cloud providers can also offer a standardized open interface that MSPs can supply their customers with at a low cost (Catteddu & Hogben, 2009). Using the cloud can give organizations access to technology in the same way as with conventional outsourcing but the difference lies in the cost. In addition, Pang & Tanriverdi (2022) argue that moving to the cloud can have a positive effect on IT security. They found that federal agencies that migrate their legacy IT systems to the cloud enhanced the defense and that they experienced fewer security incidents.

### *Suitable for SMEs*

Outsourcing to a supplier that entirely focuses on securing IT and systems could specifically give great benefits for SMEs. These companies have limited resources due to their size and IT security is a comprehensive subject. Outsourcing to an MSP can provide the ability to scale, deliver greater compliance and better efficiency of security solutions (Dodds, 2021). By outsourcing, SMEs can expect to have greater access to technical knowledge which will help them understand the risks and invest to mitigate them (Nero, 2018).

### **Security challenges of outsourcing**

The literature shows huge focus on the security challenges regarding outsourcing. However, the results indicate that there is a lack of research on SMEs specifically. Therefore, the following challenges are concerning companies in general and may

or may not be applicable for SMEs. The literature discusses issues regarding control, attack surface, internal competence, and trust, among others.

#### *Loss of data control*

The first, and biggest, issue with outsourcing one's IT services is loss of data control (di Vimercati et al., 2012). More specifically, this entails loss of confidentiality, integrity, and potentially availability. According to a report by ENISA, loss of governance is one of the top security risks of cloudsourcing (Catteddu & Hogben, 2009). This also applies to conventional outsourcing. When a company decides to outsource their IT services, their data is often stored at the provider's premises (Karyda et al., 2006). This naturally means that they cannot ensure the confidentiality and integrity of their data as the servers are controlled and managed by potentially untrustworthy entities (di Vimercati et al., 2012; Xiao & Xiao, 2012; Kaur & Singh, 2015; Almutairi & Riddle, 2018, Ashraf & Jawad, 2018; Feng et al., 2020). Furthermore, service providers may use subcontractors who the client has even less control over (Chow et al., 2009).

#### *Malicious and negligent insiders*

Malicious and negligent insiders are one risk regarding confidentiality and integrity of data. A malicious employee of the MSP or CSP can use an administrative account to get access to confidential data (Ackermann et al., 2012; Catteddu & Hogben, 2009; Khorshed et al., 2012; Xiao & Xiao, 2012; Kumar et al., 2015; CSA, 2019). They may then steal proprietary information and sell it to competitors (Rowe, 2007; Chow et al., 2009; Khan et al., 2012; Khalil et al., 2014; Wulf et al., 2019). In addition, negligent insiders are a huge concern for companies as they are the leading cause of security incidents (CSA, 2019).

#### *Multi-tenancy*

The multi-tenancy nature of MSPs and CSPs presents some risks as well. As these providers offer services to a multitude of clients, they possess a large quantity of data. Simultaneously, data are becoming the main target for cyber-attacks, making service providers a prime target for attackers (Khorshed et al., 2012; Green & Green, 2014; CSA, 2019). Moreover, in outsourcing practice, data are sent and stored over the internet. As such, adversaries can intercept, access, steal or alter data either in transit or while stored (Ackermann et al., 2012; Catteddu & Hogben,

2009; Green & Green, 2014; Wulf et al., 2019). Particularly for cloud sourcing, shared resources are a core feature of the cloud and multiple clients' data are often stored on the same physical hardware (Ristenpart et al., 2009; Catteddu & Hogben, 2009; Xiao & Xiao, 2012; Wulf et al., 2019). In such shared environments, it is possible that either errors or attacks can cause one tenant to gain access to another tenant's data (Catteddu & Hogben, 2009). Possible attacks include guest-hopping attacks, SQL injection attacks and cross-VM side-channel attacks (Chow et al., 2009; Ristenpart et al., 2009; Khan et al., 2012; Catteddu & Hogben, 2009; Khorshed et al., 2012; Xiao & Xiao, 2012; Khalil et al., 2014; Ashraf & Jawad, 2018; Wulf et al., 2019).

#### *Due diligence and audits*

Another side effect of losing data control is difficulties with due diligence and audits. Companies may not know exactly where their data is physically stored (Kaur & Singh, 2015; Wulf et al., 2019). Also, it might be challenging to perform audits at the MSP or CSP as they are often global and situated in another country. This is even harder if the provider is using a subcontractor (Bachlechner et al., 2014). These are major transparency issues. How can companies guarantee that data has been deleted according to the retention policy of the provider? How can they ensure that due diligence and audits are performed correctly? (Chow et al., 2009; Catteddu & Hogben, 2009; Khalil et al., 2014; Wulf et al., 2019).

#### *Availability*

In terms of availability, there are several risks that can lead to companies not having access to their data and services. Internet connection issues on the client side or system malfunctions on the provider side may cause loss of availability (Ackermann et al., 2012; Catteddu & Hogben, 2009; Khan et al., 2012; Ashraf & Jawad, 2018; Wulf et al., 2019). DDoS attacks may disrupt services from CSPs by overloading their systems (Catteddu & Hogben, 2009; Khan et al., 2012; Xiao & Xiao, 2012; Khalil et al., 2014; Kumar et al., 2015; Ashraf & Jawad, 2018; Wulf et al., 2019). CSPs are a single point of failure meaning that attackers can deny many users access to services simultaneously (Chow et al., 2009). Furthermore, targeted attacks against a CSU may result in account lockout after too many denied authentication attempts. Another risk is that the CSP may revoke access to their services due to financial disputes with the CSU (Kumar et al., 2015; Wulf et al., 2019). Lastly, natural disasters and other incidents such as server crashes, fires or earthquakes might lead to data being lost if the provider fails to recover it

(Catteddu & Hogben, 2009; Khan et al., 2012; Kaur & Singh, 2015; Kumar et al., 2015; Wulf et al., 2019).

### *Legal issues*

Relating to the challenge of data control are the legal issues presented by the outsourcing practice. Confidential, and sometimes sensitive, data are transferred, accessed, and stored by multiple parties. This becomes a problem especially when the service provider, and consequently the stored data, are located in another country than the client (Catteddu & Hogben, 2009; Bachlechner et al., 2014; Green & Green, 2014; Ashraf & Jawad, 2018). Different countries or regions may have different laws about liability, security and the processing and storing of personal data (Karyda et al., 2006; Wulf et al., 2019). One example of such a law is the General Data Protection Regulation (GDPR), which is the applicable data protection law for the companies included in this study. According to this piece of legislation, it is both the client and the service provider who is responsible for ensuring that all data protection principles are respected and that the processing of personal data complies with the law, regardless of whether this task has been outsourced or not (GDPR, n.d.). This is a major legal issue as many companies assume that this responsibility is automatically transferred to the service provider if they outsource the data processing tasks (Karyda et al., 2006; Kaur & Singh, 2015; Wulf et al., 2019).

### *Loss of internal competence*

Moving on from the issue of data control, the literature also identifies loss of technical skills and security competence as a challenge with outsourcing. Total security outsourcing involves moving all security functions and responsibilities out of the company, which entails a loss of technical security skills internally (Karyda et al., 2006; Rowe, 2007). Companies must exercise caution to avoid developing a technical dependency on the provider (Almutairi & Riddle, 2018). In time, this also carries the risk of halting the development of a security culture within the company and might leave employees with a lack of security awareness. This increases the risk of social engineering, phishing attacks, and human error due to lack of knowledge (Catteddu & Hogben, 2009; Khan et al., 2012; Wulf et al., 2019). The issue is further complicated if a company decides to terminate the outsourcing arrangement and return the security functions and responsibilities in-house (Karyda et al., 2006).

### *Trust*

In security outsourcing, the company and the service provider must trust each other to do their part. It is key that both parties spend enough resources and effort to prevent security incidents for the outsourcing arrangement to be successful. However, due to the sensitive nature of security, neither party can perfectly observe or verify each other's efforts (Rowe, 2007; Chow et al., 2009; Cezar et al., 2013; Lee et al., 2013; Wulf et al., 2019). Thus, a double moral hazard problem can quickly occur if both sides fail to exert sufficient effort (Lee et al., 2013). Furthermore, when security breaches happen, it is difficult to clearly attribute the liability to one party. Some providers may therefore decide not to disclose breaches to avoid potential fees or try to reduce costs by sacrificing some security aspects (Catteddu & Hogben, 2009; Lee et al., 2013; Wulf et al., 2019). Although higher quality of security services is one of the core benefits of outsourcing, the quality may actually decrease as a result of the double moral hazard problem and different incentives (Rowe, 2007; Catteddu & Hogben, 2009).

### *Provider focus*

Another issue with security outsourcing is the risk of using a single provider for security services. Two services that are often outsourced by companies are prevention and detection. If these services are outsourced to the same provider, a conflict of interest may arise due to the interdependency of the two services. Detection is all about detecting an ongoing attack, while prevention regards preventing attacks from happening in the first place. Thus, if the MSP detects an attack, they implicitly acknowledge that they failed to prevent the attack. MSPs might therefore choose to focus most of their effort on prevention and less on detection (Cezar et al., 2013).

### *Organizational insight*

Other services that are often outsourced include development and implementation of security policies. However, in this case, the policies and procedures are developed by MSPs that lack insight into the organizational context and culture of their clients. As such, the security policies are more likely to hinder business objectives and be confronted with employee resistance (Karyda et al., 2006).

## **Mitigation techniques for security issues**

While looking for mitigation techniques in the literature, we found that there is little focus on this, similarly to security benefits. Considering the challenges that were identified, the literature only provides measures for some of them.

### *Multiple suppliers*

To deal with the issue of having a single outsourcing provider and the challenges with conflict of interest this brings, one suggested solution is that organizations could use several MSPs with different tasks (Karyda et al., 2006). An organization could, for example, use one MSP for prevention assistance and another for detection. This could also be applied when using CSPs by applying a multi-cloud approach to enhance the availability of critical applications. However, this might increase the risk of leakage and integrity (Wulf et al., 2019). How much impact this approach has is not thoroughly studied but it may not have the desired effect as it eliminates the advantages that having one provider brings (Cezar et al., 2013; CSA, 2019).

### *Service Level Agreements and contracts*

Several earlier studies suggest that a focus on a Service Level Agreement (SLA) would be valuable when outsourcing (Goo et al., 2008; Beaumont, 2006; Tafti, 2005). An SLA is a formal contract used to guarantee that consumers' service quality expectation can be achieved (Wu & Buyya, 2012). To help mitigate the issue of double moral hazard, contracts including liability alignment would be beneficial from the customer's side. If the MSP would agree to be liable for attacks, their customers could expect that the MSP exert their maximum effort (Rowe, 2007). This may not be a dream scenario for the MSPs, but a solution where the MSP are rewarded for revealing security breaches and a penalty if found responsible for the breach would benefit both parties (Cezar et al., 2013). In any way it is used, an SLA is a key component to ensure that the provider is living up to the requirements. The SLA can include quality measures such as prevention of specific breaches and event response time, commitment for the provider to do certain tasks and service restoration (Wulf et al., 2019; Cezar et al., 2013). Surveys conducted also indicate that customers look at the SLA as an approach that would increase their trust in the MSP (Dickmann et al., 2010).

### *Security awareness training*

As the human factor is an important thing to consider in cybersecurity, organizations that outsource their IT services must give this extra attention. Organizations need to train their employees in security awareness as they might store sensitive data. When this data is stored in a cloud solution the employees must have knowledge about security, data privacy and risk management (Wulf et al., 2019). This would also apply to companies that engage in conventional outsourcing and store their data at an MSP. The top management is responsible for ensuring that some level of IT security knowledge and expertise is maintained within the organization (Karyda et al., 2006).

### **2.2.3 Conclusions**

The reviewed literature shows that the topic of outsourcing has been researched to some extent and both positive and negative sides of this have been discovered. It is mostly covering the challenges of outsourcing leaving the benefits and mitigation techniques with less focus. The most recent articles discussing the thesis topic are focusing more on cloudsourcing rather than conventional outsourcing as cloudsourcing is the next generation of outsourcing. For an overview of the literature review results, see figure 2.

The benefits related to security are focused on how outsourcing increases the quality of the security. By using an MSP, the companies gain access to specialists that have broad experience and knowledge regarding the subject. As the MSPs often serve several customers, they can use the knowledge gained from other clients to provide better protection.

A lot of articles in the literature address many of the same challenges. Companies that outsource might lose control of the data that they own as it is stored in facilities they do not control. Due to this loss of control, there is also a threat to the confidentiality, integrity, and possibly the availability of the data. Multi-tenancy is also mentioned as a challenge. As the service providers often serve multiple clients and have large amounts of data, they are a valuable target for hackers. There is also a possibility of gaining access to other clients' data due to errors. Furthermore, by fully outsourcing the IT services to a third party, companies can end up with no competence or experience in-house. This may make them technically dependent on the service provider and it may influence the security awareness in the company. In addition to this, if they choose to outsource to a single MSP, the provider might have a greater focus on trying to prevent incidents and less focus on detecting them. The last challenge found was that there also is a legal issue that is discussed as different countries have different laws. Is

the provider you are using following GDPR? Do the subcontractors that may access or store your data also comply with the regulations?

There are some different mitigation techniques that are mentioned which may help with some of the challenges. One discussed solution to avoid conflict of interest is to use several MSPs that focus on different tasks, but not enough research is conducted to present this as a viable solution. One recurring point is the contract between the MSP and the companies. Including an SLA could be beneficial to ensure that the expected quality of the services is met. The last mitigation technique found in literature is regarding the employees' awareness. By training the employees in security awareness the issue of human error can be mitigated.



Figure 2 Literature review results



#### **2.2.4 Gaps**

What is missing in literature is more specific research on how cybersecurity is influenced by the outsourcing practice. It is possible to see some connection between the effects on the companies and how cybersecurity is influenced, but more concrete impacts should be pointed out. Benefits related to how security will be improved and mitigation techniques for the challenges is also lacking and should be studied further. Another thing that the literature does not cover very well is how SMEs specifically are influenced. The available literature is mostly focusing on bigger companies and for SMEs it might be hard to relate to this. Lastly, we found no research about our topic in Norwegian context which presents another gap.

## **3 METHODOLOGY**

The methodology describes the research method that was used to collect and analyze data in the study. An overview of the research approach and design is first provided. Thereafter, data collection and analysis are addressed. Lastly, validity and ethical considerations of the study are discussed.

### **3.1 Philosophical paradigm**

Our philosophical paradigm is of an interpretivist nature. We believe that truth and knowledge is subjective and that experiences in life and the understanding of them shape what people perceive as real. This can for example be influenced by their culture or the environment they grow up in. Our choice of research method reflects this paradigm. In our study, we research how outsourcing impacts the cybersecurity in SMEs. Our research questions require a deeper understanding of the phenomenon and cannot be answered purely with numbers and statistics. This means that we are not doing a positivist study. Instead, we collect data in a qualitative manner by conducting interviews with SMEs about their knowledge and experience with the topic. Therefore, our findings are based on our interviewees' intersubjective understanding and what they perceive as true. Additionally, as researchers, our own experiences and beliefs will influence the way we interpret the collected data, meaning that we are doing an interpretivist study (Ryan, 2018).

### **3.2 Research design**

This exploratory study applies a qualitative research method. Qualitative research methods are beneficial when a researcher wants to study social and cultural phenomena. These methods are designed to gain an understanding of why people do what they do in the cultural context they are in (Myers, 2022). The purpose of this study is to look at how outsourcing IT services influences the cybersecurity in Norwegian SMEs. It focuses on understanding how and why companies are influenced and what can be done to mitigate the negative effects. Therefore, we believe a qualitative approach would be the most suitable method for this study.

We are looking to explain and understand a social phenomenon and qualitative research can help us accomplish this.

We chose to conduct an exploratory case study. This is the most used method in qualitative research, and it is an empirical inquiry that investigates a phenomenon in a real-life context (Myers, 2022). As we want to study different companies and try to find ways to mitigate negative effects, it is important that we understand the challenges. According to Mfinanga et al. (2019), a case study would be beneficial when the aim is to find answers to “how” and “why” questions. An ethnographic approach could also be appropriate for this study, but we found case study more suitable due to limited time to spend in the field.

### **3.3 Data collection**

The data in this study were collected through interviews. The organizations that were considered for the data collection phase were limited to Norwegian SMEs that had less than 250 employees. They were also required to have experience with outsourcing of IT services, either having done so previously or doing it currently. The collection period was limited to 2 months or until satisfactory data saturation had been achieved and no new findings emerged. The individuals that were preferred to join the interviews were CISO's, CIO's, CTO's or whoever was responsible for cybersecurity in the organizations.

To find suitable subjects for the study and stay within the limitations, a purposive sampling method was used. Companies were purposely selected based on our personal judgment and the given limitations. This was a fitting sampling method for the study as only certain companies were appropriate for the research. It also ensured a cost-effective and time-effective sampling process. Using this method, we browsed through the member list of the trade association in Kristiansand and utilized the segmentation feature at proff.no to search for companies between 20 and 250 employees and look for suitable subjects. After finding a promising candidate, we went to the organization's website to learn more about them and ensure that they met the requirements for contribution. An email was then sent to the IT manager or CEO detailing the purpose of the study and requesting an interview (see appendix A). This was repeated until we had found enough subjects for the study.

We decided to use semi-structured interviews as this would allow us to obtain detailed information about companies' experiences with outsourcing. This also enabled us to ask additional questions and delve deeper into topics that arose during the interviews. To this end, an interview guide was created with some set questions that could help steer the interviews (see appendix B). The questions were based on our research questions, findings from our literature review and

information gathered by having an informal discussion with an MSP. The interview guide contained some general questions about the company and their outsourcing relationship as well as questions about what benefits and challenges they had experienced and possible mitigations they had implemented. The questions were open ended to remove researcher bias and allow respondents to answer freely and bring up new topics.

We were able to conduct ten interviews with companies in different sectors as shown in table 2. Most of these were currently outsourcing. Only one company did not, but they had experience with outsourcing previously. Eight interviews were conducted online over Microsoft Teams and two interviews took place physically. The interviews were recorded for transcribing purposes with the respondents' consent. During the data collection phase, we observed that the interviews were a bit shorter than we initially anticipated. The interviews lasted between 19 and 39 minutes. Some of the respondents did not have much background in IT and thus had less elaborate answers. Otherwise, the interviews went as expected.

Table 2 Interview respondents

<b>ID</b>	<b>Role</b>	<b>Industry</b>	<b>Approximate size</b>	<b>Outsourcing duration</b>	<b>Interview length</b>
#1	IT manager	Entertainment	150-200 employees	10 years	24:45
#2	Security manager	Construction	200 employees	6 years	30:04
#3	IT manager	Public service	100 employees	1.5 years	30:08
#4	Senior advisor	Consulting	40 employees	12 years	35:33
#5	Production manager	Manufacturing	30 employees	13 years	19:27
#6	Lawyer	Law firm	15 employees	10 years	31:04
#7	General manager	Transportation	80 employees	2.5 years +	35:29
#8	CEO	Electronics	100 employees	15 years	25:32
#9	CTO	Communication	150 employees	16 years	32:30
#10	General manager	Maritime	60 employees	13 years	38:53

### 3.4 Data analysis

To analyze the data, we have applied a thematic analysis inspired by Braun and Clarke (2006). We chose this method because we wanted to identify patterns in our data, and it provided a rigorous way to achieve this. An inductive approach to

the analysis was chosen as we did not have any theory or hypothesis beforehand to test. We wanted to derive new findings from our research and turn it into knowledge. Using an inductive approach also allowed our results to better represent the data and not our own beliefs. The analysis process consisted of six steps as shown in table 3.

Table 3 Thematic analysis process (inspired by Braun & Clarke, 2006)

<b>Step:</b>	<b>Description:</b>
1. Familiarizing ourselves with our data	Transcribing the interview data. Reading and re-reading the data. Noting down initial ideas
2. Generating codes	Coding relevant pieces of data across the entire data set. Collating data relevant to each code
3. Categorizing codes	Creating categories based on our research objectives. Collating codes into each category
4. Generating themes	Creating themes. Collating codes into themes
5. Analyzing themes	Reviewing and validating themes. Ensuring that the coded extracts correspond to their respective themes
6. Producing the report	Selecting data extracts. Illustrating findings. Relating findings to research objectives

The first step of the data analysis process started with transcribing the interviews. This was done to gain a better understanding and insight into the interview responses and turn it into written form for further processing. As transcribing is a time-consuming task, we divided the interviews between both researchers and then read each other's transcripts to familiarize ourselves with the data.

In the second step, we proceeded to create codes based on pieces of data that were relevant to our research objectives. Furthermore, we collated all data which were relevant to each code. We used NVivo 12 Pro, a qualitative data analysis tool, during the coding process (see appendix C). The transcriptions were imported into the program, and we manually went through them to identify codes using a descriptive coding method (Miles et al., 2014). This method suited our study as it allowed us to create codes that summarized relevant topics found in the data. These could either be words or short phrases that described certain pieces of information. By focusing on the information given by the respondents, we ensured that we remained objective, limited researcher bias and stayed as true to their meaning and intent as possible.

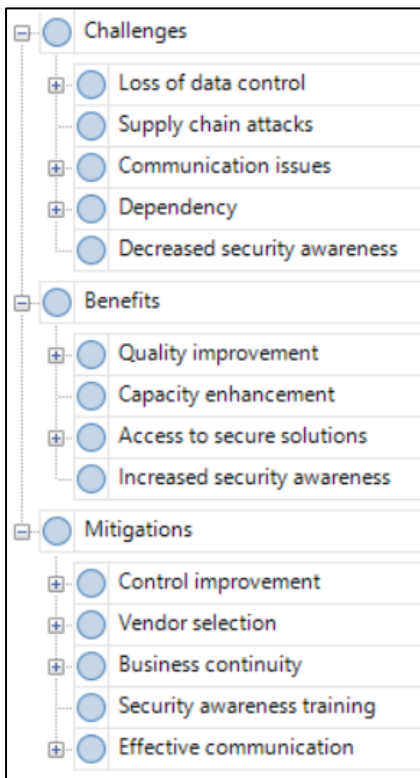


Figure 3 Themes and codes

The third step included creating categories according to our research objectives and clustering the codes into the corresponding categories. Following our objective to find security benefits with outsourcing, we created the “benefits” category. Furthermore, we also want to identify security challenges and thus we created “challenges” as a category. Lastly, we created the “mitigations” category as we aim to identify ways to mitigate the security challenges posed by outsourcing. This made it easier for us to keep track of what objective each finding was related to.

In the fourth step, we generated themes within each category. Codes that had comparable topics were grouped together and given new names. The results of steps three and four are shown in figure 3.

In step five, we analyzed the themes to ensure that they were correct and without errors. Themes were reviewed and validated to check if they worked in relation to the codes and extracts.

Inaccurate themes were renamed or combined. Incorrect codes and extracts were either moved to another theme or removed entirely.

In the last step, we finalized the analysis and wrote the findings section. Themes and codes were studied in depth and related back to the research objectives and literature. Descriptive and compelling quotes to be used as evidence in the findings were selected. The final results are reported later in the findings section.

### 3.5 Validity and reliability

To make sure that the tools, techniques, and processes are appropriate some measures have been applied. To avoid personal bias, our supervisor from UIA functioned as a moderator. The different tools and techniques were discussed with the moderator to secure that the research was valid. The interviewed companies were selected from diverse industries to get a deeper understanding of the phenomena. The interviews were done until no new answers were given which also promotes validity.

As several answers from the respondents correspond it is expected that the research is reliable. Comparison and testing of data was done with NVivo to keep

the data organized and to establish authenticity. Quotes from the interviewees are also present to support and demonstrate the findings.

### **3.6 Ethical considerations**

Because gathering data for the project is such a crucial aspect, some ethical considerations must be made. The first action was to get the research and data collection approved by The Norwegian Centre for Research Data (NSD) which is a national center and archive for research data (NSD, n.d.). The approval means that the procedures in the data gathering are accepted. The participants in the research were made aware of the procedures and a consent form was signed by every participant (see appendix D). The consent form included information regarding voluntary participation, meaning that they could freely choose to be included or excluded at any point during the project. It also mentioned how the data was anonymized and that the voice recordings from interviews were deleted after transcribing them. The only information kept from the interviews was the answers given and a description of which sector the company operates in. The research is also unbiased, and the findings represent the actual answers that were given.

## 4 FINDINGS

After analyzing the data, we reached some findings regarding our research questions. These will be presented in this section. Not all themes identified in the analysis will be included in this section as some of them are too small to be considered as findings. Topics with at least 30% presence in the interview responses are included in our findings. A complete overview of the findings identified in the analysis is provided in figure 4. When presenting our findings, we include quotes from the interviews which are highlighted in italics. All quotes are translated by us from Norwegian to English and so there is room for interpretation. A summary of the findings with some example quotes can be seen in table 5 at the end of chapter four.



Figure 4 Overview of findings



## 4.1 Security benefits of outsourcing

Firstly, in the findings, we will present the security benefits that have been identified in our study. Mainly two benefits were found: quality improvement and capacity enhancement.

### 4.1.1 Quality improvement

The most prominent finding regarding how security can benefit from outsourcing is how it increases the quality. A majority of the interviewees responded that the quality of the cybersecurity is increased when outsourcing the task. The main reason that the quality is better is the access to the competence that using an MSP gives. The MSP's deliver in-depth competence on different areas, access to updates and knowledge about the current threat landscape. One of the participants stated:

*[...] it is their competence, access to updates and what is going on related to security that makes us sleep well at night knowing that we are taken care of. Someone is handling our systems and making sure that we are protected where we need to be.*

For SMEs, this competence is hard, if not impossible, to obtain in-house due to limited resources. Another participant highlighted this by saying:

*[...] it is quite comprehensive to maintain updated on IT, especially related to the security that we are currently discussing. Keeping updated would be too hard for us to do in-house.*

An MSP also has a bigger environment that is beneficial to ensure cybersecurity. They have colleagues to discuss issues with and they can divide tasks to focus on their area of expertise. Having access to this environment ensures that the employees are updated on the cybersecurity front, and this is hard to obtain as a single IT employee in a company. As two participants said:

*They [IT employees] are dependent on being part of a network to maintain updated on security and other stuff. If you are alone in a company, it can get a bit lonely.*

*He [IT employee] needs an environment with others in the same position to spar with.*

Findings also show that the quality can be improved by the fact that the MSPs has several clients. This gives the MSP the possibility to take learnings regarding

security solutions from one customer and apply it to the others. They might also get critical questions, comments, and suggestions from one customer that might be beneficial for others. A company mentioned this when they said that:

*[...] if you use an external supplier as we do, it is more likely that they [the MSP] are met with more critical questions from customers with diverse competence internally.*

These critical questions that more “experienced” companies ask can be a huge advantage for smaller companies that do not have internal competence regarding IT security. A small company might not have the skills to verify that what the MSP delivers is of a certain standard, but by knowing that the MSP has customers with bigger demands, they can expect the MSP to deliver secure solutions. This was mentioned by a smaller company that said:

*[...] we know some of the other customers they [the MSP] have. Those are larger companies that are dependent on top security. So, it is good for us to be in the same boat as them.*

#### **4.1.2 Capacity enhancement**

The second finding that was shown as a security benefit of outsourcing is capacity. The MSPs have bigger capacity regarding manpower. Being able to have the same number of IT employees in a company as you get from using an MSP would be too expensive. Several respondents mentioned this, and it was commented that:

*For a company like ours that has few employees and limited turnover there is no possibility to have a team of IT employees to work with it [IT security]. We are too small for that.*

With bigger capacity the MSP is also able to react to several issues at a time. Encountering several issues while managing IT security in-house might force the IT department to prioritize issues. If these are security issues, it can lead to some problems not being solved as soon as they should be. The advantages brought by an MSP with a bigger workforce was highlighted by one company that said:

*If challenges would appear at the same time, we would have to prioritize what is the most important. Being the one responsible for doing this or being the one with the least important issue is an unfavorable situation. Now, we have a totally different capacity on the other end, so several issues can be solved at the same time. So, I would say that that is the main difference [outsourcing vs in-house].*

One respondent said that when they were exposed to a security incident, the help from the MSP was vital. Without the MSP they would not have been able to get operational as fast as they did, and they felt that the entire organization was helping them with their problem. He said that:

*[...] they really turned around and helped us a lot to get back to normal operation again. So, without their help it would be very hard.*

## **4.2 Security challenges of outsourcing**

Our research has also found several security challenges. These are loss of data control, communication issues, dependency, and supply chain attacks.

### **4.2.1 Loss of data control**

Out of all the challenges we identified in the interviews, what they most often brought up was the loss of data control. Not having control of your own data can pose several security challenges and it seemed like the interviewees were, to some degree, aware of this. It was said that the challenge of knowing where the MSP are storing their data was something they saw as a risk but not all was sure how to deal with this issue. The size of the MSP and which solutions they use were also a complicating factor that they mentioned when they said:

*But speaking of data storage, if that is within Europe or Norway and such, that is... that would be almost impossible to keep track of with cloud solutions.*

*The bigger and more international the supplier is, the harder it gets to check where the data is actually stored.*

The availability of the data is also a problem due to the loss of control. Different events can affect how the companies can access their data and can lead to severe problems if access is denied for a longer period of time. Events that could influence the access are smaller things like internet connection and bigger issues like sanctions in other countries where data are stored. Both issues were mentioned by respondents who said:

*There are companies that are hit really hard by what is happening further east.*

*The other [challenge] is that we are very vulnerable regarding network problems. If the network fails, we have nothing. So that is a big challenge.*

Loss of data control leads to another challenge for the different companies. Since it is hard to check how and where the MSP stores the data, this leads to the issue of trust. The companies that outsource are “forced” to trust that their MSP acts in a certain way and that they keep the data safe. It is hard to know how the MSP solves the different tasks that they are given, and the customers have no other choice than to trust that it is done correctly. Several respondents saw this as a big challenge and said:

*It is hard to know what the supplier does. Because I can ask for a solution, but I have no idea of which shortcuts or what shadow systems are used to deliver this to me.*

*[...] we can never be 100% sure that what they [the MSP] promise is actually done. [...] this is challenging work because we need to have sufficient ordering and control competence.*

#### **4.2.2 Communication issues**

Another challenge of outsourcing that can influence cybersecurity is how it impacts communication. Findings show that how the information flows might be a struggle for companies. Not having the responsibilities in-house can slow down the speed and quality of the feedback to the users and essential information might be lost. As one respondent said:

*You do not get as fast and close follow-up when outsourcing. It might depend on who you are outsourcing to but going from having IT internally to a supplier was a huge downgrade for us.*

As a more common challenge, some respondents said that response time also was worth mentioning. Even though this was introduced as a challenge with day-to-day operations, it can also impact how well the communication is during incidents. Not getting in touch with the correct people in a relatively short time can have big impacts. One respondent compared outsourcing with having people in-house and said:

*But still, we sometimes have to wait in line when calling the MSP. We would not have accepted that if we had people in-house that we could contact.*

### 4.2.3 *Dependency*

Being dependent on the MSP is an aspect that some of the respondents see as a challenge as well. If the company is dependent on the MSP, they become very vulnerable and have to rely on the support that the MSP gives. If a cybersecurity breach happens, their only way of solving the problem is by the help of another company. This issue was pointed out by several respondents who mentioned:

*When we outsource, there is a chance that we get very dependent on the MSP that we outsource to.*

*I can mention that we are vulnerable since we have this outsourcing strategy. And in such a situation [cyber-attack] we would be extra vulnerable if we outsource everything and do not have any competence in-house.*

The last quote also mentions the competence in-house. This point is also raised by other respondents as a challenge with outsourcing. Outsourcing everything can lead to less competence on internal systems, and they become dependent on the MSP to take care of everything. If the responsibility is delegated to someone else, keeping updated on cybersecurity and increasing competence internally might seem less important. One respondent said:

*That might be the case, that our competence on internal systems is not being updated. So that is of course a challenge, that you are dependent on a third party that knows everything about your company.*

### 4.2.4 *Supply chain attacks*

When a company chooses to outsource the IT services, they open themselves up to the risk of supply chain attacks. Many respondents discussed how this could impact their company and some had first-hand experience with this. By letting another company have access to their solutions, an adversary could gain entrance to their systems by hacking the supplier. One respondent said, while talking about how their systems were maintained, that:

*Giving access to external people with very high access privileges to our environment could be a way for others to gain access to us, through them.*

One interviewee described how an attack occurred on their infrastructure and said that due to low segmentation on the supplier’s side, the hackers were able to migrate to their system. Several customers were affected by this attack and the company lost access to everything they had. He said that:

*They [the hackers] went through a port and migrated to other customers. So, there was no segmentation between the customers at [MSP] it may seem.*

### 4.3 Mitigation techniques for security issues

Alongside the different security challenges that have been discovered in this project, the respondents have also mentioned several mitigation techniques that can help. These include control improvement, vendor selection and business continuity. Table 4 shows an overview of what measures can help mitigate the different challenges.

Table 4 Challenges and mitigating measures

Challenges Mitigations	Loss of data control			Communication issues		Dependency		Supply chain attacks
	Data control	Availability	Trust	Information flow	Response time	Dependent on MSP	Loss of internal competence	Supply chain attacks
<b>Control improvement</b>								
Contract	■		■					
SLA	■		■					
Control competence			■		■	■	■	
Testing	■		■					■
<b>Vendor selection</b>								
Local MSP			■	■	■			
Onshore data storage	■	■						
<b>Business continuity</b>								
Segmentation		■						■
Backup		■						■

#### 4.3.1 Control improvement

As mentioned, loss of data control can be a huge challenge and threat to security when outsourcing. However, our findings indicate that there are several techniques to increase the amount of control one has over the MSP and, subsequently, one’s data. One such way is to utilize a contract. Through a contract with the MSP, a company can somewhat control how their data are processed and stored, and ensure that legal regulations are followed, as explained by this respondent:

*When you talk about GDPR, Schrems II and other regulations regarding data storage, where they are and such, [...] we regulate this in a certain way. We do this in the contracts with all our suppliers, where we say it should be within Schrems II.*

It is also a good idea to include an SLA in the contract. This enables companies to ensure that the quality of the services they receive are as promised. This way they can control that the MSP does not shirk away from responsibilities or deliver worse security than what was agreed. Furthermore, this will over time prove if the MSP is trustworthy or not. A respondent told us about how they utilized this to secure the competence and capacity they needed from the supplier:

*We have a thorough and carefully crafted SLA that secures that delivery. Both competence wise and capacity wise. So, they have a clear obligation through the agreement, both on capacity and competence.*

Another finding is that having some competence in-house to be able to control and verify that the delivered services are in compliance with the agreement would help mitigate some issues. Respondents were mostly in accord with each other that it was necessary to have at least some degree of competence in-house to enable them to follow up on agreements. Firstly, this would slowly increase their trust level towards the MSP as they would have the knowledge to check and control that promises were held. Secondly, it would lower the impact resulting from poor response time by allowing companies to start addressing issues before coming in contact with the MSP. Lastly, it was noted that maintaining some competence within the company was necessary to not be completely dependent on the supplier. Some statements from our respondents sounds as follows:

*When you outsource you cannot rely on the supplier to do everything. You need an element of knowledge and ability to ask questions and such.*

*Outsourcing is great, but you need a minimum degree of competence internally also. To follow up, control and check.*

*We have increased from one to two IT resources (employees) internally. We need enough competence to react and follow up on the agreement. Do we get what is promised or not.*

Different forms of testing can also assist companies to gain more control over data and trust towards their MSP. Interview respondents explained how they used penetration tests and red team exercises to evaluate the security of systems provided by the MSP. When doing penetration tests, they would attempt to directly

brute force their way into the systems. Furthermore, when conducting red team exercises, they would perform social engineering against their own employees, try to acquire login credentials and see how far they could migrate through the system. These methods allowed the companies to assess services provided by the MSP and remain confident in their security. Some respondents also mentioned doing audits of the MSP to check processes and routines. Lastly, one respondent was in contact with other actors in the market to check if they delivered what they promised. Some of these points are reflected in the following quotes:

*Another thing we do to check this [level of security] is to run penetration tests. We have done this on a lot of our critical, well, basically all our critical systems and applications and when we do pen testing, it gets both the supplier and the subcontractor who owns the product on the alert. That is our way of telling them that we are aware because we need that sometimes.*

*We are often in contact with actors in the market to check if our suppliers deliver what they promise and in accordance with the SLA.*

#### **4.3.2 Vendor selection**

The interviewed companies also had some thoughts about how they chose their MSP. This choice could, according to our findings, mitigate several challenges that have been mentioned. The issue of trust could be mitigated to some degree by choosing an MSP that is a bit smaller and is a local supplier. This would also affect the response time as you are more likely to have a dedicated contact person that you have met in person. By having this personal connection, it is also expected that the information flow from the MSP to the company is better. One respondent had strong opinions about this subject and said that:

*I think we have a way better service level and personal connection by choosing a local supplier.*

Secondly, companies responded that the data control could be improved by the selection of suppliers. The supplier should be transparent regarding where they store the data and if they have a policy of only using Norwegian or European servers, this could be beneficial regarding availability issues. Having storage only in Europe would ensure that they are protected by European regulations. One answer we received when discussing challenges with GDPR was:



*We have chosen to be very careful in a legal sense and ensured that we have it [data storage] in Norway and know which data centers that are used. We also know that it is the MSP that is responsible for it.*

### **4.3.3 Business continuity**

Supply chain attacks are mentioned as one challenge and companies have different strategies to mitigate this issue. These strategies are beneficial for direct attacks, as well as they are for attacks via MSPs. They are important to ensure business continuity in case of an attack and one thing that was brought up was segmentation of the networks. Limiting what networks the attackers can access if they gain entry through the MSP, would ensure that they are restricted to certain things and some information might still be available to the company. One respondent that had worked quite a bit with ensuring this said that:

*By splitting it [the network], running traffic through firewalls that divides it into different zones and dividing the network into virtual networks and measures like that, we have limited the consequences if they are granted access.*

Another measure that we encountered regarding business continuity was backup strategies. Backing up data can be done in different ways and done correctly it can help mitigate several challenges. By doing regular backups of vital information, a supply chain or direct attack with for example ransomware can result in them getting back to normal much faster. Limiting what information can be corrupted or deleted can also help with the issue of availability. Should incidents occur at the location where the data is stored, it might not be that crucial if local backups are available. Several respondents mentioned this mitigation and said:

*We have done quite a bit regarding backups which ensures that in case of a ransomware attack, we will still have things that are not encrypted. Both offline and online that are protected against such attacks.*

*[...] and the backups are expanded even more and more secure in case of an attack. So, I think that if something should happen, we should be able to get operational reasonably fast.*

Table 5 Summary of findings

Benefits	Quality improvement	Competence	[...] it is their competence, access to updates and what is going on related to security that makes us sleep well at night knowing that we are taken care of. Someone is handling our systems and making sure that we are protected where we need to be.
		Several clients	[...] if you use an external supplier as we do, it is more likely that they [the MSP] are met with more critical questions from customers with diverse competence internally
		Environment	They [IT employees] are dependent on being part of a network to maintain updated on security and other stuff. If you are alone in a company it can get a bit lonely.
	Capacity enhancement		For a company like ours that has few employees and limited turnover there is no possibility to have a team of IT employees to work with it [IT security]. We are too small for that.
Challenges	Supply chain attacks		Giving access to external people with very high access privileges to our environment could be a way for others to gain access to us, through them.
	Communication issues	Response time	But still, we sometimes have to wait in line when calling the MSP. We would not have accepted that if we had people inhouse that we could contact.
		Information flow	You do not get as fast and close follow-up when outsourcing. It might depend on who you are outsourcing to, but going from having IT internally to a supplier was a huge downgrade for us.
	Dependency	Dependant on MSP	When we outsource, there is a chance that we get very dependent on the MSP that we outsource to.
		Loss of internal competence	That might be the case, that our competence on internal systems is not being updated. So that is of course a challenge, that you are dependent on a 3rd party that knows everything about your company
	Loss of data control	Internet connection	The other [challenge] is that we are very vulnerable regarding network problems. If the network fails we have nothing. So that is a big challenge.
		Data control	The bigger and more international the supplier is, the harder it gets to check where the data is actually stored.
		Trust	[...] we can never be 100% sure that what they [the MSP] promise are actually done. [...] this is challenging work because we need to have sufficient ordering and control competence.
Mitigations	Control improvement	Testing	Another thing we do to check this [level of security] is to run penetration tests. We have done this on a lot of our critical, well, basically all our critical systems and applications and when we do pentesting, it gets both the supplier and the subcontractor who owns the product on the alert. That is our way of telling them that we are aware because we need that sometimes.
		SLA	We have a thorough and carefully crafted SLA that secures that delivery. Both competence wise and capacity wise. So they have a clear obligation through the agreement, both on capacity and competence
		Contract	When you talk about GDPR, Schrems II and other regulations regarding data storage, where they are and such, [...] we regulate this in a certain way. We do this in the contracts with all our suppliers, where we say it should be within Schrems II.
		Control competence	Outsourcing is great, but you need a minimum degree of competence internally also. To follow up, control and check
	Business continuity	Backup	We have done quite a bit regarding backups which ensures that in case of a ransomware attack, we will still have things that are not encrypted. Both offline and online that are protected against such attacks.
		Segmentation	By splitting it [the network], running traffic through firewalls that divides it into different zones and dividing the network into virtual networks and measures like that, we have limited the consequences if they are granted access
	Vendor selection	Onshore data storage	We have chosen to be very careful in a legal sense and ensured that we have it [data storage] in Norway and know which data centers that are used. We also know that it is the MSP that is responsible for it.
		Local MSP	I think we have a way better service level and personal connection by choosing a local supplier.

## **5 DISCUSSION**

This chapter provides a discussion regarding the findings provided in chapter four and compares this to what was found in literature, as described in chapter two. Similarities and differences between our findings and the literature are important to discuss to be able to show how our findings address the gaps from previous research. Figure 5, at the end of this discussion, illustrates a clear summary of this comparison. Limitations of the study and their impact on the results are also presented.

The goal of this study was to research how outsourcing IT services in Norwegian SMEs influences their cybersecurity. During this thesis, we have examined different SMEs and their first-hand experience with outsourcing which have given a lot of topics to discuss.

### **5.1 What security benefits are associated with outsourcing IT services?**

Our findings regarding the security benefits of outsourcing for SMEs relates to our first research question. The findings agree with what we found in literature and there are clear similarities in how cybersecurity is influenced. Almutairi & Riddle (2018) mentioned that due to the knowledge and experience available at the MSP the companies will get better solutions. The findings agree with this, and they state that the competence gained from using an MSP increases the quality. As Fenn et al. (2002) concluded, this level of expertise would be hard to obtain in-house. This is directly correlating with our findings where limited resources and environment are mentioned as a basis for this. What we have seen regarding increased quality is also that by having several customers, the MSP can use experience gained from other customers and apply it to others. This is agreeing with what Feng et al. (2020) said would be a benefit for improving security quality. We saw that this also would be affected by the fact that the other customers may ask more “correct” questions regarding solutions and thus improving the overall security the MSPs deliver.

Our findings do not include a lot of new findings compared to the literature regarding benefits of outsourcing, but we saw that the respondents emphasized the benefit of capacity. Even though it is understood that the access to knowledge, and thus better quality, is a benefit of more capacity, respondents also say that the ability to react to several issues at a time is a great benefit. Having the

responsibility in-house would mean that the workforce is smaller, and they would have to prioritize issues.

In addition to our stated findings, we encountered some other benefits that were mentioned by too few respondents to be able to be used as a finding but should still be discussed. One respondent implied that the security awareness would be positively influenced by outsourcing and that the employees would have more focus on cybersecurity if this were outsourced. He thought that the employees would take information from an external entity more serious than if they had their own IT employees. We are not sure if this can be applicable to other companies since this was a small company where internal communication was more informal and maybe this is why information from outside vendors felt more important to them. Another thing brought up is how access to secure systems is a benefit of outsourcing. A couple of respondents discussed how using big outsourcing suppliers would improve their security by delivering well established solutions with integrated security and system integrity. Others may not have highlighted this because it might be expected that improved competence will make systems more secure.

## **5.2 What security challenges are associated with outsourcing IT services?**

Our research has also produced findings regarding the second research question. These are related to potential security challenges with outsourcing. When it comes to the literature, most of our findings are present in previous research. Several authors have argued that outsourcing leads to a loss of confidentiality, integrity, and availability of data as it is being processed and stored by potentially untrustworthy third parties (di Vimercati et al., 2012; Xiao & Xiao, 2012; Kaur & Singh, 2015; Almutairi & Riddle, 2018, Ashraf & Jawad, 2018; Feng et al., 2020). Furthermore, ENISA regards loss of governance as one of the top security risks (Catteddu & Hogben, 2009). Due to the sensitive nature of security, neither the company or the provider can perfectly observe or verify each other's actions, making trust a challenging subject (Rowe, 2007; Chow et al., 2009; Cezar et al., 2013; Lee et al., 2013; Wulf et al., 2019). Additionally, Kaur & Singh (2015) and Wulf et al. (2019) point out that companies may not know exactly where their data is stored, which is a major issue. In terms of availability, the literature states several challenges related to this, including dependency on internet connection. These are all issues that match our findings regarding loss of data control.

Our research also shows that outsourcing might lead to a state of dependency where the company becomes dependent on the MSP and the services it provides. Respondents were particularly concerned that outsourcing would drain their

internal competence and leave them with little cybersecurity knowledge and skills. The literature supports these findings by identifying total security outsourcing as a risk. According to Karyda et al. (2006) and Rowe (2007), total security outsourcing entails a loss of technical security skills internally. Consequently, a technical dependency on the provider may arise as stated by Almutairi & Riddle (2018).

Lastly, there are some similarities regarding the challenge with supply chain attacks. The multi-tenancy nature of MSPs and CSPs has been identified as a risk in the literature. Due to having numerous clients, service providers have access to a lot of systems and data (Khorshed et al., 2012; Green & Green, 2014; CSA, 2019). Hence, if they get breached, the adversaries have a direct path to their customers, making them an ideal target for supply chain attacks. This is consistent with our findings as concerns were expressed over the possibility of being attacked either through the supplier or another client. One respondent had even experienced this themselves and described how they were compromised by an attacker who migrated from another client.

Our research has also found a new challenge which is not represented in the literature. This refers to communication issues. Firstly, our findings indicate that outsourcing negatively influences the information flow regarding cybersecurity. Secondly, they also show that the response time could be impacted. We could not find any mention of this issue in the literature. Therefore, as this was one of our smaller findings, its validity should be questioned. It is entirely possible that the communication problems that our respondents experienced was a niche issue specific to their situation. One could certainly understand that this would be the case if they e.g. outsource to a huge, global provider who must concern themselves with a massive number of clients simultaneously. However, it is difficult to know without further research or supporting literature.

Another thing that differs between our findings and the literature is the issue of legal and regulatory compliance. According to the literature, outsourcing to an MSP located in another country without complete data control is a major issue. In addition, we mentioned earlier that we had a conversation with an MSP before the collection phase took place and they told us that GDPR compliance was the biggest challenge for Norwegian companies that outsource. Therefore, we expected this to show in our findings as well. Surprisingly, it did not. It might have something to do with the fact that they are required to comply with these regulations and do not wish to expose themselves to us. Another explanation could be that they simply lack the knowledge to regard GDPR as an issue at all. In any case, we cannot conclude that legal issues are a challenge of outsourcing for Norwegian SMEs.

Our research resulted in one additional challenge which was not significant enough to be included as a finding. One respondent stated that outsourcing decreased the employees' security awareness. In contrast, another stated that

outsourcing increased the security awareness as mentioned in the previous section. An explanation for this may be that they differed in size. One of them was a small family business with a flat organizational structure and informal culture. The other was much bigger in comparison. Furthermore, it might have been a factor that one of the respondents only had experience with outsourcing while the other had experience with both strategies.

### **5.3 In what ways can SMEs mitigate these challenges?**

During this project, we have seen many different techniques that could help mitigate challenges with outsourcing IT services which relates to our last research question. Our findings include several measures and even though there are some similarities with literature, our findings are more comprehensive. The literature included many sources that mentioned a contract with SLA as a valuable measure to secure quality of the service, avoid double moral hazard and ensure that the provider is living up to their requirements (Goo et. al., 2008; Beaumont, 2006; Tafti, 2005; Wulf et al., 2019; Cezar et al., 2013). Our findings agree with this as they show that an SLA can be used to control the capacity and competence provided by the supplier. They also agree with earlier studies which found that an SLA would increase the company's trust in the MSP (Dickmann et al., 2010). Our findings also emphasize how a contract can make sure that legal regulations are followed and that it enables them to regulate the agreements regarding data storage.

The most significant measure to alleviate issues with outsourcing, according to findings in our study, was having some in-house competence. Having employees with some sort of IT skills could help them control the relationship with the MSP better and avoid being too dependent on them. This is something that we did not encounter in literature as a mitigation technique which we find a bit strange. The literature did describe the importance of security awareness training and that companies needed to have some level of IT security knowledge within the organization, but this was more focused on day-to-day operations (Karyda et al., 2006). There is a significant difference between having general knowledge regarding cybersecurity and privacy risks and having dedicated personnel with in-depth knowledge. Having the latter would enable them to ask critical questions and follow up on the agreements with the MSP and are more highlighted in our findings.

Another finding in our study that is not present in literature is regarding testing. The respondents introduced different ways of testing the security provided by the MSP. By doing penetration tests, red team exercises and conducting audits they felt that they increased the data control and trust in the MSP. We also saw that

choosing the correct vendor could impact the same challenges. Our findings show that smaller and local vendors would be preferable and that this would help with not only these, but several other challenges presented. This might be more specific to our research compared to literature as this study has focused on Norwegian SMEs whereas the literature is composed of international studies. As Norwegian and European companies are forced to follow GDPR with strict rules regarding data storage etc., they might be more focused on where the vendors are localized.

The last finding regarding mitigations that we found is also something that was missing in literature. The interviewed companies stated that having enhanced focus on business continuity would mitigate supply chain attacks and availability issues. By segmenting the network and having good backup routines, they could mitigate the outcome of incidents and secure a faster recovery. The research articles used in this thesis did not tend to include very technical elements of how outsourcing influences cybersecurity, which may be the reason we did not find these measures included. The articles covered a more general picture regarding the thesis topic.

As previously mentioned, security awareness was mentioned in the literature as a form of mitigation. Our study shows insignificant results regarding this, as only two respondents mention this as a measure. They used reminders and examples to make sure that the employees were on high alert regarding security. They both mentioned “sikkerhetsmåneden” which is a yearly event that is supposed to remind everyone on the importance of security. Norwegian companies might be ahead of international companies when it comes to security awareness as these practices appear to be well developed in Norway. Respondents may therefore see this security measure as implied which can be an explanation to why this was not mentioned in more interviews. Furthermore, our study hints at some measures that can improve the communication between companies and MSPs. One respondent thought it was a huge benefit to have a local contact person inside the MSP who the company could have direct contact with. This way, they avoided having to fill out a standardized form if something urgent came up and could instead contact this person directly to quickly resolve the problem. Another respondent also noted that direct contact with any potential subcontractor would help greatly.

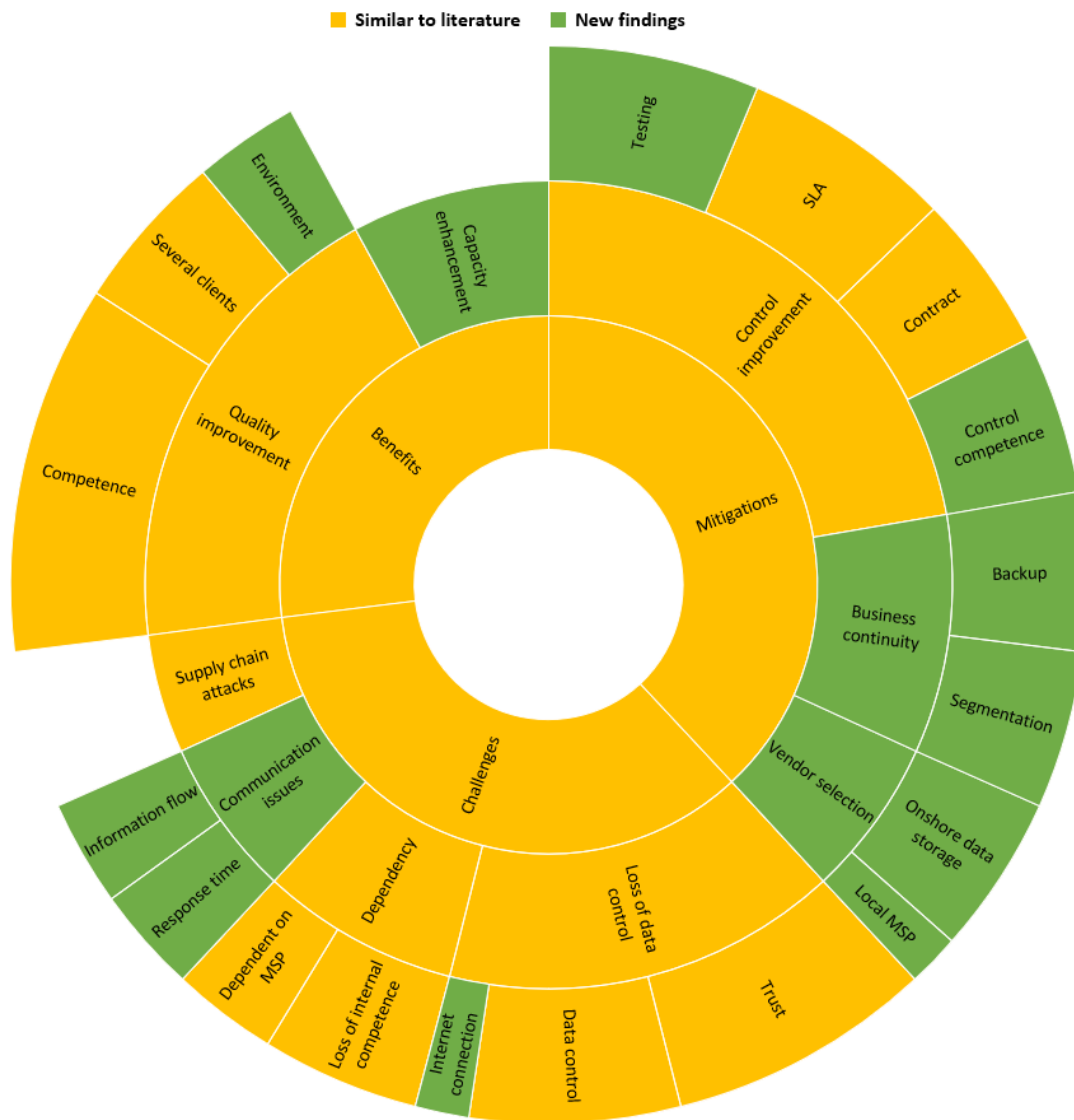


Figure 5 Literature and findings comparison

## 5.4 Limitations

The findings of this study must be seen in light of some limitations. The first limitation that should be mentioned is regarding the sampling method. Purposive sampling was used, and this might make the findings prone to researcher bias as we use our own personal judgment to select participants. However, developing specific criteria for who to include enabled us to limit this. Related to the respondents, it should also be mentioned that most of the companies that were interviewed in this study were from Kristiansand due to the sampling method used to find the interview subjects. We contacted 85 companies in total and tried to include several areas of Norway, but the majority of the respondents were local.



This may harm the ability to apply the results to all Norwegian SMEs as most of them are from a certain area within Norway.

The second limitation is regarding the sample size. As this is a qualitative study, the goal is to thoroughly investigate and truly understand our topic. While the number of conducted interviews were deemed to be sufficient, one could argue that ten interviews are too few and that more findings would possibly be discovered with more interviews.

Limited access to data is the third limitation which should be discussed. This is an issue for two distinct reasons. Firstly, due to the sensitive nature of our topic, respondents might be reluctant to answer every question completely. This also affected the sample size of the thesis. Many companies that were contacted declined the request for an interview due the topic in question. Secondly, access to data was limited due to the knowledge of the interviewees, or rather the lack thereof. Some of them had limited knowledge regarding IT security and describing how outsourcing influenced the cybersecurity thus proved difficult. Even though they were responsible for IT and the outsourcing relationship, not all had the necessary experience. This was why they chose to outsource the responsibilities in the first place.

The last limitation is related to time constraints. As we are students conducting the research, there is a relatively short deadline before delivery. This influences how possible it is to conduct as many interviews as we might want. With more time, a more thorough study could be conducted, and the findings would have even more credibility.

## 6 CONCLUSION

In this thesis, we have explored the phenomena of outsourcing IT services and have expanded our knowledge on how this influences the cybersecurity in Norwegian SMEs. By conducting qualitative research with respondents from Norwegian SMEs that outsource their IT services, we have compared this to existing literature on the topic and found new aspects that should be considered when outsourcing. Previous literature has to some degree examined this and some things are more discussed than others. There are benefits and challenges with outsourcing that have been identified by several researchers prior to our study, but as mentioned in the gaps in literature, it lacked some mitigation measures and a focus on Norwegian SMEs. Therefore, we asked ourselves “How does outsourcing IT services influence the cybersecurity in Norwegian SMEs?” in hopes of finding additional benefits and challenges and addressing the gaps in literature regarding mitigation measures.

Our study found that access to competence is the biggest benefit and that the companies that outsource get better quality of their security. The capacity in terms of manpower that the MSPs can bring was also an important benefit. The main challenges identified are loss of data control, communication issues, dependency, and supply chain attacks. Loss of data control poses a challenge in terms of trust towards the MSP and confidentiality, integrity, and availability of data. Communication issues negatively influence *how* the companies get information and *when*. The study also shows that companies can end up being dependent on their MSP as a result of a loss of internal competence. Supply chain attacks are a challenge as well due to the multi-tenancy nature of MSPs. Our research shows that these challenges can be present in different ways and severity. To deal with them, several measures that could be applied to mitigate their likelihood or outcome have been identified. The main finding here is that companies should have some control competence in-house when outsourcing. Having some expertise within the company would enable them to check up on agreements and make them less dependent on the MSP for security related issues. Other mitigation techniques identified in this study include writing a clear contract with an SLA and testing the supplier and their services to ensure that they are secure. Lastly, segmentation and backups should be considered to enhance business continuity.

For further research, a more comprehensive study including more respondents should be conducted. This thesis provides a good overview of how SMEs are influenced and brings up many different aspects that could be further investigated

in a more thorough study. By using our findings in a large-scale quantitative study, more data could be gathered about how our findings relate to other Norwegian companies and which ones are more common. Some research comparing SMEs to larger companies would also be interesting to see what benefits and challenges are universal regardless of size. In addition, outsourcing of IT services might be influenced by national and organizational cultures and this can be other avenues for future research. Lastly, we believe more research on Norwegian companies in general should be conducted as there is little representation of Norwegian sources in the literature.

## REFERENCES

- Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012). Perceived IT security risks of cloud computing: Conceptualization and scale development. *Thirty Third International Conference on Information Systems*. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.7295&rep=rep1&type=pdf>
- Almutairi, M., & Riddle, S. (2018). State of the art of IT outsourcing and future needs for managing its security risks. *2018 International Conference on Information Management and Processing (ICIMP)*, 42-48. IEEE. <https://doi.org/10.1109/ICIMP1.2018.8325839>
- Ashraf, A., & Jawad, M. (2018). Cloud Computing: Major Challenges and Counter Acts. *International Journal of Advanced Research in Computer Science*, 9(2), 618-625. <https://doi.org/10.26483/ijarcs.v9i2.5861>
- Amedia. (2021, Desember 29). Dataangrepet: Det vil ta tid før situasjonen er normal. Retrieved 04.03.22 from: <https://www.amedia.no/aktuelt/nyheter/item/dataangrepet-det-vil-ta-tid-for-situasjonen-er-normal>
- Bachlechner, D., Thalmann, S., & Maier, R. (2014). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. *Computers & Security*, 40, 38-59. <https://doi.org/10.1016/j.cose.2013.11.002>
- Beaumont, N. (2006). Service level agreements: An essential aspect of outsourcing. *The Service Industries Journal*, 26(4), 381-395. <https://doi.org/10.1080/02642060600621563>
- Bisson, D. (2021, May 20). *The State of Small Business Cybersecurity in 2021*. Security Intelligence. Retrieved 20.01.22 from: <https://securityintelligence.com/articles/state-small-business-cybersecurity-2021/>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
- BullGuard. (2020, February 19). *New Study Reveals One In Three SMBs Use Free Consumer Cybersecurity And One In Five Use No Endpoint Security At All*. BullGuard. Retrieved 21.02.22 from: <https://www.bullguard.com/press/press-releases/2020/new-study-reveals-one-in-three-smbs-use-free-consu.aspx>
- Catteddu, D., & Hogben, G. (2009). *Cloud Computing: Benefits, risks and recommendations for information security*. Retrieved from: <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>
- Cezar, A., Cavusoglu, H., & Raghunathan, S. (2013). Outsourcing information security: Contracting issues and security implications. *Management Science*, 60(3), 638-657. <https://doi.org/10.1287/mnsc.2013.1763>

- Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. *Proceedings of the 2009 ACM workshop on Cloud computing security*, 85-90. <https://doi.org/10.1145/1655008.1655020>
- CSA. (2019). *Top Threats to Cloud Computing: Egregious Eleven*. Retrieved from: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven>
- Dickmann, F., Brodhun, M., Falkner, J., Knoch, T. A., & Sax, U. (2010). Technology transfer of dynamic IT outsourcing requires security measures in SLAs. *International Workshop on Grid Economics and Business Models*. 1-15. [https://doi.org/10.1007/978-3-642-15681-6\\_1](https://doi.org/10.1007/978-3-642-15681-6_1)
- Dodds, S. (2021). When is the right time to outsource your security function?. *Network Security*, 2021(5), 16-19. [https://doi.org/10.1016/S1353-4858\(21\)00054-4](https://doi.org/10.1016/S1353-4858(21)00054-4)
- European Commission. (n.d.). *SME definition*. European Commission. Retrieved 31.01.2022 from: [https://ec.europa.eu/growth/smes/sme-definition\\_en](https://ec.europa.eu/growth/smes/sme-definition_en)
- Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA)*. Retrieved from: [https://www.europol.europa.eu/sites/default/files/documents/internet\\_organised\\_crime\\_threat\\_assessment\\_iocta\\_2020.pdf](https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf)
- FBI. (2021). *Internet Crime Report 2021*. Retrieved from: [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)
- Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2020). To outsource or not: The impact of information leakage risk on information security strategy. *Information & Management*, 57(5). <https://doi.org/10.1016/j.im.2019.103215>
- Fenn, C., Shooter, R., & Allan, K. (2002). IT security outsourcing: how safe is your IT security?. *Computer Law & Security Review*, 18(2), 109-111. [https://doi.org/10.1016/S0267-3649\(02\)03009-1](https://doi.org/10.1016/S0267-3649(02)03009-1)
- Fleutiaux, F. (2017, November 10). *Cloudsourcing is the new outsourcing*. LinkedIn. Retrieved 14.02.22 from: <https://www.linkedin.com/pulse/cloudsourcing-new-outsourcing-fran%C3%A7ois-fleutiaux/>
- Gartner. (n.d.A). *Small And Midsize Business (SMB)*. Gartner. Retrieved 14.02.22 from: <https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses>
- Gartner. (n.d.B). *Managed Service Provider (MSP)*. Gartner. Retrieved 14.02.22 from: <https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider>
- GDPR. (n.d.). *GDPR data controllers and data processors*. GDPR. Retrieved 25.02.2022 from <https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/>
- Goo, J., Huang, C.D., & Hart, P. (2008). A path to successful IT outsourcing: interaction between service-level agreements and commitment. *Decision Sciences*, 39(3), 469-506. <https://doi.org/10.1111/j.1540-5915.2008.00200.x>
- Green, K.B., & Green, B.P. (2014). Reining in the risks of cloud computing. *Internal Auditing*, 29(5), 29-35. <https://www.proquest.com/trade-journals/reining-risks-cloud-computing/docview/1626831802/se-2?accountid=45259>
- Hendy, J. (2021, May 19). *Why Cybersecurity Outsourcing Continues to Grow*. Future of Sourcing. Retrieved 17.02.22 from: <https://futureofsourcing.com/why-cybersecurity-outsourcing-continues-to-grow>

- Interpol. (2020). *Cybercrime: Covid-19 impact*. Retrieved from: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
- Kampenes, I. (2021, October 27). [Conference presentation]. Sikkerhetsdagen 2021. Grimstad, Norway.
- Karyda, M., Mitrou, E. & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, 14(5), 403-416. <https://doi.org/10.1108/09685220610707421>
- Kaur, M., & Singh, H. (2015). A review of cloud computing security issues. *International Journal of Grid Distribution Computing*, 8(5), 215-222. <http://doi.org/10.14257/ijgdc.2015.8.5.21>
- Khan, A.U., Oriol, M., Kiran, M., Jiang, M., & Djemame, K. (2012). Security risks and their management in cloud computing. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 121-128. IEEE. <https://doi.org/10.1109/CloudCom.2012.6427574>
- Khalil, S.M., Khreishah, A. & Azeem, M. (2014). Cloud Computing Security: A Survey. *Computers*, 3(1), 1-35. <https://doi.org/10.3390/computers3010001>
- Khorshed, M.T., Shawcat Ali, A.B.M. & Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, 28 (6), 833-851. <https://doi.org/10.1016/j.future.2012.01.006>
- Knapp, K. (2018, May). *Cloud sourcing*. Techtarget. Retrieved 19.02.22 from: <https://www.techtarget.com/searchcloudcomputing/definition/cloud-sourcing>
- Kumar, M., Meena, J., Singh, R. & Vardhan, M. (2015). Data outsourcing: A threat to confidentiality, integrity, and availability. *International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1496-1501. IEEE. <https://doi.org/10.1109/ICGCIoT.2015.7380703>
- Lee, C.H., Geng, X. & Raghunathan, S. (2013). Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research*, 24(2), 295-311. <https://doi.org/10.1287/isre.1120.0447>
- Mfinanga, F.A., Mrosso, R.M. & Bishibura, S. (2019). Comparing Case Study and Grounded Theory as Qualitative Research Approaches. *International Journal of Latest Research in Humanities and Social Science*, 2(5), 51-56. <http://www.ijlrhss.com/paper/volume-2-issue-5/5-HSS-366.pdf>
- Miles, M.B., Huberman, A. M. & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd edition). SAGE Publications, Inc.
- Morgan, S. (2020, November 13). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. Cybercrime Magazine. Retrieved 17.01.22 from: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Myers, M.D. (2022, March 2). *Qualitative Research in Information Systems*. Association for Information Systems (AISWorld). Section on Qualitative Research in Information Systems. Retrieved 18.03.22 from: [www.qual.auckland.ac.nz](http://www.qual.auckland.ac.nz)
- Nero, R.L. (2018). *Risks, benefits, and perceived effectiveness of outsourcing it network security in small businesses: A multiple-case study*. [Ph.D. thesis]. Capella University.

- NHO. (n.d.). *Fakta om små og mellomstore bedrifter (SMB)*. NHO. Retrieved 14.02.22 from: <https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/>
- NorSIS. (2021). *Trusler og Trender 2021*. Retrieved from: [https://norsis.no/wp-content/uploads/2021/03/NorSIS\\_Trusler\\_Trender\\_2021\\_Digital.pdf](https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf)
- Nortura. (2021, December 21). *Nortura er utsatt for et dataangrep*. Nortura. Retrieved 04.03.22 from: <https://www.nortura.no/nyheter/nortura-er-utsatt-for-et-dataangrep>
- NSD. (n.d.). *About NSD - Norwegian Centre for Research Data*. NSD. Retrieved 16.03.22 from <https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/>
- Okoli, C. & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, 10(26). <https://asset-pdf.scinapse.io/prod/1539987097/1539987097.pdf>
- Overby, S. (2017, November 6). *What is outsourcing? Definitions, best practices, challenges and advice*. CIO. Retrieved 14.02.22 from: <https://www.cio.com/article/2439495/outsourcing-outsourcing-definition-and-solutions.html>
- Pang, M.S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of US federal government. *The Journal of Strategic Information Systems*, 31(1). <https://doi.org/10.1016/j.jsis.2022.101707>
- Peričić, T.P. & Tanveer, S. (2019, July 23). *Why systematic reviews matter. A brief history, overview and practical guide for authors*. Elsevier. Retrieved 15.02.22 from: <https://www.elsevier.com/connect/authors-update/why-systematic-reviews-matter>
- Ponemon Institute. (2019). *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*. Retrieved from: [https://www.keeper.io/hubfs/2019%20Keeper%20Report\\_Final%20\(1\).pdf](https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf)
- Regjeringen. (2021, November 12). *Norge fortsatt blant de ledende landene i Europa på digitalisering*. Regjeringen. Retrieved 03.05.22 from: <https://www.regjeringen.no/no/aktuelt/norge-fortsatt-blant-de-ledende-landene-i-europa-pa-digitalisering/id2886756/>
- Renaud, K., & Weir, G.R. (2016). Cybersecurity and the Unbearability of Uncertainty. *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 137-143. IEEE. <http://doi.org/10.1109/CCC.2016.29>
- Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM conference on Computer and communications security*, 199-212. <https://doi.org/10.1145/1653662.1653687>
- Rowe, B.R. (2007). *Will outsourcing IT security lead to a higher social level of security?*. [Master thesis, North Carolina State University]. NC State University Libraries. <https://repository.lib.ncsu.edu/handle/1840.16/441>
- Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse researcher*, 25(4), 41-49. <https://doi.org/10.7748/nr.2018.e1466>
- Sarangam, A. (2021, February 20). *Cloud Sourcing: A Complete Guide in 6 Points*. Jigsaw Academy. Retrieved 14.02.22 from: <https://www.jigsawacademy.com/blogs/cloud-computing/cloud-sourcing>

- Syntax. (2021). *2021 IT trends: A Year of New Industry Benchmarks*. Syntax. Retrieved from: <https://info.syntax.com/ebooks/3/syntax-it-trends-benchmark-report-2021>
- Tafti, M.H.A. (2005). Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, 105(5), 549-560.  
<https://doi.org/10.1108/02635570510599940>
- Trellix. (2022, January 19). *Trellix 2022 Threat Predictions*. Trellix. Retrieved 09.02.22 from <https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/2022-threat-predictions.html>
- Verizon. (2021). *2021 Data Breach Investigations Report (DBIR)*. Retrieved from: <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>
- di Vimercati, S.D.C., Foresti, S., & Samarati, P. (2012). Managing and accessing data in the cloud: Privacy risks and approaches. *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 1-9. IEEE. <https://doi.org/10.1109/CRiSIS.2012.6378956>
- Wu, L., & Buyya, R. (2012). Service level agreement (SLA) in utility computing systems. *Performance and dependability in service computing: Concepts, techniques and research directions*, 1-25. IGI Global.  
<http://doi.org/10.4018/978-1-60960-794-4.ch001>
- Wulf, F., Strahringer, S., & Westner, M. (2019, July). Information security risks, benefits, and mitigation measures in cloud sourcing. *2019 IEEE 21st Conference on Business Informatics (CBI)*, 258-267. IEEE.  
<https://doi.org/10.1109/CBI.2019.00036>
- Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, 15(2), 843-859.  
<http://doi.org/10.1109/SURV.2012.060912.00182>



# APPENDIX

## Appendix A - Email

Forespørsel om intervju

Hei,

Mitt navn er Jarle Nordby Johnsen og sammen med Christian Kittilsen studerer jeg Cybersikkerhet - Sikkerhetsledelse ved Universitet i Agder. Vi skriver nå en masteroppgave om hvordan outsourcing av IT tjenester påvirker IT sikkerheten i norske bedrifter. Vi ønsker å se på hvilke faktorer som blir påvirket av det å la andre ta hånd om IT tjenestene og om dette har noe å si for cybersikkerheten.

Vi er på jakt etter bedrifter som enten outsourcer eller har outsourcet IT tjenester tidligere og som kan delta i et intervju. Vi ønsker henholdsvis å intervju den eller de som har oversikt over IT løsningene i bedriften.

Oppgaven er utarbeidet med vår masterveileder Devinder Thapa fra UIA. Informasjon om lagring av data som blir samlet inn, retningslinjer og samtykkeskjema vil bli tilsendt dere i eget dokument på forhånd.

Intervjuet er et semistrukturert intervju, der du blir bedt om å svare på forberedte spørsmål, men oppfølgingsspørsmål kan forekomme. Intervjuet vil ta inntil 45 minutter å gjennomføre og vi ønsker å høre litt om hvordan outsourcing av IT har påvirket deres bedrift.

Hvis du av en eller annen grunn ikke vil svare på spørsmålene som blir presentert, og/eller vil trekke deg ut av forskningsprosjektet, kan du gjøre dette til enhver tid.

Ved godkjenning ønsker vi å ta opp intervjuet i form av lyd for transkribering. Både bedrifter og personer som deltar vil bli anonymisert og vi vil kun registrere bransje dere opererer i.

Ta gjerne kontakt om du har noen spørsmål angående prosjektet og vi håper på et positivt svar.

Mvh

Jarle N Johnsen, Tlf 40444445  
og Christian Kittilsen, Tlf 99359424

## Appendix B - Interview guide

**Bransje:**

**Dato:**

**Varighet:**

### **Generelt**

Q1. Hva er din stilling i selskapet?

Q2. Hvor mange ansatte er det i selskapet?

Q3. Hvordan håndteres IT biten i deres selskap? Både generell IT og sikkerhet?

Q4. Outsourcer dere onshore eller offshore? Altså, lokalt eller globalt eller til Cloud providers?

Q5. Hvor lenge har dere outsourcet?

### **RQ1**

Q6. Hvorfor har dere valgt å outsource? / Hvilke faktorer gjorde at dere valgte å outsource IT?

Q7. Ser du noen andre positive sider med outsourcing?

Q8. Hvordan har outsourcing påvirket IT sikkerheten i selskapet? Både teknisk og sikkerhetsforståelse.

### **RQ2**

Q9. Ser du noen utfordringer med outsourcing i deres bedrift?

Q10. Er det noen andre negative sider ved å outsource du vet om?

Q11. Får dere den hjelpen dere trenger når dere trenger den?

Q12. Tror du det er noen forskjell på å outsource lokalt eller globalt?

### **RQ3**

Q13. Har dere gjort noen tiltak for å mitigere disse utfordringene?

Q14. Kan du se for deg noen andre tiltak som eventuelt kunne mitigere nåværende utfordringer?

Q15. Har dere tidligere hatt utfordringer som er fjernet ved å gjøre tiltak?

### **Avslutningsvis**

Q16. Er det noe mer du vil legge til før vi avslutter?

## Appendix C - NVivo

Outsourcing.nvp - NVivo 12 Pro
?

**Quick Access**

- Files
- Memos
- Nodes
- Data
- Files
- Interview transcript
- File Classifications
- Externals
- Codes
- Nodes
- Relationships
- Relationship Types
- Cases
- Notes
- Search
- Maps
- Output

**Explore**

Query Visualize

Code Auto Range Code Code Coding

Undo

Classification

File Classification

Detail View Sort By

Navigation View

Find

Workspace

**Nodes**

Name	Files	References	Created On	Created By	Modified On	Modified By
Challenges		9	30 09/03/2022 14:26	JUN	03/05/2022 11:23	CK
Loss of data control		8	18 25/04/2022 12:59	CK	02/05/2022 14:13	CK
Supply chain attacks		3	3 21/03/2022 11:33	JUN	06/05/2022 11:47	CK
Communication issues		3	4 25/04/2022 11:46	CK	02/05/2022 18:53	CK
Dependency		3	4 25/04/2022 12:20	CK	25/04/2022 12:53	CK
Decreased security awareness		1	1 20/04/2022 12:16	CK	06/05/2022 11:53	CK
Benefits		8	26 09/03/2022 14:25	JUN	03/05/2022 11:03	CK
Quality improvement		8	18 02/05/2022 14:36	CK	16/05/2022 10:12	CK
Capacity enhancement		5	6 21/03/2022 10:57	JUN	16/05/2022 10:12	CK
Access to secure solutions		2	3 25/04/2022 11:13	CK	06/05/2022 11:54	CK
Increased security awareness		1	1 05/04/2022 12:55	CK	06/05/2022 11:55	CK
Mitigations		7	36 09/03/2022 14:26	JUN	06/05/2022 12:59	CK
Control improvement		4	20 25/04/2022 13:13	CK	06/05/2022 11:56	CK
Vendor selection		4	5 25/04/2022 13:50	CK	05/05/2022 13:19	CK
Business continuity		3	9 25/04/2022 14:05	CK	25/04/2022 14:05	CK
Security awareness training		2	3 21/03/2022 13:47	CK	06/05/2022 12:59	CK
Effective communication		2	2 25/04/2022 14:15	CK	16/05/2022 10:23	CK

CK
39 Items

## Appendix D - Consent form

# Forespørsel om å delta i forskningsprosjekt

## Hvordan outsourcing påvirker IT sikkerheten i norske SMBer

Denne informasjonen er tiltenkt personer og bedrifter som det er ønskelig at skal delta i et forskningsprosjekt om hvordan outsourcing av IT tjenester påvirker IT sikkerheten. Dette skrevet inneholder informasjon om målene med prosjektet og hva en eventuell deltakelse vil innebære.

### Formål

Vi er to studenter som studerer Cybersikkerhet - Sikkerhetsledelse ved Universitet i Agder. Vi skriver nå en masteroppgave om hvilke påvirkninger og utfordringer små og mellomstore bedrifter kan ha eller får ved å outsource IT til andre.

### Hvem er ansvarlig for forskningsprosjektet?

Oppgaven er skrevet av Jarle Nordby Johnsen og Christian Kittilsen i samarbeid med veileder Devinder Thapa fra UIA.

### Hvorfor får du spørsmål om å delta?

Vi har behov for data innsamlet via intervju fra 10-15 forskjellige SMBer i varierte bransjer. Det er ønskelig med intervju av daglige ledere, CEO, CISO, CTO, IT ansvarlige eller lignende. Hovedmålet er at personene har oversikt over hvordan IT håndteres i bedriften.

### Hva innebærer det for deg å delta?

Som deltaker i denne undersøkelsen vil du delta på et intervju som vil vare ca 30 minutter. Dette kan gjennomføres enten fysisk eller via Teams/Zoom e.l. Spørsmålene som stilles er laget på forhånd, men oppfølgingsspørsmål basert på dine svar kan forekomme. I intervjuene kommer det (ved godkjenning) til å bli brukt diktafon. Dataene innhentet vil bli analysert, anonymisert og brukt i masteroppgaven. Alle rådata fra diktafon vil bli slettet.

### Frivillig deltagelse

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Data om deltakere i undersøkelsen er ikke relevant og det er ingen intensjon om å skulle kunne identifisere disse. All innsamling og behandling av data vil være i tråd med retningslinjene fra UIA og Norsk Senter for ForskningsData (NSD).

### Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket..

- Data som blir behandlet i denne studien vil kun være tilgjengelig for oss som studenter og vår veileder Devinder Thapa. I tillegg eventuelle digitale kommunikasjonsprogram som f.eks. Zoom eller Teams. .
- Videre er det også iverksatt tiltak for å sikre at ikke uvedkommende får tilgang til data under og etter intervjuene:
- Møtelenke vil ikke deles åpent.
- Møtet vil være passordbeskyttet.
- Det vil bli benyttet lobby/venterom for å slippe inn riktige personer i møtet.
- Under behandlingen vil dataene bli lagret på et SD-kort på en diktafon fra det intervjuet. Etter transkribering vil all rådata bli slettet fra SD-kort.
- Navn på bedrift og intervjuobjekt vil bli erstattet med en kode.

### **Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 4 Juni 2022. Rådata blir slettet underveis i prosjektet og all informasjon som ligger i masteroppgaven vil være anonymisert.

### **Hva gir oss rett til å behandle personopplysninger om deg?**

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitet i Agder har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

### **Dine rettigheter**

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Masterstudent Jarle Nordby Johnsen ved Universitetet i Agder, kan kontaktes på e-post [jarlej13@uia.no](mailto:jarlej13@uia.no) eller tlf +47 404 44 445.
- Masterstudent Christian Kittilsen ved Universitetet i Agder, kan kontaktes på e-post [chrik16@uia.no](mailto:chrik16@uia.no) eller tlf +47 993 59 424
- Professor Devinder Thapa ved Universitet i Agder, kan kontaktes på e-post [devinder.thapa@uia.no](mailto:devinder.thapa@uia.no) eller på tlf +47 952 56 430
- Vårt personvernombud Johanne Warberg Lavold ved Universitet i Agder, kan kontaktes på e-post [personvernombud@uia.no](mailto:personvernombud@uia.no)

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på e-post [personverntjenester@sikt.no](mailto:personverntjenester@sikt.no) eller på tlf 53 21 15 00

Med vennlig hilsen

Jarle Nordby Johnsen & Christian Kittilsen,  
Masterstudenter

---

-----

## Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i et intervju.

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

-----

(Signert av prosjektdeltaker, dato)