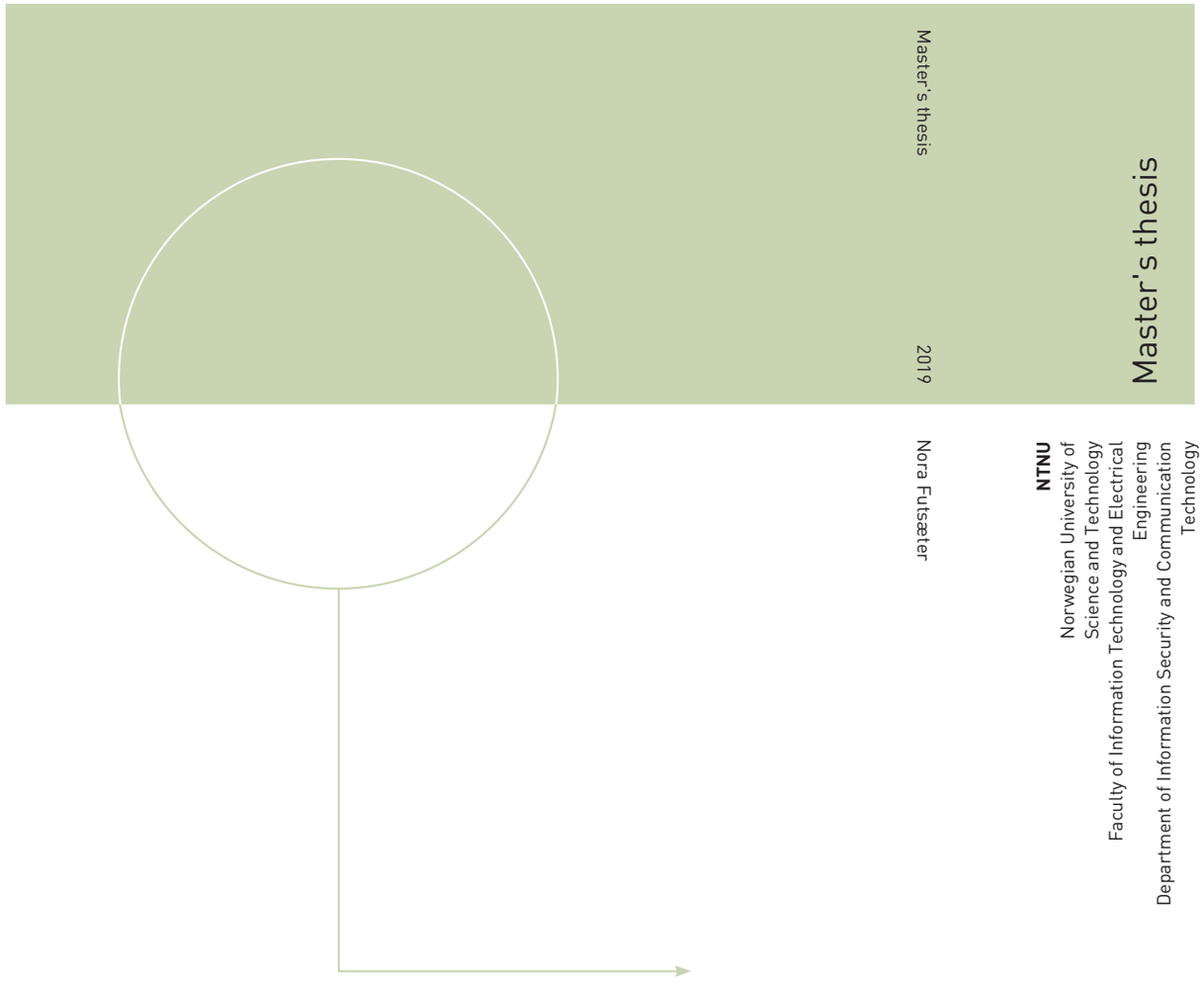

Master's thesis

2019

Nora Futsæter

**NTNU**
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

Nora Futsæter

# Best practices and motivational factors for information security in startups

## An exploratory case study of four Norwegian tech startups

June 2019

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of
Science and Technology

# Best practices and motivational factors for information security in startups

An exploratory case study of four Norwegian tech startups

Nora Futsæter

Communication Technology
Submission date: June 2019
Supervisor: Erlend Andreas Gjære
Co-supervisor: Karin Bernsmed

Norwegian University of Science and Technology
Department of Information Security and Communication
Technology

**Title:** Best practices and motivational factors for security in startups

**Student:** Nora Futsæter

**Assignment given:**

Startups are important for society, both for creating new workplaces and representing a driver for innovation and entrepreneurship. New technology possibilities, new ways for entrepreneurial financing, inspiration from new companies such as Airbnb, Instagram, Snapchat and Uber, in addition to a media coverage of startups might all be signs of a focus on startups in the society. The Government in Norway has also addressed the need for startups in order to create workplaces and granted both funding for startups and funding for research of startups. In addition, investments in Norwegian startups are larger than ever.

At the same time, there is an increasing trend that small businesses businesses are victims to cybercrime activities. Small businesses and startups may be considered low-hanging fruits. In January 2019, the Norwegian Government launched a new national strategy for cyber security, emphasising that cyber security is everyone's concern. However, little research on how startups work with security has been performed. While security benefits from stability and risk reduction, innovation is often defined by fast iterations and high risk appetite. Although startups depend on both, there are scenarios where security may receive less attention than in more established enterprises.

Previous studies have focused more on technical testing of security measures in startups, how agile and security fit together and identifying influencing factors for companies in general to implement security. However, there is limited knowledge on how startups actually work with product security and security awareness, and how their work could be improved. Specifically, little is known about factors that motivate the startups to implement security measures and how is this expressed through their work.

The overall aim is therefore to develop a basis for improved security in startups, by identifying factors that contributes to relevant security measures. To achieve this, the following three main tasks will be addressed:

- Review some relevant existing frameworks and guides relevant for Norwegian startups, in order to develop an applicable guide for interviewing startups regarding security.
- Perform semi-structured interviews with 3-5 Norwegian startups applying this guide, with the goal to identify factors that motivate them to implement security

measures and how is this expressed through their work.

– Suggest a prototype with the aim to help startups improve future best practices regarding security.

| | |
|---|---|
| **Responsible professor:** | Karin Bernsmed, IIK |
| **Supervisor:** | Erlend Andreas Gjære, Secure Practice |

# Abstract

The technology industry is undergoing a revolution. New technology leads to an increase in innovation and establishment of startups. However, new technology are accompanied by new threats. For instance, Norwegian companies, organizations and public sectors are increasingly victims of advanced information security attacks, with major economic consequences. The Norwegian government has an increasing general focus on information security by e.g. launching a National Cyber Security Strategy.

The last couple of years there has been focus on startups in Norway. Startups, which are *temporary organization designed to search for a repeatable and scalable business model*, and by some defined as *a state of mind*, have received increasing public and end user attention, resulting in increased investments. However, startups may be characterized by little resources and an ad-hoc working process with the goal of getting the product to the market fast, which make them particularly vulnerable.

Previous research has focused on security frameworks, security in agile development process, investigated how SMEs work with information security and one study has taken a technical approach to test some startups against known vulnerabilities. However, little research has specifically addressed information security issues in startups. In particular, there is no systematic information about how different Norwegian startups work with security on an overall and specific level; e.g. what they actually do to reduce their vulnerability to e.g. cyberattacks. Although research has indicated that motivational factors are important when working with security in organizations in general, little is known about motivations in startups to work with information security.

This exploratory case study is the first to investigate different aspects of information security in Norwegian startups, taking both technical, organizational and motivational aspects into account. First, a review of some potential relevant frameworks and guides was performed. Important topics identified by the review of existing guides and frameworks regarding information security helped to form the hypotheses. The main topics were categorized and aided the work to develop an applicable interview guide. These hypotheses were then tested by semi-structured interviews of four Norwegian startups, in order to identify elements of their security activities and their motivation to perform these.

The review of existing potential relevant materials for guides and frameworks related to information security identified existing materials which had elements of relevance for security in startups. However, the entire guides were not covering all topics reported as important by the startups. Much of their practical day to day work covered some of the important aspects mentioned in the guidelines or frameworks. The interviews identified that the startups typically had established some elements of systematics for security management, and made sure that a person (internal in the management or external expert) supported the management in security issues. Training and awareness around information security was of importance, but the startups varied in how the training of employees was conducted. Interestingly, while media focus on the cyberattacks and economic consequences, this study found that external factors (e.g. GDPR fines, reputational damage and customers trust), as well as internal motivational factors (e.g. entrepreneurial spirit, a belief in the product they are making) play important roles for how startups are working with security.

In conclusion, in light of the ad-hoc process and lack of resources typically seen in startups, the results here indicate that there is a need for specific guidelines designed for startups tailormade for their way of working. Furthermore, the creation of platforms and a sharing culture between startups for security issues can be suggested. Importantly, the employees' motivational factors need to be taken into account when developing these new guidelines and sharing platforms, with the ultimate goal to reduce vulnerability related to security issues in existing and future startups.

# Sammendrag

Teknologibransjen gjennomgår en revolusjon. Med innovasjon og ny teknologi kommer også stadig nye trusler. For eksempel er norske bedrifter, organisasjoner og offentlige sektorer i stadig større grad ofre for avanserte digitale angrep, med derav følgende store økonomiske konsekvenser. Den norske regjeringen har også et økende fokus på digital sikkerhet og lanserte f.eks. i januar 2019 en Nasjonal strategi for digital sikkerhet.

De siste årene har det vært fokus på oppstartbedrifter i Norge, såkalte «startups». Disse kan defineres som en midlertidig organisasjon laget for å finne ut og skape en repeterbar og skalerbar forretningsmodell, og defineres av noen som en «mental tilstand». Oppstartbedriftene har fått økende oppmerksomhet fra både offentlig og privat næring samt sluttbrukere, noe som har resultert i økte investeringer. Slike bedrifter kan imidlertid preges av få ressurser og en spontan og løst definert arbeidsprosess hvor hovedfokuset er å få produktet til markedet raskt, noe som kan gjøre dem spesielt sårbare.

Tidligere forskning har fokusert på sikkerhetsrammeverk, sikkerhet i agile utviklingsprosess, undersøkt hvordan små og mellomstore bedrifter arbeider med informasjonssikkerhet og en studie har tatt en teknisk tilnærming til å teste noen oppstartbedrifter mot kjente sårbarheter. Imidlertid har det vært lite forskning om hvordan oppstartbedrifter jobber med informasjonssikkerhet. Spesielt er det ingen systematisk informasjon om hvordan forskjellige norske oppstartbedrifter jobber med sikkerhet på både et generelt og spesifikt nivå; f.eks. hva de egentlig gjør for å redusere sin risiko mot f.eks. dataangrep eller datalekkasjer. Forskning har også indikert at motivasjonsfaktorer er viktige når man arbeider med sikkerhet i organisasjoner generelt, men lite er kjent om ulike motivasjonsfaktorer er involvert i oppstartbedriftenes arbeid med informasjonssikkerhet.

Denne utprøvende casestudien er den første som undersøker ulike aspekter av informasjonssikkerhet i norske oppstartbedrifter, og tar hensyn til både tekniske, organisatoriske og motivasjonsfaktorer. Først ble det gjennomført en gjennomgang av noen potensielle relevante rammeverk og veiledere for informasjonssikkerhet. Temaer som ble identifisert av denne gjennomgangen ble kategorisert og dannet grunnlag for hypotesegenerering knyttet til informasjonssikkerhetspraksiser i norske oppstartbedrifter, og utvikling av en anvendbar intervjuguide. Disse hypotesene ble deretter testet gjennom intervjuer av fire norske oppstartbedrifter, for å identifi-

sere elementer av deres sikkerhetsaktiviteter og deres motivasjon for å utføre disse.

Gjennomgangen av eksisterende potensielle relevante veiledninger og rammeverk knyttet til informasjonssikkerhet identifiserte eksisterende materialer som hadde elementer av relevans for sikkerhet i oppstartbedrifter. Imidlertid dekket ikke noen av disse alle emner som ble rapportert som viktige for oppstartbedriftene. Mange aspekter av oppstartbedriftenes praksiser relatert til sikkerhet ble også dekket av veilederne og rammeverkene. Intervjuene identifiserte f.eks. at oppstartbedriftene vanligvis hadde etablert noen elementer av systematikk for sikkerhetsadministrasjon, og sørget for at en person (intern i ledelsen eller ekstern ekspert) støtter ledelsen i sikkerhetsspørsmål. Opplæring og bevissthet om informasjonssikkerhet var viktig, men oppstartbedriftene varierte i hvordan opplæring av ansatte ble utført. Media fokuserer ofte på de digitale angrepene og økonomiske konsekvenser, mens denne studien fant ut at motivasjonsfaktorer spiller en viktig rolle. Det ble funnet at eksterne faktorer (for eksempel GDPR-bøter, omdømmeskade og at kunder stolte på dem), samt interne motivasjonsfaktorer (f.eks. entreprenørånd og en tro på produktet de lager) spilte viktige roller for hvordan oppstartbedriftene jobber med sikkerhet.

Studien konkluderer med at oppstartbedrifter, som ofte er preget av en løst definert arbeidsprosess og mangel på ressurser, har et behov for skreddersydde retningslinjer tilpasset oppstartbedriften og deres arbeidsform og virkelighet. Videre kan etableringen av felles læringsplattformer og en delingskultur mellom oppstartbedrifter for temaet sikkerhetsproblemer foreslås. I tillegg er det viktig at de ansattes motivasjonsfaktorer tas i betraktning når man utvikler disse nye retningslinjene og plattformer for deling, med det overordnede målet å redusere sikkerhetsutfordringer i eksisterende og fremtidige oppstartbedrifter.

# Preface

This thesis is a master thesis for MSc in communication technology studies at Norwegian University of Technology (NTNU). This thesis is based on the specialisation Information Security. The work and the report itself has been produces between January and June 2019. In addition, a pre-project was conducted during the previous semester autumn 2018.

First of all, I would like to thank my supervisors for their support and for their courage to let me explore the little researched field of security practices in Norwegian startups! I am grateful to my responsible professor Karin Bernsmed for her many advises and inputs on the thesis, and to my supervisor Erlend Andreas Gjære for his knowledge, experiences, insight to the topic and valuable discussions of startups. I sincerely thank all interviewees for taking their time and sharing their thoughts and security practices with me. Without them, no potential security practices in startups would have been found! Last, but by no means least, I would like to thank my family and friends for supporting me through this work: thank you!

Nora Futsæter
Trondheim, June 2019

# Contents

# List of Figures

# List of Tables

# Chapter 1
# Introduction

The technology industry is undergoing a revolution. With innovation and new technology, new business models are being developed at high speed, and new customers' needs are identified. The importance of new technology is global. As of 2017, the five most valuable Norwegian companies were technology companies [2], and internationally startups such as Uber[1] and Airbnb[2] have changed entire sectors [3]. With new technologies there are new potential business ideas which can lead to innovation within an existing organization, and leading entrepreneurs to create a new startup. A startup may be defined as a *temporary organization designed to search for a repeatable and scalable business model* [4], while others might characterize them to be an organization characterized by youth and immaturity, limited resources, multiple influences and dynamic technologies and markets [5]. Others again do not focus on these characteristics, but rather identify themselves as a startup with their mentality stating that *Startup is a state of mind* [6]. Either you want your groceries delivered at your front door by kolonial.no[3], an interactive classroom environment by using Kahoot[4], or sell energy from a solar panel produced by Otovo[5] placed on your roof, you are interacting with a startup. In common, all these startups started with an initial good business idea and want the world to use their products or services.

Investments in Norwegian startups are larger than ever, and the year 2018 was no exception. The Norwegian startup ecosystem is growing fast, with a total of 185.5 million dollars invested in Norwegian startups in 2018 [7]. This was an increase of approximately 70% compared to 2017 [7], indicating a signal of an increased focus on Norwegian startups. The Norwegian Government are also emphasize the important role of startups, by funding startup initiatives and addressing the need for partnership with startups [8].

[1] For more information about Uber https://www.uber.com/no/nb/
[2] For more information about Airbnb https://www.airbnb.no/
[3] Kolonial.no is an online grocery store https://kolonial.no/om/
[4] Kahoot! is a game-based learning platform https://kahoot.com/
[5] Ovtovo makes solar panel for private homes https://www.otovo.no/

In general, new technologies are accompanied by new information security threats. In recent years, there have been an increasing number of attack against Norwegian organizations, with the attacks being more and more advanced [9]. It has been known for a while that larger firms often become victims of hacker attacks. Examples are the recent ransomware attacks such as Wannacry [10], targeted attacks against larger firms such as the attack on Visma [11] or targeted attacks towards the public health sector in Norway [12]. Cyberattacks or data breaches may result in major economic consequences and impact on the organizations. *Mørketallsundersøkelsen* from 2018 reported that organizations being victims to data breaches had costs from 54.000 to 2 mill NOK [9].

However, also smaller companies may be victims of data breaches and cybercrime activities [13]. In America, 14 out of 30 millions small businesses were breached by cybercriminals in 2016 [13]. Small and midsize firms fall victim to the vast majority of data breaches because they tend to lack sufficient security measures and trained personnel, and hold data that is valuable to hackers (e.g., credit card numbers, protected health information). Furthermore, it was reported that there was an increase in attacks towards organizations connected with a supply chain, where the attacks target the weakest link in the supply chain[9]. Recent reports state that 54 percent of small and medium sized enterprises, commonly referred to as SMEs, that were victims to cyberattack or a data breach got out of business within six months [14].

Startups may be characterized by several features that make them particularly vulnerable to cyberattacks. Their youth and immaturity, limited resources and dynamic technologies [5], can result in startups facing uncertainties and risks affecting their work. Most startups do not make it due to commonly referred to risks for example market fit risks, product risks, partner risks, team risks, sales risks. Thus, startups could be considered to represent "low hanging fruits" for cyberattacks. However, similar to established organizations, many startups are not aware of all risks due to information security.

## 1.1 Research questions

In order to reduce the vulnerability to cyber attacks, there is a need for general and specific guidelines on how to prevent security risks.

Previous studies have focused on startups and their processes, how they grow or how they are organized [5]. In addition, a research group on SINTEF has focused on Security for Agile Software Development [15], with agile being a development process found in many development teams, exploring how one can combine the agile development process with high speed delivering with security requirements.

In addition, one study has also performed a technical vulnerability test on some Norwegian startup [16]. However, there are in general few research papers on information security in startups per se. While there are some guides and frameworks that are designed for SMEs or larger organizations, it is unknown whether these guides could be relevant for Norwegian startups. The Norwegian Government launched a National Cyber Security Strategy both relevant for public and private sector in addition to authorities [17, January 2019]. It can be assumed that most of the existing information security guidelines are developed on a more general level and/or targeted at larger companies. Although some guidelines are directed towards SMEs, there is not much available information about specific guidelines for information security activities that address information security risks in startups. Based on available guidelines and frameworks, and on interviews of some startups, this thesis will investigate how Norwegian startups are working with information security, in order to identify if there are some practices which could be regarded as best practices.

Furthermore, recent research has also made interesting suggestions that motivation and motivational factors are important improving security in organisations [18]. Furthermore, that both situational and personal factors are relevant for the end-users behavior related to security activities. However, it is unknown whether motivational factors play a role in the startups' work with information security, and how motivation affects this work.

The aim of this thesis is to explore information security issues in Norwegian startups. Specifically, it will give an overview over available frameworks and guidelines for information security with relevance to startups, and through interviews investigate what startups are focusing on regarding information security and which security activities they are performing. Motivational factors regarding the work on and implementation of information security practices in Norwegian startups are also explored.

The research questions for this study are:

- **Research question 1:** What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?

- **Research question 2:** What existing information security practices are found in Norwegian startups?

- **Research question 3:** What motivational factors for information security are found among startups?

## 1.2 Contributions

Given the research questions, this study contributes with an initial approach for exploring the field of information security in startups. Taking an exploratory approach, this study is the first to identify information security practices in Norwegian startups, in regards to how they work and how they implement security activities in their work. This is also the first study to identify the importance of motivational factors in the startups' work with information security.

Figure 4.1 and 4.1 are unique and a result of the review of some potential relevant frameworks and guides for information security, where main information security topics are categorized. In addition, the citations from the interviews in (table) 4.3 give an unique picture of information security practices in Norwegian startups, and the importance of motivational factors. Based on these finding two suggestions for prototypes is presented.

Furthermore, this thesis can also be of inspiration for future research in the field of information security in startups, with the ultimate goal to reduce vulnerability related to security issues in existing and future startups.

## 1.3 Outline

The thesis is structured as follows:

**Chapter 1:** Introduces the topic of the thesis including the motivation for this topic.

**Chapter 2 Background and related work** looks at relevant terms and definitions for both information security and startups. In addition, previous work conducted in the area of security in startups and selected related subjects are presented.

**Chapter 3 Methodology:** explains how this study was conducted in terms of methodology.

**Chapter 4 Results:** presents the results from both the review related to research question 1, including a presentation of the related frameworks and guides reviewed. Then, the main interview findings related to research questions 2 and 3 are presented. In addition, suggestions for two prototypes with the goal of improving security in startups is presented.

**Chapter 5 Discussion:** discusses the results related to the research questions. Furthermore, this chapter presents a discussion of the methodology. In addition,

it includes a presentation of potential future research for the topic information security in startups.

**Chapter 6 Conclusion:** presents the conclusion for this study.

# Chapter 2
# Background and related work

This chapter looks at previous work conducted in the area of security in startups and selected related subjects. It will also present some different terms and concepts which will be relevant for the thesis. First, definitions and relevant materials for information security management will be presented (2.1). Furthermore, there will be an introduction to startups and their processes. Different frameworks and prior research on information security frameworks which could be relevant for startups will be presented. In addition, prior research on information security practices in startups and research including agile development will be presented (2.2). Lastly, a background on motivational theory and its relation to include security in startup is explored. In addition, influential factors for information security in organizations is presented (2.3).

## 2.1 Information security management

Information security can be defined as *"Protection of the confidentiality, integrity and availability of information assets, whether in storage processing, or transmission, via the application of policy, education, training and awareness, and technology"* [19, p. 2]. Every organization is unique, and according to Whitman and Mattord book on information security management [19] there is none fits all when when working with information security. Consequently, there are as many ways to implement information security as there are organizations or firms implementing it.

In information security a framework is *"a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security control, including InfoSec policies, security education and training programs, and technological controls"* [19]. Hence, a framework is a generic document or outline in order to describe how an organization can address information security. A framework can further affect how the employees will implement different security controls or different aspects regarding security referred to in the framework.

With the framework including general guidelines which organizations can adapt, information security policies are *"written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets"* [19, p. 140]. Hence, the policies are formal statements and rules about the organizations information security philosophy. However, policies do not describe operations and how to comply with these policies.

Organizations may have different practices, procedures or guidelines for how to comply with the policies. Procedures can be defined as *step-by-step instructions designed to assist employees in following policies* according to Whitman and Mattord. Practices are *"Examples of actions that illustrate compliance with policies"* [19, p. 144]. Subsequently, a best practice is a practice that can be considered to be the practice giving best results in a specific industry or a similar organization [19]. Guidelines are *"Non mandatory recommendations the employees may use as a reference in comply with a policy"* [19], and can be considered tips or additional information for how one can address information security policy. Hence, on an overall level there are strict definitions on what practices, procedures and guidelines which is relevant for security. However, these are not specifically discussed in a startup context which may have less formal definitions in their work on information security.

### 2.1.1 Process in startups

In recent years there has been a growing interest to solve future challenges [3]. Entrepreneurs can work with these challenges either in an existing establishment or in a startup. Characteristics for startups are that they accumulate from the entrepreneurs andor founders that have a business idea which has the potential result in a scalable business model. Hence, startups are new businesses with the goal to create something new or combine different resources leading to the startup growing [3].

Startups can be categorized according to their ambitions [3]. If their ambition is to establish a subsidiary income they are categorized as a hobbystartup. If their wish is to establish their own place to work they are categorized as livelihood startups. Lastly, if their ambition is strong growth and technology bound they are categorised as growth startups. This growth evolves in different stages: first an idea and development phase, then an establishment phase followed by a commercialisation phase, and lastly a growth phase [3]. This growth phase is mainly characterized as the phase when the startup already has a product on the market and focus on further structuring of the organization systems for production, sales and distribution [3]. However, even though these phases are clearly defined in the literature, this may not entirely be reflected in real life startups.

Startups can face different challenges during all these stages. Especially in the

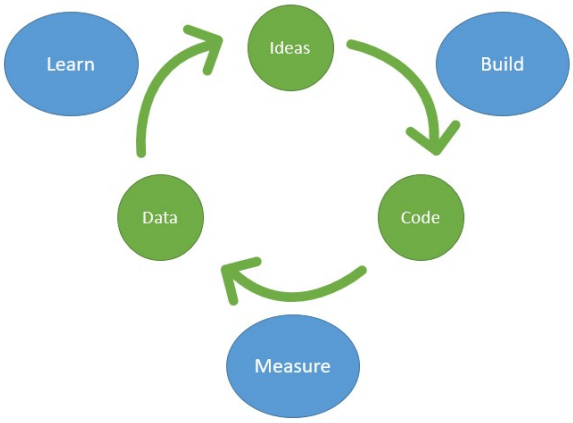


**Figure 2.1:** The lean startup framework. The figure shows the different phases; build, measure and learn. First one comes up with an initial idea, then one builds this idea. In order to find out if this result matches the needs for their customer, the built product is measured. Lastly, the results from the measure will used to learn what their next iteration of their product will be like [20]

first phases there are risks and factors for uncertainty that startups face, e.g. there is a need to find out that there is a market demand for what they are making. In addition, they often face shortage of resources, both in terms of human and capital resources [3]. However, to minimize uncertainty and the use of resources, startup can perform experiments. This is in startups often done by a process called Lean startup. However, the Lean startup process can also be applicable for other types of organizations than startups in order to address factors for uncertainty. In 2008, Eric Ries presented the Lean startup process which aims to create and manage startups and minimize the time to market [20]. The approach uses small iterations with continuous innovation with the activities build, measure and learn, as shown in figure 2.1.1. In order to have a process that matches the startups need to push their product to the market fast, the Lean startup can be applicable [20].

Although not directly comparable, agile is a type of software development process which also aims to add business value earlier in the software development process is agile development [21]. Instead of delivering the whole product at once, agile development aims to *Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale* and uses smaller

iterations [21].

In general, literature suggests that process can be difficult in a startup [5]. Firstly, process maturity requires repeatability, however the youth and dynamism of startups practically preclude repeatability. Process in startups in general is often characterized by an ad hoc approach, or by improvisation [5]. The lean startup framework and agile has some elements of repeatability and consists of many small iterations when developing a product (2.1.1). This may have implications for what kinds of information security frameworks which can be relevant for startups.

### 2.1.2 Information security frameworks and practices

Finding relevant information security frameworks for businesses can be a challenge. In general, businesses may have designated information security frameworks regarding information security. Small and medium-sized enterprises commonly called SMEs are businesses that have less than 250 employees [22]. A study from 2016 [23] looked at 110 SMEs in Scotland and how they struggle with security advice. They concluded that most SMEs expressed a need for advice regarding information security. The SMEs also expressed an high uncertainty, even though they had access to free advice online. However, the amount and content had lead to confusion and uncertainty. There are some frameworks relevant for SMEs such as those presented by the National Cyber Security Center in UK [24] [25], and a guide from NorSIS [26]. However, established enterprises and startups work differently according to Sutton [5], which may have consequences with their work in security matters.

In general, when selecting information security practices there are some considerations which one can follow [19]. These can be the following questions:

- Does your organization resemble the target organization of the recommended practice?
- Are you in a similar industry as the target of the recommended practice?
- Do you face similar challenges as the target of the recommended practice?
- Is your organization structure similar to the target of the recommended practice?
- Can your organization expend resources at the level required by the recommended practice?
- Is your threat environment similar to the one assumed by the recommended practice?

**Table 2.1:** Questions to consider when selecting recommended information security practices [19]

Prior work has concluded with that there are no specific frameworks that focus

on information security in startups. However, even though entire frameworks and guides are not specifically designed for startups, they may include elements in existing frameworks and guides that may be relevant for information security in startups. It is unknown if guides and frameworks aimed for SMEs might be relevant for startup. There might also be less formal guides that are aimed for startups. Hence, research question 1 *What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?*

## 2.2 Security practices in agile and startups

In agile software development there are several studies that show how to include information security in the process. A study from Nicolaysens team focusing on how software security fits into software development projects where agile methodologies are used [27] found that for most of the companies functionality was more important than security. Furthermore, only one of the companies tried to combine software security with the agile methodology. The study focused on companies with the agile process called Scrum methodology [28]. Nicolaysens team [27] also found that it is necessary that every person in the project is involved in the security activities from start. In addition, the combination of agile and security can be difficult. They proposed that teams can integrate parts of security activities into their process activities. Another study on agile and nonfunctional testing [29] found that the agile philosophy with adding value early to the customers [30] is not easily resolvable with quality attributes such as nonfunctional requirements. This can result in insecure systems.

A study focusing on software Security Skills, Usage and Training Needs in Agile Teams found some security activities [31]. The most used security activities found were code review, static code analysis and pair programming [31]. These security activities could also be presented as best practices for the agile teams. They studied two agile teams and found that skills of the team drives the kind of activities that are performed, and not so much cost and benefit. In addition, effective software security adoption in agile setting is not automatic, it requires a driver. The organizations also agreed that they needed training on secure design and secure coding.

When studying information security on a technical level, research have indicated that startups have little focus on secure coding. A study on startups and test on their corresponding web application from 2018 [16] revealed that all startups had severe security holes. The web applications were tested if they were secure against vulnerabilities presented in OWASP top 10. OWASP top 10[1] is a list with the 10 most critical web application security risks and are based on a broad consensus in

[1]The Open Web Application Security Project Foundation is a open community which works for enabling support material for secure applications. For more information [32].

the community of security experts. OWASP say that «*Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code*» [33]. The startups tested [16] that had the most severe security holes were also the one with the least knowledge about OWASP top 10. These startups did not use a systematic approach to ensure information security [16].

In conclusion, prior research has focused on some security practices in agile and tested some web applications from selected startups. However, little is known regarding specific practices regarding information security practices in startups. Research question 2 will answer *What existing information security practices are found in Norwegian startups?*

## 2.3 Motivation and influencing factors relevant to the implementation of information security in startups

There are several motivational factors that can affect both the individual and influence what the organization focuses on. This may also be of relevance for the implementation of security practices in startup. Motivation can be defined as *To be motivated moves one to do something* [34]. Hence, motivation can lead to behaviour and actions. Furthermore, motivation can be distinguished into different types, with *intrinsic motivation* often referred to as *internal* being that a person wants to do something because it is interesting or enjoyable [34]. On the other hand, *extrinsic motivation* often referred to as *external* being that a person does something because it can lead to a desired consequence [34]. Intrinsic and extrinsic motivation are referred to in business context, where one can be do tasks and assignments by own free will (internal), or can work on an activity for reasons that lie outside the activities intrinsic value for the person (external) [3]. However, motivation is often a mixture of both intrinsic and extrinsic motivation.

Previous studies on information security and motivation have actually indicated that motivation is important when addressing security. Stantons group [18] study on information security found that end user behaviour related to security was dependant on both situational and personal factors. These findings highlight the importance of studying motivational factors regards to information security in organizations. A study from 2016 [35] also presented that developers attitude and motivation is a important factor for the implementation of secure software development practices in enterprises. Moreover, they found that *developers carry "not my problem" mentality when it comes to securing the system because they do not believe that they make mistakes which cause vulnerabilities in the system* [35]. In addition, a study comparing code developed by startups with freelancers found out that startups managed to implement more secure code [36]. They also looked at the relationship between

knowledge and secure code, and suggested that one of the key characteristics that distinguished the two groups appeared to be motivation. For the startups there was a lack of strong correlation between knowledge about security and the security of the resulting product which may indicate that startups might be more motivated and dedicated to making a quality product [36].

In general, there can be several influencing factors which can affect how the the organizations prioritize security. In SMEs a study [37] identified three factors that are important for motivation of decision makers regarding information security, both positive and negative. Most important was the reputation in regards to their customers, than the level of information security compared with the security threats in the industry. Lastly, SMEs decision makers were motivated by focusing on business priorities instead of information security [37].

A review on factors influencing implementation of secure software development practices [35] found several factors important for information security. First the developer's skill, experience and knowledge is important for understanding the potential security threats, and lack of understanding these can lead to the developer unwillingly introducing vulnerabilities in the development process. This is also important for startups [38], and the factors *Human capital* especially in the term of *talent* is important for the startup ecosystem. Moreover, *It is the talent of founders and early employees through which startups are created and scaled* [38]. Another factor that influences the implementation of secure software development practices are adequate development time and budget [35]. However, in startups studies have found out that limited resources often are a characteristic for startups [3] and that the limited resources are an important factor for influencing the process [5]. In addition, when battling with limited resources the process is seldom a priority, when the startup company often aims to minimize the time to market [5], which may influence their focus on security.

There are also factors on an organizational level which can influence information security in an organization. Security training and awareness with the goal being that the organization has an effective security program is also a factor influencing the implementation of software security practices [35]. There are also factors defining the organizations culture and how this might influence the effectiveness of the implementation of security management. Changs group [39] found that control oriented organizational traits and consistency have a positive effect, while flexible oriented organizational traits such as innovativeness were not associated with information security management principles. Thus, organization culture is important for the effectiveness of implementing information security management. In addition, top management support and building and retaining a security team were also stated as important factors [35].

Taken together, previous studies show that motivation is important for the implementation of security practices and that there are a lot of influencing factors for prioritizations in organizations and startups. However, there has been little focus on motivational factors for employees implementing security in startups. Therefore, identifying why startups implement information security activities and what motivates the employees to actively include security measures is of importance. Hence, research question 3 *What motivational factors for information security are found among startups?*.

# Chapter 3
# Methodology

This chapter presents the research methodology applied in this study. First, the research topic (3.1), research questions (3.1.2) and the thesis research design (3.2) will be presented. Then, the methods for the data collection, both the review of frameworks (3.3) and the semistructured interviews (3.4) and their corresponding analysis of the results will be presented. In addition, how these results can be further used is presented (3.4.4). Finally, methodological considerations for the review of frameworks and interviews (3.5), and ethical considerations will be presented (3.5.1). The overall process of this study is shown in figure 3.

## 3.1 Research topic, research questions and hypotheses

### 3.1.1 Research topic

The goal of the preproject (September to December 2018) was to identify and refine the research topic and formulate the research questions. The main topic of this study is *what are* and *what could be* information security practices for Norwegian startups. The research topic was decided by the researcher and based on interest [40]. When deciding for yourself is a more exploratory approach with few or no constraints, and the research can be driven by interest. However, this approach is not as straight forward as having the decision made for you [40]. It was important to have a clear research topic as this forms the basis for the research and was important to do before you can start researching [40].

### 3.1.2 Research questions

There are several types of research questions, and depending on how they are designed can affect what kind of methodology one should use. Since the area of security in startup has had little prior research the research questions had the goal to describe and explore this field [40]. According to Robson, [40] research can be used to explore, to describe and/or to explain. Having the purpose to describe and to explore are

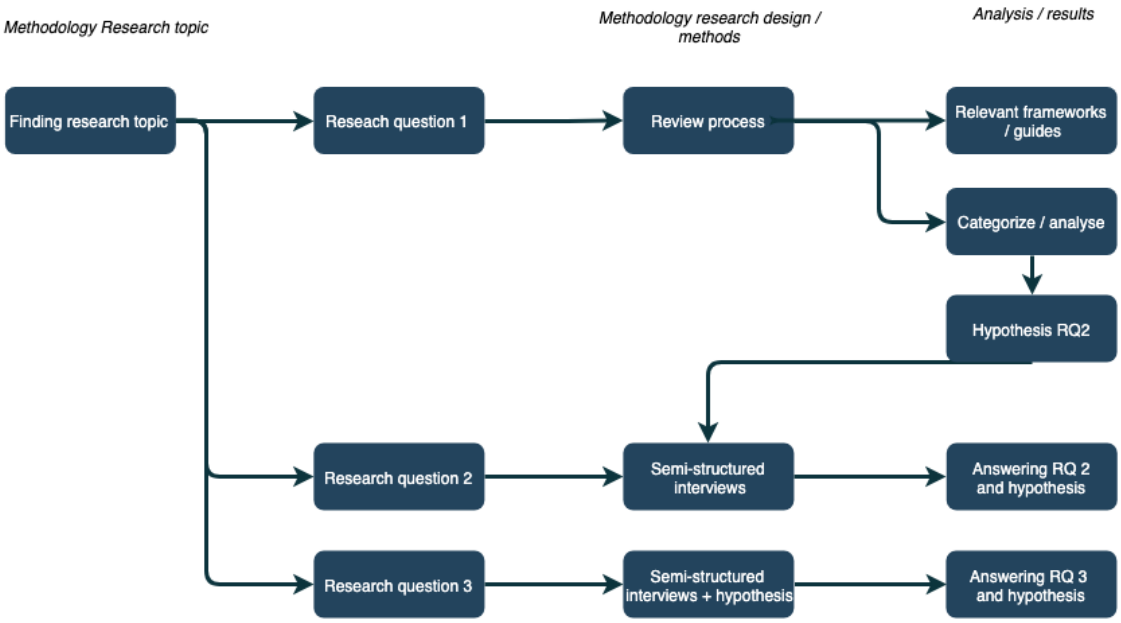


**Figure 3.1:** Overall methodological process of this thesis: First, the research topic was found and the research questions were formed. Then, the methods for the different research questions were chosen, and this resulted in their corresponding results in order to answer the research questions.

useful in researching fields with little prior research, it is useful to include 'what' and 'how' questions [40]. These research questions have the purpose to explore and describe. In this thesis, the purpose was to explore and describe and only 'what' questions were included.

**Research question 1: What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?**

As stated in the background only few, if any, studies have researched what could be relevant information security practices for startups. In order to generate a hypothesis and an applicable interview guide for interviewing startups regarding security, the overall aim for Research Question 1 was to identify existing material relevant for information security in startups.

This was conducted by:

– Reviewing selected potential relevant frameworks and guides for information security and explore their potential applicability for startups.

- Identifying whether there are similar guidelines or commonalities from the different guides.

- Assess whether these guidelines could be relevant for a startup and their way of working.

- Based on these findings relevant hypotheses and interview guide (Appendix C) were made

**Research question 2: What existing information security practices are found in Norwegian startups?**

The preproject gave a clear impression that there are different opinions about if startups work with information security, and, if so, what they actually do (results not published). It was therefore interesting to identify "state-of-art" regarding information security practices in Norwegian startups.

The goal of research question 2 was therefore to:

- Use the hypotheses and interview guide to identify what startups actively do to implement information security

- To evaluate whether there are commonalities of the security practices in the different startups by performing semi-structured interviews with 3-5 Norwegian startups applying the interview guide

**Research question 3: What motivational factors for information security are found among startups?**
From literature, it has been suggested that motivation may influence the security in organizations, and this might also explain how they work with security. Therefore, this research question specifically aimed to target motivational factors in startups.

The goal of research question 3 was therefore to:

- Identify why startups work with security and what motivates them in this work, by analyzing the interviews regarding motivational factors.

- Analyzed which factors are mentioned, and this might also explain how they work with security.

## 3.2 Research design

The methodology for the review and interviews were based on principles from *Real world research* by Colin Robson and Kieran McCartan [40] and *Kvalitative Forskningsmetoder* by Aksel Tjora [1]. In addition, the analysis part of the qualitative interviews were based on analysing methods from *Interviews. An introduction to qualitative Research Interviewing* by Steinar Kvale [41].

As the research questions were formed as 'what' questions the results will be non-numerical. In addition, not knowing what the research will end up with and the way the research questions are formed calls for a flexible design [40].

With the research questions all exploring different approaches to the main theme information security practices in startups, a case study exploring this topic was chosen [40]. Case studies and together with ethnographic studies and grounded theory studies the most commonly used methods in flexible design [40].

With the overall goal being security in Norwegian startups, the group of interest for this case study was Norwegian startups. Case studies often focus on an individual or group [40]. In addition, the context of the Norwegian startups were taken into account. Furthermore, case studies can be applicable when studying firms and organization and their culture, best practices and/or policy implementation [40]. Hence, a case study approach of startups and how they work with security is an appropriate fit.

## 3.3 Review of frameworks and guides

This section will include the methodology for how the review of potential relevant framework and guides for information security in order to answer research question 1 *What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?* First, the search strategy, data collection and data analysis will be presented. Lastly, an explanation of how the mapping of these results ended with hypotheses for the interviews is presented. The review process was inspired by performing a literature review which consisted of; decide on focus, develop research questions, choice of search strategy, consideration on ethical issues, recording of search findings, preparation of data for analysis, analysis and interpretation of the data and reporting of findings [40].

### 3.3.1 The research questions forming the focus of the review

Taking apart research question 1, *What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?* formed the way the review process was conducted.

The parts about *... some existing knowledge and frameworks for information security...* can include frameworks and guides different from sources. The part *existing knowledge and framework for information security* can include huge amounts of material. According to Tjora [1] the materials can have different form such as scientific papers, case specific or different medias. Furthermore, it is important to find their context including who authoredpublished them, who is their target group and what are their purpose. The review on these relevant publications and materials was carried out as a metaanalysis, which can be used to create an overall picture of theories and methods [1]. Including the formulation *some* resulted in the researcher being flexible in the decision on what to include.

With the term information security this can include many different frameworks and guides. The last part of the research question states *... relevant for Norwegian startups* specifically includes Norwegian guides and frameworks which may not be relevant for startups in other countries. Since Norwegian startups are the target group, sources from Norwegian actors were important. In addition, the guides and frameworks needed to take the context of the startups into account when determining the relevance. Lastly the middle part *... with the potential of being relevant...* affect the search strategy and weakens the need for a strict process and makes the strategy flexible.

The search strategy for finding relevant materials consisted of three different strategies. In addition, to finding relevant materials the goal was also to form a basis for the interview guide. It was therefore important at this stage to talk with startups and ask which guides and frameworks they had heard about, and including these in the search. This first search was done through the networking phase [40] of the preproject([42]results not published). These were initial networking conversations about what they had heard about. Then, the responsible professor and supervisor also provided some additional information regarding guides and framework the could be relevant for startups in their experience. This was relevant since the supervisor also has a security startup. Lastly, a internet search for information security framework and guides was conducted. It has to be emphasized that this was not an exhaustive search, and there may be other relevant frameworks and guides for startups.

The guidelines for choosing the materials included the following:

- Guide or framework being mentioned by either a startup, supervisor or through search
- Guide or framework including security activities
- Guide or framework including a organizational aspect of information security

– Guide or framework aimed for organizations with some similar characteristics as startups

### 3.3.2 Recording of data and analysis

The guides and frameworks were analysed using a process inspired by thematic coding analysis [40]. The materials from the search were included in a excel document including their headlines. Then the process of reading the framework and guides to get an overview of the content resulted in some initial codes [1]. Next, the qualitative data were categorized by main themes [1] and color coded in the document. This was done in order to identify what themes and topics were found across different materials. Hence, if there were elements of similar topics in several guides or framework these were coded as the same category. The result of this color coded mapping are presented in 4.1.

The codes, later referred to as categories, were then used to formulate the hypotheses to research question 2 about best practices in Norwegian startups. This in order to see what kinds of themes and practices were mentioned in both the reviewed framework and guides and in the interviewed startups.

### 3.3.3 Considerations for the review

Several factors may have affected the reliability of the findings for the review. The reliability of the results is the *stability or consistency with which we measure something* [40, p. 105]. Which materials were included were dependent (reliability) on the startups and persons being asked and personal opinions. In addition, the mapping of the themes were done by one researcher and can be affected by this researcher's interpretation of the content. Hence, the search is not reproducible [40].

## 3.4 Semi-structured interviews

In case studies, as this study is, several methods can be used to answer the research questions [40]. In this study, semistructured interviews were used. Interviews are frequently used in case studies, and there are several types of interviews (e.g. structured interview, semi-structured interview and unstructured interview [40]). These semiinterviews used an interview guide, as seen in Appendix C. However, compared to a fully structured interview, semiinterviews are more flexible. The questions are the same for different interviews. However, in semistructured interviews the interviewee can change the order of the questions and ask followup questions. In addition, even though the interview is based on a interview guide, the interviewer can do minor customization to the questions being asked in each interview.

With this study being a case study, the data can evolve during the data collection, and in these cases semi-structured interviews are widely used [40]. This results in a less formal way of communication which can be an advantage when interviewing. When using in interviews in case studies the interviewer assumes that the person can tell them about their own experiences in addition to information about the organization according to Tjora [1].

For choosing interviews, several considerations were made. This included whether or not it was practically feasible and how one could do this, what kind of resources and contact one has, what can be read into the different results and resources available [1]. When answering the research question *What information security practices are found in startups?* one could interview startups, do desk-based research, questionnaires or observational methods. According to [40] one can use as a rule of thumb observational studies to find out what people do in public, interviews or questionnaires to find out what people do in private, interviews or attitude scales to find out what they think and feel and standardised test to find out their abilities. Research question 3 *What motivational factors for information security are found among startups* focus on factors and personal opinions for people working in startups. This could then be answered through questionnaire or interview. According to [1] one needs to consider practicalities and therefore a interview which can cover both research question 2 and 3 was less time-consuming than two different methods. With the goal of the research being finding some best practices regarding information security, and not to find what is representative practices for Norwegian startups this study can be conducted with a smaller number of interviewees. Therefore interviews was an appropriate method for this study.

### 3.4.1 Planning and making

When planning for the semistructured interviews there were several factors that needed to be addressed.

#### Recruiting respondents

The respondents were recruited through networking during the initial phase of the study. There were some factors involved when selecting respondents. However, these were not cut in stone, but more guidelines when recruiting.

- A business identifying themselves as a startup
- From Norway
- Tech industry
- Growth startup (2.1)
- Growth phase (2.1)

The goal was to find some practices used in Norwegian startups regarding information security. According to Kvale [41] the number of interviewees depend on the research's goal. Therefore a smaller number of respondents was suitable. Initial talks with startups showed that people working there were very busy, resulting in time-consuming work recruiting potential interviewees.

A strategic selection when recruiting respondents was also discussed in the literature [1]. The main rule when choosing respondents to qualitative studies is that one chooses respondents that for some reason are able to make reflective statements comment on the topic in question. This is oppose to quantitative studies where the study in most cases needs to be representative. However, their own motivation for participating in this study might affect the results and answers during the interview.

#### Interview phases

The semistructured interviews were structured in three phases as shown in figure 3.4.1. The first phase was a few minutes of warm up questions [1]. The first phase was a warmup phase with questions with the goal of making the interviewee start talking and getting comfortable. This phase lasted only for a couple of minutes. During this phase the interviewees was asked about a few demographic background variables and an initial question about their startup context.

The second phase 3.4.1 was the reflection phase, and it was here the interviewee was asked questions related to the research topic [1]. In this part the interviewees were asked about if and how they worked with information security and motivational factors trying to get information confirming or denying the hypotheses. The interview guide also included different followup questions in case the first answer did not include enough information. In this phase the interviewer's personal capabilities were important.

The last phase was the windingup phase 3.4.1 and this phase was to end the reflective phase and normalize the situation between the interviewer and interviewee čitekvalitativmetode:2012.

### 3.4.2 Conducting

Employees from four startups were interviewed at their place of work around February and March 2019. They were all taped on a dictaphone so they could later be transcribed. In order to ensure valid description all interviews were recorded in addition to being transcribed [40]. However, one interview, as described in table 5.5 was conducted at their place of work and in person. Facetoface interviews are preferred because it makes a more natural atmosphere for the interviewee [40] and

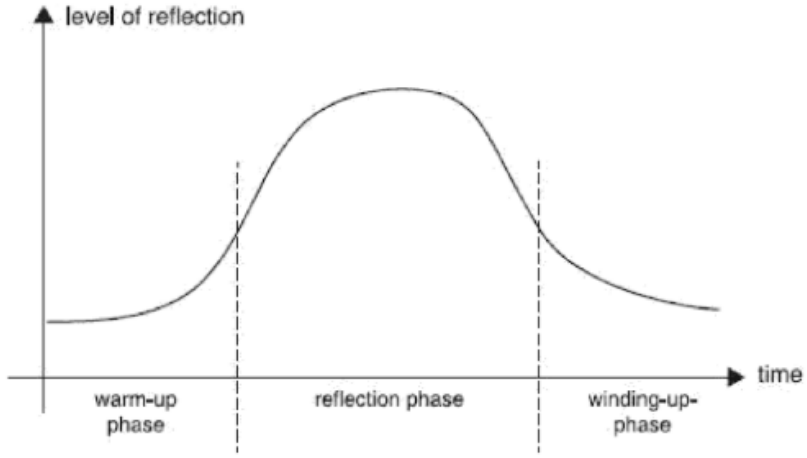


*Figure 6.1* The phases of the in-depth interview

**Figure 3.2:** The phases of the in-depth interview: first a warmup phase, followed by a reflection phase and a windingup phase concluding the interview. [1]

potential of failure of the communication devices used. The last interview used a video conference solution Appear.in, due to practical considerations.

The following startups were interviewed:

### Startup A

Startup A is a tech startup founded some years ago in Norway. They consist of between 20-40 employees and make a physical product. This product is on the market and can be purchased by both private users as well as businesses. They have already had some versions on this product. Hence, they can be considered as being in a growth phase [3].

### Startup B

Startup B is a Norwegian tech startup, and consist of 40-100 employees. They make a digital tool for digitalisation of processes. Their product is on the marked and is purchased by businesses. They can therefore be considered as being in a growth phase [3].

### Startup C

Startup C is a Norwegian tech startup delivering a communication solution. Their product can deal with sensitive data, and it is already on the market. They have between 5-15 employees. Even though they have fewer employees than the other startup, they can still be considered as being in a growth phase [3].

**Startup D**

Startup D is a Norwegian tech startup delivering a communication solution. Their product can deal with sensitive data, and it is already on the market. They have between 20-40 employees. They can be considered as being in a growth phase [3].

Table 5.5 presents information about the interviews, duration, who was interviewed and the quality of the interview. "Quality" refers to a subjective measure of a sound quality of the audio recordings. Sound quality of the audio recordings.

| # | Date | Venue | Duration | Interviewee role | Quality |
|---|---|---|---|---|---|
| A | 29.01.19 | Their offices | 1h 6 min | CTO | Good |
| B | 05.02.19 | Their offices | 1h 1 min | Developer | Good |
| C | 05.02.19 | Their offices | 1h 4min | Data Protection Officer (DPO) | Fair |
| D | 12.02.19 | Video conf. | 44 min | Data Protection Officer (DPO) | Fair |

**Table 3.1:** Information about the interviews in chronologically order

### 3.4.3 Analysis of interviews

The analysis of the interviews consisted of four steps; interviewee describing, interviewee discover, interviewee interprets and interviewer interprets [41]. The first three steps of the analysis were performed during the interviews. First, the interviewees described their situation. They talked about their experience with how their startup works with security. In this part there was no analysis or interpretation from the interviewee side [41]. This was reflected through the warmup questions and initial question. Then, when asking questions or followup questions the interviewee could start to reflect and discover new aspects of what they are talking about [41]. This was the second step of the of the analysis phase. They could see new meanings of what they are experiencing [41]. In order to get to this level of analysis followup questions gave the interviewee room to expand their answers is important. This can be according to Robson [40] adding a period of silence, an enquiring glance or saying "mhhhmmm..". In addition, always asking "why" after the interviewee has answered makes the interviewee reflect on their own answer. The third step was when the interviewer makes interpretations and then the interviewee can either confirm or deny this statement [41]. This was done through repeating parts of what the interviewee just said [40]. This is important for the interview in such a way that there is only one interpretation of what the interviewee really said and meant [41]. This was done through followup questions and resulted in self-clarifying interview [41].

The last part of the analysis was when the researcher analysed the transcribed interviews [41]. First the transcribed interview was structures, this was done by colorcoding relevant parts of the interview. Then unnecessary materials of the text was removed and significant material was discovered making the materials ready for further analysis. Next, the different answers which corresponded to the different hypotheses where marked in order to have results which could either confirm or disprove the hypotheses. In addition, using meaning condensation the whole interview was read through to finds themes that dominated the natural meaning condensation as clear and easy [41]. Then the content connected adjacent to the different hypotheses were collected per hypothesis and then compared.

### 3.4.4 Prototype development

Based on findings from the interviews, a suggestions on a prototype with the aim of improving security practices in startups will be presented.

Results related to the research questions often generates new problems or new questions [43]. This thesis will explore different aspects of information security in startups, and based on these findings one might discover suggestions or improvements. Being an exploratory case study, it is unknown what can be the results from the interviews. However, the problem description includes a last task *Suggest a prototype with the aim to help startups improve future best practices regarding security.* This study will present a suggestion for designing a prototype [43], which will be presented in results.

## 3.5 Generalisability, reliability and validity

With research involving people there are methodically considerations one needs to address when discussing the validity of the results [40]. This section will address the validity, generalizability and reliability of the study.

The reliability of the results, often in qualitative research referred to as dependability relates to consistency and replicability of the results [40]. This study being a qualitative study involving people cannot be directly replicated by an independent investigator [40]. There are several reasons for this, all affecting the trustworthiness. First of all, the direct circumstances of the semistructured interviews cannot be recreated since *Social life contains elements which are generalizable across setting and other element that are particular to given setting* [40]. Thus, there are elements which are the key to social science such as finding out what some information security practices in startups are. However, it does not provide for a predictive power. Hence, even though all four startups did the same security practice, it cannot be concluded that all startup are doing the same practices.

Qualitative methods cannot have the same approach as statistical generalisations [40]. There are several reasons for this including it needs a large representative sample for the target group. In a qualitative study and this study the quality of the data is considered more important, and therefore researchers must sample adequate data and the appropriate data. Hence, these results can be used for analytic generalisability. This study examines different information security activities in startups, and the method and results can be used for suggestions for other when investigating security in startups.

Validity of the results are related to whether we find the actual answers to the research question asked in the introduction is often referred to as credibility in qualitative research [1]. The interviewers behaviour can have a lot of influence over the interviewee, and therefore the interviewers capabilities are important for the credibility and dependability of the results [40]. In this study the interviewer only has minor knowledge to interviewing, and this might also affect the credibility. Due to this, the interviewer trained on interviewing test responder in order to address this weakness. This included focusing on not ask leading questions, giving the respondent time to reflect and the use of non-verbal language to get the person continue talking. Other issues which may affect the credibility can be recording quality and thereby the transcriptions.

The transferability of the results are unknown. Some measures were taken in order to make the results transferable to similar situation with similar parameters [40]. This is why the sample of chosen startups had some inclusion criterion.

### 3.5.1 Ethics

When conducting research involving persons it is important that this research should not harm the persons involved in any way [40], and the following activities were conducted.

First an application for research approval was sent to the Norwegian Privacy Services for research data [44]. This application is shown in Appendix A. The corresponding approval is attached in Appendix D.

All respondent had to read through and if deciding to participate commit to a declaration of consent, as shown in Appendix B. There it is also stated that the consent could be withdrawn through the use of email contact. When interviewing there where no questions about personal information, as seen in Appendix B. However, if the interviewee or interviewer mentioned a name of an individual or the startup these were in the transcribed version transcribed as NAMEXX or Startup #. In order to make it difficult to recognize the individual startup, the startup name as

well as sector and size are not explicitly presented in this thesis. The data including personal data such as Audio recordings will also be deleted when not needed.

# Chapter 4
# Results

This chapter presents the results from the review of relevant framework (4.1) and results from the interviews (4.1). For the literature review first the results of the coded guides and frameworks will as categories (4.1). Furthermore, an introduction about the different frameworks and their coding is presented. Then, the different hypotheses created for the interviews using the categories will be presented (4.2). From the interviews the results will be presented under the corresponding hypothesis (4.3). Lastly, two potential prototypes for improving information security in startups will be presented (4.4).

## 4.1 Review of existing frameworks and guides

Research question 1 : What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?

In order to identify existing knowledge and frameworks which could be relevant for startup there was first a selection of materials based on the questions presented in table 2.1.2 and the process as presented in section 3.3.

The result of this approach was the following guides and frameworks presented below. After this initial selection, the different frameworks were mapped. This process is presented in section 3.3.2. Coding of the different themes in the guides and frameworks ended up with the following codes as shown in Figure 4.1. The hypothesis connected with the categories are presented under the corresponding category.

When selecting the frameworks which were included in the study, the questions presented in table 2.1.2 were considered. Based on number of employees, guides for SMEs were included since these could face similar challenges due to their number of employees. In addition, the information security management framework ISO27001 and guide from NSM. Lastly, some technical guides and overview of security activities were also included.

**Figure 4.1:** List of categories from mapping of frameworks

- Category 1: Organizational, overall, planning
- Category 2: Product requirement and design
- Category 3: Product coding / testing
- Category 4: Release, maintenance
- Category 5: Infrastructure
- Category 6: Personnel security and training

The results from the interviews answering the hypothesis are presented in section Interview findings 4.3.

### 4.1.1 ISO/IEC 27001

The information security standard ISO/IEC 27001 [45] specifies the management in organization when working with information security. The goal of the standard is to provide requirements for establishing, implementing, maintaining and continually improving the information management system. There are objectives for the different information security controls and examples of what those security controls can be. Organizations implementing these requirement can be certified after an audit.

This ISO standard is a management system and specifies how to have management controls regarding information security. Hence, this is on an organizational level, and most of the chapters from the standard have been coded as category 1, as shown in figure 4.1. The part about competence and awareness have been coded as Category 6; personnel security and training.

### 4.1.2 NSMs grunnprisipper for IKT-sikkerhet

The Norwegian National Security Authority is the authority in Norway with the purpose of protecting regarding national security [46]. One of their tasks is also to give information and advice about information security. They have a guide with consisting of four principles about how one should secure their ICT systems including the steps "Identify", "Protect", "Maintain and discover" and "Handling and restore" [47].

These principles and underlying measure are to protect systems and their associated infrastructure [47]. Hence, many of the measures, as shown in figure 4.1, are coded as Category 5; infrastructure. In addition, the categories 1 with the organizational aspect, category 6 with personnel security and category 4 with maintenance are also represented.

| ISO 27001 | NSMs grunnprinsipper for IKT-sikkerhet | Norsis - cybervirksomhet for små virksomheter |
|---|---|---|
| 1 Understanding the organization and its context | **1. Identifisere** | Grunnleggende cybersikkerhet |
| 2 Understanding the needs and expectations of interested parties | Kartlegge leveranser, verdikjeder, enheter, programvare, brukere og behov for tilgang | Beskytt filene og enhetene dine: oppdater programvare, sikre filene, krev passord, krypter enheter og bruk totrinnsbekreftelse. |
| 3 Determining the scope of the information security management system | 2. Beskytt (sikker tilstand for IKT miljøet for å motstå eller begrense skaden ved dataangrep | Beskytt ditt trådløse nettverk |
| 4 Information security management system | Ivarta sikkerhet i anskaffelse, utviklingsprosesser, sikker design av IKT miljø og konfigurasjon | Fysisk sikkerhet |
| **5 Leadership** | Ha kontroll over IKT-infrastruktur, opprettelse, bruk av deaktivering av brukerkonti | Hvordan beskytte utstyr og dokumenter |
| 1 Leadership and commitment | Kontroller bruker av administrative privileger, dataflyten inn til virksomheten og mellom sikkerhetssoner | Hvordan beskytte informasjon på enhetene dine |
| 2 Policy | Beskytt data ved lagring og kommunikasjon, e-post og nettleser | Skadevare |
| 3 Organizational roles, responsibilities and authorities | Etabler hensiktmessig logging | Hvordan beskytte din virksomhet |
| **6 Planning** | 3. Oppretthold og oppdag | Phising / falske e-poster |
| 1 Actions to address risks and opportunities | Opprettholde den sikre tilstanden i IKT systemet over tid etterhvert som virksomheten utvikler seg | Hvordan det fungerer |
| 2 Information security objectives and planning to achieve them | Etabler en prosess for endringshåndtering, planlegg implementering av endringer og vurder konsekvensene av disse | Hvordan beskytte virksomheten |
| 7 Support | Beskytt IKT-systemene mot skadevare. Bruk gjerne automatiserte verktøy. | Om du blir rammet |
| 1 Resources | Verifiser konfigurasjonen ved bruk av automatisert verktøy for sporing av endringer. | E-post autentisering |
| 2 Competence | Gjennomfør inntrengingstester og øvelser for å teste den totale styrken i virksomhetens forsvarsmekanismer. | Brukerstøttesvindel |
| 3 Awareness | Overvåk og analyser IKT-systemet for å bygge en situasjonsforståelse av handlinger og aktiviteter i nettverket. | Hvordan det fungerer |
| 4 Communication | Bruk automatiserte verktøy for jevnlig sårbarhetskontroll av infrastrukturen. | Hvordan beskytte virksomheten |
| 5 Documented information | Ta sikkerhetskopier, og verifiser at tilbakekopiering er mulig. | Sikker fjerntilgang |
| 8 Operation | 4. Håndter og gjenopprett | Hvordan beskytte enheter |
| 1 Operational planning and control | Forbered virksomheten på håndtering av hendelser. | Ekstern tilkobling til nettverk |
| 2 Information security risk assessment | Etabler en plan for håndtering av hendelser, og øv planen med de som er involvert. | Del 8: 10 anbefalte tiltak |
| 3 Information security risk treatment | Vurder og kategoriser hendelser. | Etabler tilstrekkelig systematikk for sikkerhetsstyring, og sørg for at en fagperon støtter ledelsen i arbeidet |
| 9 Performance evaluation | Kontroller og håndter hendelser. Loggfør alle aktiviteter underveis. | Inkluder digital sikkerhet i virksomhetens risikoarbeid. Etabler tydelig ansvar og effektive rapporteringslinjer til ledelsen og styret. |
| 1 Monitoring, measurement, analysis and evaluation | Etabler varslingslister over kunder, ansatte og andre som er berørt. | Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene. |
| 2 Internal audit | Iverksett gjennopprettingsplan. Tiltak vil variere avhengig av type hendelse. | Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset treningsprogram jevnlig for å fremme god sikkerhetskultur. |
| 3 Management review | Evaluer og lær av hendelseshåndteringen i etterkant. | Sats på god bestillerkompetanse, og gjør en risikovurdering som forankres hos ledelsen. |
| 10 Improvement | | Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Skru på logging og kontroller viktige logger jevnlig. |
| 1 Nonconformity and corrective action | | Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer |
| 2 Continual improvement | | Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC. Krypter viktig informasjon når den lagres på bærbare medier og når den sendes over nettet. |
| | | Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk totrinnsbekreftelse, eller som et minimum sterke passord. |
| | | Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvinger som tester planen. |

**Figure 4.2:** Potential relevant frameworks and guides with colorcoding according to their categories, part 1

| Cyber security: small business guide | Cyber security: small business guide actions | BSIMM | Datatilsynets veileder |
|---|---|---|---|
| Backing up your data | **Policy actions - staff determining overall policy** | Governance | Training |
| Keep your backup separate from your computer | Identify and record essential data for regular backups. | Strategy & Metrics | Requirements |
| Consider the cloud | Create a password policy | Policy & Compliance | Design |
| Read our cloud security guidance | Decide what access controls your users need so they can access only the information and systems required for their job role. | Training | Koding |
| Make backup part of your everyday business | Decide what staff need access to USB drives | Construction / Intelligence | Test |
| Protecting your organisation from malware | Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup. | Attack Models | Production setting |
| Install antivirus software, prevent staff from downloading dodgy apps | Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically. | Security Features and Design | Forvaltning |
| keep all your IT eqipment up to date | Technical actions - actions carried out by technical staff | Standards and Requirements | |
| Control how USB drives can be used | Switch on your Firewall. | Verification / Touchpoints | |
| Switch on firewall | Install and turn on Anti-virus software. | Design Review / Architecture Analysis | |
| Keeping your smartphones and tablets safe | Block access to physical ports for staff who do not need them. | Code Review | |
| Switch on password protection | Consider making a password manager available to your staff to secure their passwords. | Security Testing | |
| Make sure lost or stolen devices can be tracked | Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud. | Deployment | |
| Keep your device and apps up to date | Set automated back-up periods relevant to the needs of the business. | Configuration and Vulnerability Management | |
| Dont connect to unknown wi-fi hotspots | Switch on password protection for all available devices. | Software Environment | |
| Using passwords to protect your data | Install and turn on tracking applications for all available devices e. g. Find my iPhone. | Penetration Testing | |
| Switch on password protection | Enable two-factor authentication for all important accounts (eg email). | | |
| Use two factor authentication for important accounts | Apply restrictions to prevent users downloading 3rd party apps. | | |
| Avoid using predictable passwords | Install the latest software updates on all devices and switch on automatic updates with periodic checks. | | |
| Help your staff cope with password overload | Training and awareness actions - carried out by staff implementing training and awareness | | |
| the mainnsm | Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords. | | |
| Avoiding phising attacks | Create a Cyber Security training plan that you can use for all staff. | | |
| Configure accounts to reduce the impac of successful attacks | Include details of your 'Password' policy explaining how to create a non-predictable. | | |
| Think about how you operate | Include how to spot the obvious signs of phishing. | | |
| CHeck for the obvious signs of phising | Include details of your reporting process if staff suspect phishing. | | |
| Report all attacks | Include details on how your business operates and how they deal with requests via email. | | |
| Keep up to date with attackers | Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network). | | |

| Coding |
|---|
| organizational, overall, planning |
| Product requirement and design |
| Product coding / testing |
| Product production, forvaltning, operations |
| Infrastructure |
| Personell security and training |

**Figure 4.3:** Potential relevant frameworks and guides with colorcoding according to their categories, part 2

### 4.1.3 NorSIS cybersikkerhetsguide for små bedrifter

NorSIS is a partner of the government in Norway and the Norwegian center for information security [48]. Their role is also stated in the National Cyber Security Strategy is to improve both companies and private individuals knowledge on cyber security, with their top priority being small and medium-sized enterprises. In January 2019, they presented the first part of their guide for security in small businesses were they present advice and information about what businesses should do. This is focusing on threats and how one can protect themselves against them [26]. In March 2019, they added a new part to this guide based on the National Cyber Security Strategy including ten recommended measures to improve digital security in businesses [49].

*NorSIS cybersikkerhetsguide for små bedrifter* is a hands on guide with specific tips on how one can protect a business. Many of the tips are about how one can configure and protect their assets, coded as category 5: infrastructure (figure 4.1). In addition, some of the measures are more on a organizational level and therefore coded as category 1, and lastly some measures are more on a personnel and training level and coded as category 6.

Regarding the parts originally presented in the Norwegian Cyber Security Strategy there are several organizational aspects categorized as category 1. In addition, there are some measures related to infrastructure categorized as category 5 and one measure related to category 6.

### 4.1.4 Cyber security: small business guide

The National Cyber Security Center is the UK authority on cyber security [25]. They work with and support different private and public sectors in the UK, the general public and also has a focus on SMEs (small and medium enterprises). This work includes incident response and recovery as well as preventive work. They have made a small business guide for showing how SMEs can protect their organisation's data, assets and reputation [24]. NCSC empathises that this guide is targeted to smaller businesses, charities and private persons, and that you don't need to protect a critical infrastructure system in order for it to be relevant.

This guide is divided into 5 parts including different categories of actions small businesses should make [24]. Part 1 about backup is coded as Category 4 maintenance, part 2 is about malware protection and coded as category 5 infrastructure, and the last three parts are measures coded as category 6 (figure 4.1).

### 4.1.5 Cyber security: small business guide actions

The National Cyber Security Center has also produces a guide with relevant actions for the guide presented above [50]. This guide is a one-pager including 26 relevant security actions targeted to small businesses [24]. The activities are divided into three sections; policy actions, technical actions and training and awareness actions.

The first part of the guide including the policy actions are coded to category 1 since they are on an organizational level, as seen in figure 4.1. Part 2 and 3 about technical actions and training and awareness include many tips about awareness and tips about what to include in security training and awareness and is therefore coded to category 6 ( figure 4.1). Part 2 also consist of some technical aspects coded as category 5: infrastructure.

### 4.1.6 BSIMM Framework

BSIMM is a framework that studies real-world implementations of software security in different organizations [51]. It is a descriptive measurement which the organizations themselves participate and register which software security initiative they do. Then they get feedback on what other organizations in their field are doing [51]. There are 112 different security activities grouped in four different categories.

Part 1 of BSIMM is about Governance and is mostly coded as category 1 (figure 4.1). However, the measures about training is coded as category 6. Part 2 about making attack models, security features and design and requirements is coded as category 2: product requirement and design. Part 3 about verification and security touchpoints is coded as category 3. And lastly, part 4 about deployment is coded as category 4 product to release.

### 4.1.7 The Norwegian Data Protection Authority Guide Data protection by design and by Default

The Norwegian Data Protection Authoritative has made a guide for how businesses can develop products according to the requirements presented in article 25 of GDPR[1]. This is how on can include privacy in all steps of the development process, from planning to maintenance [53].

Since this guide is about product development, the guide is mostly coded as the categories about product development process (figure 4.1). Part 1 about training is coded as category 6, part 2 and 3 about requirements and design as category 2,

[1] General Data Protection Regulation is a regulation in the EU involving data protection and pricavy for citizens in EU and European Economic Areas. For further information [52]

coding and testing as category 3 and the parts about release and maintenance as category 4.

## 4.2 Using the categories from the review to develop an applicable interview guide and form hypotheses

The review of existing guidelines and frameworks resulted in the categories presented below, and clearly show that the different guides and framework have different focus.

### 4.2.1 Category 1: Organizational, overall, planning

Category 1 is included in five of the frameworks/guides. This is therefore also included in the interview guide part 2 termed Organizational level security. In the section termed "Persons" it is asked about how they are organized and who is working with security. Also in the last part of the interview it is asked about what they think could be relevant frameworks for other startups. From this category these hypotheses were made:

- H1: Startups has a distribution of responsibilities and roles related to security
- H2: Only one person in the startup is seeking information regarding security

### 4.2.2 Category 2-4: Product development

Since all the startups selected for the present study are making a product, the categories about product security was included. The development process is therefore included in the interview guide. This section is mostly based on "Datatilsynets veileder" [53] and the BSIMM [51], focusing on specific stages in the development process. Even though backup is coded under category 4, specific questions about backup is asked in the section called "checklist".

- H4: Startups take steps to secure their product in several stages of a development process.

### 4.2.3 Category 5: Infrastructure

Several of the guides have comprehensive sections about how to secure ICTsystem. This was not prioritized in the interviews due to time limitations. Therefore none of the hypotheses are linked to infrastructure. However, there is one question in the checklist about USB drives which is relevant for this category.

### 4.2.4 Category 6: Personnel security and training

This category was mentioned in all the framework and guides, and was therefore included in the guide in several parts.

- H3: There is a requirement that you learn a lot yourself

## 4.3 Interview findings

This chapter presents the findings from the interviews conducted. The interview guide is attached as Appendix C. The findings are divided into two parts. The first part corresponding to research question 2 *What existing information security practices are found in Norwegian startups?* 4.3.1. This section is further divided into the hypotheses formed after the literature review 4.2. The second part corresponds to research question 3 *What motivational factors for information security are found among startups?* 4.3.2. This chapter is also further divided into the related hypothesis.

For each hypothesis, related findings from the interviews are presented. First, the hypothesis is stated, then it is concluded about what was found in the interviews regarding this statement. This conclusion is then supported by the statements listed in the tables. The tables consist of three columns, the first includes the startup alias, the second presents the statement relevant for the hypothesis. The third column is a result of the analysing method presented in 3.4.3. This is the theme or subject to the particular statement, and it is presented in order to make it easier to understand in which context this particular statement is included. The statements include both statements which support or disapprove the hypothesis.

In this part the goal is to present the statements objectively, and personal opinions and analysis is not included. In Chapter 5 Discussion the different hypothesis and research questions are discussed.

### 4.3.1 What existing information security practices are found in Norwegian startups?

Hypotheses 14 is about security practices found in Norwegian startups. The following hypotheses are based on findings related to the review.

#### H1: Startups has a distribution of responsibilities and roles related to security

All startups had a distribution of the responsibility of information security. First a brief explanation about characteristics of the findings will be presented, and then the respondents exact statements to support these findings.

**One main** person could be pointed at as being the persons with the overall responsibility for security in their startup. This person could either be a person with a technical background or a person working with a organizational aspect on security.

**Several persons involved** in the different security activities was mentioned in all interviews. In all startups the responsibility regarding security was not just one person's' responsibility, but several others were also involved. However, this was be expressed in several different ways.

Table 4.1 presents the different statements from the startups regarding hypothesis 1 and the main subjects supporting this hypothesis listed above.

| # Startup | Statements from interviews regarding roles and distribution of responsibility | Subject |
|---|---|---|
| 1 Startup A | "*Det er flere, det er mest direkt, mest på it sikkerhet er det jeg som har det overordnede ansvaret og jobber en del med det"* | One main |
| 2 Startup B | *"Det er en sikkerhetsansvarlig"* | One main |
| 3 Startup C | *"Og så er jeg informasjonsikkerhetsansvarlig"* | One main |
| 4 Startup D | *"CTO er jo security officer, så den personen så har hovedansvar for sikkerhet."* | One main |
| 5 Startup A | *" (...) meg med det som går på it sikkerhet. Jeg har også jobbet en del med hu som jobber med digital markedsføring, og særlig det med rundt GDPR i fjor vår og det og egentlig få gjort det. (...) så det er hun som har tatt ansvaret for."* | Several persons involved |
| 6 Startup B | *"Eller om det ville bli innkalt til et sånt security [...] møte der man tok det."* [when asked about who would be involved in a decision regarding security] | Several persons involved |
| 7 Startup C | *"Vedkommende som er lead developer hos oss fungerer som fagressurs for meg på det tekniske"* | Several persons involved |
| 8 Startup D | *Jeg jobber mest med personvern, CTO er jo security officer, så den personen så har hovedansvar for sikkerhet. Men jeg vil jo si at sikkerhet er noe alle utviklerne jobber med da."* | Several persons involved |

**Table 4.1:** Statements regarding roles and responsibilities in startups

### H2: Only one person in the startup is seeking information regarding security

As presented in H1, in all startups there are more than one person involved in the activities regarding security. When asked about who is seeking information about security some of the startups said that more than one person did this. The persons involved in seeking information were different for the startups, and different kinds of involvement are presented below. Since only one person from each startup was interviewed, it is difficult to conclude whether they could speak on behalf of the others working with security in the startup, or not.

**Several** persons seek information regarding information security. This was found in several interviews.

**One main** person presented itself as the main person seeking information regarding information security.

**Distribution for different types** of information security was mentioned by some startups. Some of the startups mentioned that they had some who worked with the GDPR implementation while others worked with product security.

**External parties** were involved in their work with information security for two of the startups. Instead of having their own employees to seek information, they hired external parties to help them with this security work.

Table 4.2 presents the different statements from the startups regarding who seeks information about security. The main findings are presented with the relevant statements from the interviews and a column with the subject relevant for the hypothesis is presented.

| # Startup | Statements from interviews | Subject |
|---|---|---|
| 1 Startup A | *"Når det kommer til it-sikkerhet er det nok jeg som CTO og som i begynnelsen i software development, så har vært et spisset ansvarsområde (...) og hun som har ansvar for digital markedsføring så da hadde vært gjennom et GDPR compliant løp (...) så hu hadde jo en del erfaring med det som ikke er rent teknisk, men mer hva som er rent regulative krav, hvordan skrive man en privacy policy. "* | Several |
| 2 Startup B | *"Jeg hadde spurt først ville jeg spurt folk jeg tror hadde ville ha kompetanse på det. som også kan inkludere sikkerhetsansvarlig da."* [when asked about where interviewee seeks information] | Several |

| | | |
|---|---|---|
| 3 Startup C | *"Det er primært meg. Men det er klart det er sikkerhetsmessige aspekter som det er fornuftig å drøfte med, utviklerteamet er jo en del av det når vi diskuterer sikkerhet."* [when asked about who seeks information] | One main + distributed for different types |
| 4 Startup D | *"Men jeg vet at veldig mange er flinke til å lese seg opp på ting, på en måte de som er på nett da. (...) Så folk søker aktiv opplysninger om de tingene de jobber med"* | Several |
| 5 Startup A | *"og de er jo utviklet av mindre erfarne utviklere, så da prøve jeg i størst mulig grad å lære dem sikkerhetsprinsippene da (...). Så mens jeg jobber med de da prøver jeg også å minne dem på ikke funksjonelle krav som sikkerhet i software." (...) Informasjonssikkerhet så er det primært basert på min erfaring og hun som har ansvar for digital markedsføring så da hadde vært gjennom et GDPR compliant løp"* | Distributed for different types |
| 6 Startup C | *"vi søker nok heller etter å søke folk som kan det, at vi egentlig tenker å forsterke det med å hente noen inn som er dedikert på det."* [when asked if someone else in the startup seeks information about security] | External parties |
| 7 Startup D | *"og så har jeg en jurist som er veldig god på personvern som jeg kan sparre med."* [when asked about where interviewee seeks information] | External parties |

**Table 4.2:** Statements regarding who seeks information about security in startups

### H3: There is a requirement that you learn a lot yourself

Hypothesis 3 is about the startups expectations to their employees and what is important regarding learning. The startups all mention that it is important to learn yourself or to have experience. And, as mentioned in H2, some startups use external parties instead of learning that specific activity themselves.

**Experience** of their employees is important for the startups. Two of the startups explicitly say that having people who can work independently and have experience is important.

**Learning from others** is also a characteristic mentioned in one interview. In this case the main person working with security teach the others.

**Learn yourself** is a characteristic for some of the startups. This is either seeking the information yourself or seeking information through discussion in a group.

**External** parties are involved in some of the startups doing specific security activities.

Table 4.3 presents different statements relevant for the hypothesis about the requirements for employees to learn about security. The statements are from the interviews and the subject related to this specific statement is under the third column.

| # Startup | Statements from interviews | Subject |
|---|---|---|
| 1 A Startup | *"for min del er jo det aller mest erfaring fra tidligere, gjennom virke som konsulent så har jo det vært veldig sentralt fordi vi har jobbet opp mot mye store private og statlige foretak der sikkerhetskravene har vært en del av både kravspesifikasjonen eller en del som kunden har stilt veldig eksplisitte krav til. (...) Informasjonssikkerhet så er det primært basert på min erfaring og hun som har ansvar for digital markedsføring så da hadde vært gjennom et GDPR compliant (...) så hu hadde jo en del erfaring med det som ikke er rent teknisk."* | Experience |
| 2 Startup B | *"At det er veldig fokus på at man skal ansetter selvdrevne og tillitsfulle folk, og hvis man gjør det er det mye som løser seg av seg selv"* | Experience |
| 3 Startup A | *"så da prøve jeg i strøst mulig grad å lære dem sikkerhetsprinsippene da, (...). Så mens jeg jobber med de da prøver jeg også å minne dem på ikke funksjonelle krav som sikkerhet i software."* | Learn from responsible person |

| | | |
|---|---|---|
| 4 Startup B | *Når det gjelder fokus på sikkerhet er det noe som diskuteres i liksom i enkeltcaser, og om man da evt tar det videre. Hvis på en måte man føler det er nøye å ta videre. jeg hadde spurt først ville jeg spurt folk jeg tror hadde ville ha kompetanse på det. som også kan inkludere sikkerhetsansvarlige da. Men typisk ville jeg, litt fra case til case kan man kanskje ta en besltuning på det der og da og se på om noen har noe kunnskap, eller vet at her finner man en ressurs på det.* | Learn yourself |
| 5 Startup C | *"Det er jo ofte sånn at man finner ut ting, og så ser man på hva slags policier har andre, og hvem kan vi tenker er flinke på dette. og egentlig se på hvordan det er gjort, og da finner man mye fornuftig."* | Learn yourself |
| 6 Startup D | *"Så jeg vet at de som jobber med det følger med på sider som handler om sikkerheten til de løsningene vi bruker da. Og fanger opp liksom "oi, nå ser det ut som det er noen sikkerhetshull herog har vi dobbeltsjekket sånn og sånn". Så jeg tror det er mye type bransjeblogger, følge med på sidene til de teknologiene vi bruker da, sånn sett."* | Learn yourself |
| 7 Startup C | *nei, vi søker nok heller etter å søke folk som kan det, at vi egentlig tenker å forsterke det med å hente noen inn som er dedikert på det."* | External |
| 8 Startup D | *"men gjør er under oppsyn at en advokat som kan det. så hvis jeg skriver noe så sender jeg det til han og så leser han gjennom det og sånn ting da. så det er jo mye an gjør, men alle de faglige tingene kommer fra noen som kan det da?"* | External |

**Table 4.3:** Statements regarding learning about security in startups

**H4: Startups take steps to secure their product in several stages of a development process.**

The startups all work with product development. This hypothesis is about their product development process and to see is they include security in several steps of this process. The guide from the Norwegian Data Protection Authority 4.1.7 is used to define steps in the development process for comparison. The security activities mentioned in the quotes are not necessarily covering the different steps in the guide,

but they are related to that part of the process. Hence, the statements marked as training are about different security activities the startups are doing towards training.

**Training** was involved in the startups is different ways. Startup C had activities for awareness, while B presented their general guidelines for security. Startup D included discussions about security in a forum where relevant security issues where presented, while startup A had onetoone tutoring from the CTO informing about security practices while coding.

**Requirement** related to security was mentioned by all startups. Some mentioned regulative requirements, while other mentioned customer requirements including security requirements.

**Design** related to security mentioned in order to be compliant and how the startup could comply with the requirements.

**Coding** included some security measures. The startups gave specific examples of how they include security in the coding process.

**Testing** and security testing was involved for the startups in different ways. While some presented that security testing was done each time there was a change involved with internet, others had some tests or considerations that were performed during code review.

**Release** of the product were mentioned as a part of the process from the two startups were the interviewees had technical background. Here they talked about their process with version control and code review.

**Maintenance** of the product was explicitly mentioned by one startup and this was done in partnership with their customer hosting their service. However, specific security measures in this phase was not mentioned.

Table 4.4 consists of relevant statements for the hypothesis and what the startup communicated about their development process. Statements related to different steps are presented. All the startups mentioned some measures they did regarding security in several steps. This is not a exhaustive list of the security activities they do during the development process, but includes the steps they have mentioned in the interview.

| # Startup | Statements from interviews | Steps |
|---|---|---|
| 1 Startup A | *"så da prøve jeg i strøst mulig grad å lære dem sikkerhetsprinsippene da, (...). Så mens jeg jobber med de da prøver jeg også å minne dem på ikke funksjonelle krav som sikkerhet i software."* | Training |
| 2 Startup B | *"Det er generelle retningslinjer på sikkerhet som er utarbeidet. (...) og så hvordan man sikrer seg mot det sånn rent konkret er jo at alle , alt materiale som ligger her over natta som det ligger data på låses inn på safe. Alle har kryptert datamaskin, og alle tjenestene er 2factor på, men det er også passord og behandlet av passord som alle har installert på pcen sin og bruker til passorden. der har vi både personlige passord, men vi har også en passordgenerator som kan opprette fellespassord på ting. så vil si at hvis et er en innlogging et sted med en bedriftskonto, en felleskonto så har de aller fleste tilgang til det gjennom en passordløsning (...) er noe alle nyansatte må gå gjennom og sette opp kontoen på den måten. "* | Training |
| 3 Startup C | *" ja, vi har til og med hatt en lek vi at hvis du går fra maskinen din ulåst har du selskapets velsignelse til å gjøre pranks på de andres pc så lenge det ikke er noe skade for produktet sende ut tøys på slack. (...) Med det leken der har folk skjønt at det er lurt å skru på dynamic lock. "* | Training |
| 4 Startup D | *"vi har snakket om social hacking, snakket om to faktor autentisering. som sånn da vi skulle innføre det så var det først tema på morgenen sånn gjør du det, og så var det en egen ansatt som gikk fra pult til pult gjennom hele kontoret. og da hjalp det ikke å si sånn "ja jeg har installert og og bruker diskkryptering" da skulle han inn og du skulle vise at du hadde gjort det, og "har du printet ut sikkerhetskodene dine?" det var noen som sto over skulderen din til du hadde implementert det da. "* | Training |

| | | |
|---|---|---|
| 5 Startup A | *" hva som er rent regulative krav, hvordan skrive man en privacy policy, og hvordan kan vi sikre at vi gjør det riktig med e-postlistene og sånne ting. (...) og det har vi har fått noe sånn som GDPR gjør jo også at folk utenfor ren it også har blitt mer bevisst. (...) har gjort at det har blitt et mer tema. og nå når vi bruker tredjepart softawre er det ting vi må tenke mer på. "* | Requirements |
| 6 Startup B | *"en sånn generell årvåkenhet og forsiktighet når det gjelder data. og vi sitter jo da på kundedata som da ikke skal deles nødvendigvis. Både med folk som er inne på kontoret og ting som er konfidensielt sånn sett, og også definert at det ikke skal være åpent på internett og andre kunder som er inne på applikasjonen. og det er det et fokus på. "* | Requirements |
| 7 Startup C | *"så hvis vi skal gjøre noe må vi planlegge det og så må det utvikles. hvis det har noe som helst impact på informasjonssikkerheten må det gjøres en risiko og sårbarhetsanalyse, så må det gjøres på endringen."* | Requirements |
| 8 Startup D | *"Det er jo litt i researchfasen også, for det er jo ofte vi må sette oss inn i et nytt domene og se på hva sikkerhetskravene er der da. "* | Requirements |
| 9 Startup A | *"vi har senddesk for all innkommende korrespondanse på support og eposten vår, hvordan blir det da når brukeren skal få slettet det vi har lagret. da må vi sjekke at har den software as a service løsningen i hvert det vi trenger for å kunne være compliant."* | Design |

| | | |
|---|---|---|
| 10 Startup C | *"er sikkerhet en del av produktutviklingen, så det kommer jo opp jevnlig på forskjellige måter, (...) og så det vi bygger, det bygges jo egentlig med dette in mind, så alle dataelementer har en controller og eiere og på en måte. så vi vet hvem som er datacontroller for det her. så vi kan restricte det opp og ned i alle mulige permutasjoner. og så er det en database som i utgangspuntket er unmutable. det er sjeldent sletting og slettehensyn. hvis du tenker produktbehandler og har adgang til en del data, så er det jo slik at det er lite av det som er samtykkebasert, så ingen kan kreve data portability på det. "* | Design |
| 11 Startup D | *" så vil jo på en måte si at det er en del av alle prosessene, fra design tanke på hvordan løsningen skal settes opp og til den er ferdig og mens den lever videre da. det er jo litt som personvern da, du blir jo på en måte aldri ferdig,"* | Design |
| 12 Startup A | *"Vi prøver heller å følge opp noen gode praksiser med verktøyene og rammeverkene vi bruker. Ting har jo blitt veldig mye bedre de senere årene med at moderne rammeverk i større grad legger opp til hvordan vi skal bruke ting. ved å bruke skytjeneste gjør at du sjøl ikke lenger er ansvarlig for den underliggende plattformen. vi prøver å unngå å liksom i størst mulig grad bruke software as a service løsninger for å unngå sjøl å og plattform as a service. så ikke virtuelle maskiner og ikke egne OSer og databaseservere som vi må patche."* | Coding |
| 13 Startup B | *"en typisk sikkerhetslapp kan være at vi ikke burde bruke / ikke mikse API kode som skal håndtere tilganger med faktisk kode som gjør de beregningen eller hva de nå skal gjøre da. At det burde være to sentralt applikasjoner, eller det kan være at det den applikasjonen har noe API endepunkter som eksponeres til brukere, noen bare til internt brukere, det burde være tydelig"* | Coding |

| | | |
|---|---|---|
| 14 Startup C | *"Hvis du har logget inn som admin i applikasjonen så får du ikke, du kan ikke manipulere loggene, det er endringssporbarhet, hvis du har aksess til databasen kan ingenting i appen endres her. "* | Coding |
| 15 Startup D | *" Sånn som videokommunikasjonen er WebRTC, som på en måte har mye innebygd som man ikke kan sette opp uten å ha kryptering innebygd. Så jeg vet at de som jobber med det følger med på sider som handler om sikkerheten til de løsningene vi bruker da. "* | Coding |
| 16 Startup A | *"ikke sikkerhetssjekker, men vi har tester på noe av det. og så har vi stagingmiljøet som det går til først da. Vi jobber veldig mye med det nå med større grad av automatisert tester ,også på ganske lavnivå ting hvor vi lager support boards for å styre hardwaren i test. for primært for å redusere feil og for å redusere regresjonstest tid."* [when asked about having automated security tests] | Test |
| 17 Startup B | *" eller sånne ting som at "oi, nå la vi til et API endepunkt som er et annet, som gjør noe annet da. Ikke bare en til av det samme eller en til som gjør noe tilsvarende, faktisk er en helt annen greie. og det burde separeres ut. og alle de tingene er en del av en code review og det er ikke noe sånn spesifikke, jeg har ikke en sånn sikkerhetscheckliste jeg går gjennom, det har jeg ikke, men det er alltid en del av vurdering. "*[when asked about how they perform a code review] | Test |
| 18 Startup C | *"hvis det har noe som helst med internett så må vi gjøre en ekstern sikkerhetstesting"* | Test |
| 19 Startup D | *"men vet at vi kjører standardiserte tester på koden og sånn, vet ikke hva slags verktøy det er da, men havi har liksom brukt noe andre verktøy som har dekket liksom sånn endepunkter og sånn sting da. Det er mye egentesting og noe eksterne verktøy da."* | Test |
| 20 Startup A | *"da bruker vi pull requester på git og så assinger vi en til to andre. hensikten med den er såklart også å, da vil jo potensielle sikkerhetsting fanges opp"* | Release |

| | | |
|---|---|---|
| 21 Startup B | *"prodsetting er når det, med en gang det er ferdig. når det er gått gjennom, jeg tror de aller fleste tingene har autoprodsetting fra en masterbranch fra github. Når pullrequesten er code reviewet med en godkjent review og bygg er grønt så merger man og så prodsettes det"* | Release |
| 22 Startup C | *"sånn i forhold til helseopplysninger, og det må implementeres av sykehuspartner som drifter på sykehusene."* | Maintenance |

**Table 4.4:** Statements regarding different steps in a development process and how the startups include security

### 4.3.2 Motivational factors

In this section, the following hypotheses are related to research question 3 *What motivational factors for information security are found among startup?*. The hypotheses are aimed to explore out why startups work with security and what motivated them in this work. As in section 4.3.1, the hypotheses are presented and the statements from the interviews as well as the statements' subject. These findings are then presented in table 4.5, 4.6 and 4.7, and can either support or disapprove the hypotheses.

#### H5: Startups are aware of risk and their own risk appetite

In order to explore what motivates the startups to include security, this hypothesis aims to identify if risks are experienced as relevant for startups. All startups had in one form or another mentioned risks during their interview. While some mentioned that they had a overall picture of their risks, others only mentioned that is was a part of their consideration when developing their product.

**Aware,** in terms of being aware of their risks andor risk appetite was found in all startups. All had to some extent thought about risks.

Table 4.5 consists of relevant statements for the hypothesis and what the startup said about risks during the interviews. Statements related to risks are presented below, supporting this hypothesis. The subject of the statement is presented together with the statement.

| # Startup | Statement from interviews | Subject |
|---|---|---|
| 1 Startup A | *"ja, vi har jo hatt en sånn overordnet for den totale risikoen i produktet. Det går på, det er jo også ting som er god praksis når man skal sertifisere produktet med det å tenke gjennom hvordan kan det her, hvilke problemer kan oppstå (...) hvis vi bruker den her, for å unngå at vi lager et produkt som kan gjøre skade. SÅ her har vi risikovurderinger med forskjellige risikoer og sannsynligheter og tiltak og konsekvens. (...) Det er jo nesten sånn at vi har valgt å ikke implementere fullverdig løsning for det enda for det at der må vi ha good call på det."* | Aware |
| 2 Startup B | *"og det vil jo alltid være en vurdering om, når man handler den case nr 2 så er det alltid en vurdering om er dette problem nå, hva er risikoen med sånne ting, og da blir sånne ting diskutert. Og jeg kan ikke si at det liksom alltid det blir første pri dersom man finner ut at dette er et potensielt problem, men per nå fungerer det så er det ikke nødvendigvis slik at det blir prioritert. Men at hvis det blir en pain, hvis man opplever at vi har ikke oversikt så vil man ta det."* | Aware |
| 3 Startup C | *"i realiteten er det sånn at det må gjøre en risikosårhet. så hvis vi skal gjøre noe må vi planlegge det og så må det utvikles. hvis det har noe som helst impact på informasjonssikkerheten må det gjøres en risiko og sårbarhetsanalyse" "nei, altså hvis vi nedprioriterer det får vi ikke satt det i produksjon."* | Aware |
| 4 Startup D | *"Vi har ikke råd til å gå på en skikkelig sikkerhetssmell da. Som gjør at man tar det veldig seriøst vil jeg si, sammenlignet med en del av de litt større som er sånn, det går bra, var litt dårlig for ryktet deres. og så kommer de seg videre da"* | Aware |

**Table 4.5:** Statements related to awareness about risks

### H6: Customers trust and requirements are important for their priorities

Hypothesis 6 is aimed to check if the startups mention customer trust and requirements as a motivational factor when implementing security measures. Both trust

and requirements were mentioned by all startups. However, for one this motivational factor was tightly linked with not only their direct customer, but also to the end user.

**Trust** from customers was important for the startups and also mentioned by all startups. This trust could either be directly linked to their customers, or to their end customer.

**Requirements** from customer were mentioned by all startups. They said that both requirements due to regulations and their customers requirements were important.

Table 4.6 consists of relevant statements for the hypothesis and what the startup said about their customer. Statements related to this are presented below supporting this hypothesis. The subject of the statement is presented together with the statement.

| # Startup | Statements from interview | Motivational factor |
|---|---|---|
| 1 Startup A | *"særlig nå som vi går mot b2b så er det viktig at bedriftene kan stole på oss" "og det er veldig en sånn tillitserklæring. (...) Det er jo noe som gir veldig positivt omdømme. men hvis vi hadde fått noen andre skandaler så kunne det vært skadelig når vi skal gjøre innsalg mot bedrifter og vil bli tatt seriøst som en ny startups da som ikke har en stor track record og stor grad av tillit."* | Trust |
| 2 Startup B | *"og hvis Startup B er / skal ha livets rett så kan man ikke, så må det funke.* [when talking about their need to be secure]. *Fordi å feile på sikkerhet betyr, kan bety at enkeltkunder trekke seg, og for en startup så kan enkeltkunder være viktige nok. (...) En også at vi har kunder som vi må håndtere informasjon ordentlig på. Helt sikkert lovmessig, men også fornuftighetsmessig, På en måte som går mer utover det at det er et omdømme utad, men det ansvaret vi har for kundene sine data. som vi jo tross alt sitter på. så liksom en kombinasjon av den at vi på ta ansvar for kundenes data"* | Trust |
| 3 Startup C | *"at det er er samfunnsansvar, at hvis du behandler helseopplysninger så har du en plikt til å holde dem.* | Trust / Social responsibility |

| | | |
|---|---|---|
| 4 Startup D | *"vi som selskapet får veldig mye spørsmål om informasjonssikkerhet og hvordan vi sikrer, og da tror jeg det er å holde seg oppdatert og kunne svare på hva de lurer på, og så lurer folk på noe nytt og så må man sjekke opp det hva er det for noe. så tror på en måte at vi blir litt tvunget til å holde oss oppdatert bare basert på de spørsmålene vi får da. det er veldig positivt at vi har en kundemasse som driver den utvikling og at de faktisk bryr seg."* | Trust |
| 5 Startup A | *"at vi vil at ting skal være i henhold til regulative myndighetskrav vi har også personer på informasjonssikkerhet som er veldig bevisst"* | Requirements |
| 6 Startup B | *"Åpenbart så har man avtaler med kundene og det inkluderer jo også informasjonsbehanling"* | Requirements |
| 7 Startup C | *"nei, altså hvis vi nedprioriterer det"* [talking about security] *"får vi ikke satt det i produksjon. vi kan ikke ikke gjøre da. da får vi ikke funksjonaliteten på plass. (...) så hvis vi tenker at det har noe å si for informasjonssikkerhet så snakker vi først med sykehuset om det. og så prater vi med dem, og så snakker rundt og avklarer det, vi ønsker å avklare de momentene tidligst mulig, og så før vi legger masse utviklingstid i det. og så vet vi erfaringsmessig at det er ikke alltid ting blir som det er tenkt, for det viser seg at vi må gjøre det i stedet. Så vi har en løpende dialog med dem. "* | Requirements |
| 8 Startup D | *"den må være kjempesikker å bruke, (...) og ha trygge sikre produkter er kjernen i det vi gjør da. (...) det er jo grunnlaget for de produktene vi har da. får ikke solgt XX som ikke er trygg å bruke"* | Requirement |

**Table 4.6:** Statements regarding the startups thoughts about their customers trust and requirements.

### H7: Startups only use external motivational factors as motivation for their work with security

The startups mentioned several different motivational factor for working with security. These were not only external motivational factor, but also internal such as own integrity. Different factors mentioned are presented below and the statements

supporting these factors are presented in table 4.7.

**Product integrity** was mentioned by all startups. They said that they had ownership towards the product, and wanted to make a good product.

**Own integrity** was also mentioned by all the interviewees. They wanted to make a good product, and they mentioned that this was because they took pride in what they made.

**Reputation** and reputation damage was mentioned by one startup as a motivational factor for working with security.

**Laws and regulations** were mentioned as motivational factors. These can be the same as with the factor for requirements for hypothesis 6.

**Topdown** is a factor in such a way that the management is promoting that security is important. Two startups mentioned that their management was saying that security was important.

**Social responsibility** as also mentioned in hypothesis 6 is also presented here and is a motivational factor.

**Investors** role was discussed. However, this was not communicated as an important motivational factor. The one startup said that they had the investors support, but that they themselves had focused on security before the investors expressed any need for it.

**Customers knowledge** was a motivational factor for one startup. They had noticed that their customers were aware about security issues.

Table 4.7 presents statements about motivational factors related to security in startups. Some factors are already mentioned in hypotheses 5 and 6 concerning risks and customers trust and requirements. The statements relevant for motivational factors are presented, and the factor is presented next to the relevant statement.

| # Startup | Statements from interviews | Motivational factors |
|---|---|---|
| 1 Startup A | *"hensikten med den er såklart også å, da vil jo potensielle sikkerhetsting fanges opp, men det er også vel så mye det med kompentanseoverføreing mellom mer enn en teammedlem, så flere har sett på koden, og så er det det å øke kodekvaliteten. (...) det ene er det er jo det at vi har ganske høy integritet i firmaet at vi ønsker å gjøre ting så riktig så mulig"* | Product integrity |
| 2 Startup B | *"jeg tror de alle fleste her er inneforstått med og har eierskap nok til produktet til at det, vi kan ikke ha noe problem med det, det må funke, og hvis xx er / skal ha livets rett så kan man ikke, så må det funke.* | Product integrity + reputation |
| 3 Startup C | *"en motiverende faktor å prøve å lage det bedre da, og fikse litt dårlig informasjonssikkerhet som det jo er. (...) Det er en motiverende faktor for å gjøre informasjonssikkerheten bedre da. på et felt hvor det er viktig og hvor det egentlig ikke er så bra idag. "* | Product integrity |
| 4 Startup D | *"jeg tror det kanskje er litt sånn med typen produkt vi lager da. på en måte, du lager en xx (...) og ha trygge sikre produkter er kjernen i det vi gjør da. For det first så hadde vi jo vært helt sykt fucked hvis vi gjorde noe sykt dumt. og vi har en tanke om at ting skal ha innebygd personvern. det skal være veldig sikre da"* | Product integrity |

| | | |
|---|---|---|
| 5 Startup A | *"vi har også personer på informasjonssikkerhet som er veldig bevisst, altså type linux brukere som er super skeptiske til alt og alle av tjenester, og den type personlighet og holdninger farger jo over også på bedriften. De er veldig opptatt av at vi ikke skal bruke ting om uetisk overfor brukerne. (...) Det er jo kanskje særlig litt det som personligheten til den enkelte i bedriften, det er det å være veldig bevisst på det, og veldig kristisk til hvilke ting man selv bruker. da får man jo en personlig motivasjon med å gjøre ting så skikkelig som mulig.(...)så det har kanskje vært en intern motivasjon kanskje, det å lage et type produkt vi som ingeniører ønsker å lage, og få de andre rundt som kanskje ikke er tekniske til å forstå hvordan tingene henger sammen. "* | Own integrity |
| 6 Startup B | *"det er nok definitivt en sånn egen stolthet inni det også, at når man lager ting så skal man ha det på det rene. (...) og så en yrkesstolthet er sikkert helt inne i det også. jeg synes ikke man skal undervurdere det på en måte, (...) Jeg har gjort mitt beste for å få det til så bra som mulig, men liksom helthet så er det ikke bra, det har enormt mye med motivasjon å gjøre for arbeidet man gjør da. og skal være glad i det man gjør så må man også bry seg om det man gjør. så det er en motivasjonting da. (...) det betyr veldig mye for motivasjon og for arbeid og jobbe. jeg vet ikke, noe av det verste jeg vet om er å gjøre ting som jeg ikke synes blir bra."* | Own integrity |
| 7 Startup D | *"Jeg tror på en måte at det å lage sikre trygge ting er på en måte noe utviklerne føler veldig på selv da. (...) mer at det er en holdning at det er noe man skal bry seg om da. Det er ikke gøy å gjøre en feil på de tingene, det er ikke det du ler av. det er ikke morsomt da"* | Own integrity |

| | | |
|---|---|---|
| 8 Startup A | *"Tredje er jo omdømmetap, altså i Startup A for oss så er brand veldig viktig, vi har jobbet mye med det både med miljøprofilen og den visuelle profilen, hva vi er opptatt av som firma, og da er det veldig viktig at vi ikke får på en måte noe store grove graverende avvik der da og kan få tillits og omdømmetap. (...) og det med brand og design tankegang har vært sentralt helt siden oppstarten. og da faller egentlig alt man gjør med at man blir bevisst med hvordan man blir oppfattet."* | Reputation |
| 9 Startup A | *"så det er jo da særlig da med muligheter med salg og da opp mot investorer vi skal ha et solid inntrykk for å få finansiering til selskapet."* | Investors |
| 10 startup A | *"at vi vil at ting skal være i henhold til regulative myndighetskrav. (...) og særlig det med rundt GDPR i fjor vår og det og egentlig få gjort det. sånn teknisk er det ikke så komplisert. det er litt mer det å skrive privacy og faktisk gjøre den jobben som er litt krevende."* | Laws and regulations" |
| 11 Startup B | *"Potensielle risiko på det er liksom både lovmessig oppfølging, men også ht vi kan miste kunder, som vi ikke trenger på en måte" "plutselig må man lese gjennom GDPR noen ganger og plutselig må man skrive et informasjons sikkerhetsstyringssystem. og så må man slå opp i ting, og se hvordan andre har gjort det, og finne ut hvordan skal den policien være. "* | Laws and regulations |
| 12 Startup C | *"de fleste som driver en liten bedrift blir aldri etergått i sømmene, de må aldri vise noe de har gjort. det er bare hvis ting går galt at det blir et issue for dem. for oss så blir det, vi får ikke lov å gjøre noe uten at det her er gjort,s å vi må dokumentere det og vise det frem, det er en større grad av kontroll for oss enn det er for andre. eller vi må kunne forvente en større grad av kontroll."* | Laws and regulations |
| 13 Startup D | *"ja, veldig mye etter innføringen av GDPR. eller folk har jo spurt om sikkerhet før det og."* | Laws and regulations |

| | | |
|---|---|---|
| 14 Startup A | *"Mest på it sikkerhet er det jeg som har det overordnede ansvaret og jobber en del med det, og så jobber vi veldig mye med"* [When asked about who works with security] | Topdown |
| 15 Startup D | *"men jeg vet at de to som var med å starte det sammen med XX og de som kodet de første tingene at det var veldig viktig for de da. så det kan jo godt hende at det er litt personavhengig, men de var veldig sånn snakket mye om det, var linker til å ta opp veldig sikkerhetsrelaterte ting. (...) jeg tror det var mye av hvem de er da som har dannet en litt sånn kultur i bedriften, her bryr vi oss om de tingene. og det er på en måte viktig å bry seg om de tingene, det er greit å bruke tid på de tingene, dette skal vi gjøre ordentlig da.(...) og sikkert også da fordi de personene som folk ser litt opp til som har jobbet her lenge. fordi de bryr seg så er de gode forbilder. som jeg tror smitter over på folk som begynner her, så man får det litt sånn inn da. det er viktig."* | Topdown |
| 16 Startup C | *"at det er er samfunnsansvar, at hvis du behandler helseopplysninger så har du en plikt til å holde dem."* | Social responsibility |
| 17 Startup C | *"vi har i hvert fall investorenes støtte, om det er noe krav vil jeg ikke si, det er vi som har tatt det opp først, så det er vi som i første omgang har sagt at dette gjør vi for dette. og i hvert fall ovenfor styret og tilsvarende som ofte er med i det daglige"* | Investors |
| 18 Startup D | *"og hos oss er det med sikkerhet noe veldig gjennomsiktig. vi må svare på det ofte. det er mange som sitter på den informasjonen. og da må det jo for det første være bra og noe vi kan stå inne for,(...) så det er, vil si at det er en kjempemotivasjon, og det at du jobber med xx. ingen har jo lyst til at xx skal komme på avveie. Og det er hovedmotivasjonen at det har så mye med det vi gjør."* | Customers knowledge? |

**Table 4.7:** Statements regarding the startups thoughts about why they work with security

### 4.3.3 Chosen practices

**H8: Startups have some basic guidelines on how employees should work securely**

Hypothesis 8 was to check if startup have some guidelines for personnel security. The practices asked about were based on the Cyber security small business guide [24] and Cyber security small business guide actions [50]. The hypothesis was answered through the last part of the interview with yes or no questions. However, some of the answers could not be coded as strictly yes or no. Overall the startup performed at least one of the guidelines, and startup C communicated that they the performed nine of the guidelines.

Table 4.8 presents the questions about practices and what the different startups answered.

| **Practice** | **A** | **B** | **C** | **D** |
|---|---|---|---|---|
| Do employees receive practical guidelines to construction of passwords or a password policy? | no | yes | yes | a little |
| Are the employees required to use 2 factors authentication? | no | yes | yes | yes |
| Do you have guidelines for use of connected devices such as USB? | no | no | no | no |
| Do you have a policy for locking your machines? | no | yes | yes | no |
| Do you use disk encryption?? | no | yes | partial | yes |
| Do you have routines for backup? | yes | yes | yes | yes |
| Do you use a cloud storage / file sharing service? | | yes | yes | yes |
| Do you have a asset list? | no | no | yes | maybe |
| Do everybody have access to everything, or is the access divided? | divided | divided | divided | divided |
| Do you have automatic security tests? | no | no | yes | yes |

**Table 4.8:** Checklist with different practices and the startups answers

## 4.4 Prototype security guide for startups

The last goal for this thesis was to develop some sort of prototype improving information security practices in startups. From the interviews and results two main prototypes would be interesting to further investigate.

First, the interviews found some practices which was in common for the startups. These might be called best practices and could form a basis for guidelines for information security in Norwegian startups. In section 4.4.1 some of these findings are presented as a suggestion on what could be a future guidelines aimed for Norwegian startups. This is not a final guide, only a start on what could be a guide based on already found practices in startups. The aim of such a guide could be that it was based on practices already found in startups, and therefore could be applicable for other startups as well. A premise for that this is a potential guide is that the startups in an earlier stage can be inspired by these steps. It needs to be emphasised that this guide cannot be used for a verification whether what they are doing is enough. That would call for further studies.

The startups also mentioned several different practices for how they learned about information security, and several mentioned that earlier experience was important. Therefore, a platform where startups can share security practices is suggested in section 4.4.2

### 4.4.1 Prototype 1: Suggestions for future guidelines for security in startups

This section includes elements which could be relevant for future guidelines for security in startups.

A guide could include other startups motivational factors for why startups work with security:

- **Why we (startups) focus on security** *"the people working with the product have ownership to the product, and it our startup is to survive it has to work"*, *own integrity* and reputation.
- **Implement security measures from the very beginning** said all the startups contributing in this thesis.

A guide could also include elements of what other startups already did:

- **Checklist** with security practices such as the one from the interview guide.

- **Organizational level tips:** startups in this thesis all had one main person responsible for information security and there were several persons involved.
- **Including security in the development process:** startups in this thesis all had several actions regarding security in different steps of the development

### 4.4.2 Prototype 2: Suggestion for helping startups improve their security practices

A platform for sharing could potentially help startups improve their work with information security. This is inspired by some startup practices which had forums for discussion and a platform where they could address issues related to information security.

Important aspects for sharing:

- Being relevant and tailormade for startups
- Startups being able to share their security practices
- Startups being able to share their experiences, also negative, without getting reputational damage

# Chapter 5
# Discussion

This study investigated different aspect of information security in startups with three main approaches in order to identify the current situation for information security practices in startups. This chapter will discuss the findings presented in chapter 4, this in order to answer the research questions, and their implications for the development of future best practices regarding information security in startups.

The first section 5.1 presents the answer to research question 1 *What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?*. Section 5.2 answers research question 2: *What existing information security practices are found in Norwegian startups?*. Next, section 5.3 presents research question 3 *What motivation factors are found among startups?*. Following, section 5.4 looks at the contextual considerations for the semistructured interviews related to both research question 2 and 3. Next, the suggestions for the prototypes for improving security in startups will be discussed(5.6). Then, section 5.5 discusses the methodological considerations. Lastly, section 5.7 will present some thoughts on what could be interesting topics to investigate further, and discuss some future perspectives in regards to information security in startups.

## 5.1 Research question 1: What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?

Briefly, this section will first answer research question 1, then discuss interesting findings in the frameworks and guides related to different categories presented in Results 4.1. Then, the various security practices in Norwegian startups as identified by the interviews and their relationship to these existing guidelines and framework will be addressed. There are several considerations when selecting an information security practice, as stated in table 2.1.2. This study did not find any existing frameworks which were entirely targeted towards startups. However, parts and categories from

the different guides were found to be relevant also for startups. Especially, the parts about personnel security from the guides for small businesses had some corresponding practices of high relevance. Interestingly, none of the startups mentioned the use of the reviewed guides or frameworks reviewed here.

The review revealed that there were several guides and frameworks for security practices available. The reviewed materials give only some examples of existing frameworks and guides, and hence, do not give a full picture of the guides and frameworks available. However, the review clearly demonstrated that existing guides and frameworks cover aspects ranging from overall an organizational level to more specific "to do" tips regarding information security. The frameworks and guides reviewed are targeted towards larger organizations or SMEs, and are not specifically targeted towards startups.

As presented in chapter 4.1, category 1 consisted of materials concerning parts of guides and frameworks including an organizational view on information security. Since ISO 27001 [45] is a framework for information security management system specification, the overall content identified was on organizational aspects. The hypotheses 1 and 2 were based on the assumptions that startups did not have much organization of roles and responsibilities as suggested by previous literature [5]. However, the interviews revealed that there were some similarities between existing practices in startups and and topics covered in ISO27001 [45]. First, ISO27001 states that one should define organizational roles and responsibilities. Through hypotheses 1 and 2 there was found that the startups all had one main person responsible for the information security. However, their practices were less standardized than described by ISO27001. In addition, there were more persons involved in the security activities in all startups. However, their roles were not as standardized as ISO27001. Interestingly, the need to appoint specific persons responsible for security, this is not specifically mentioned in the guides for SMEs. Therefore, the guidelines identified in the guides for SMEs [24] [50] may not be directly applicable for organizational security practices for startups.

For category 2-4 concerning product development were mostly included in the more technical guides such as Datatilsynets guide for Data proctection by design and default [53] and in BSIMM framework [51]. It is important to emphasize that the BSIMM framework in itself is not a guide. It is a measurement of different security activities that different organizations do. However, the security activities can also be used as inspiration as for what security activities different sized organization perform. Some of the activities in BSIMM could also be found as one of the most used security activities in agile teams [31]. In addition, hypothesis 4 showed that the startups took steps to secure their product in several stages of the development process. Hence, these above mentioned materials for information security in the development process

could be relevant and performed in startup.

Category 6, concerning personnel security and training, were present in all guides and frameworks. The content of category 6 ranged from a overall importance, to specific tips. This topic was in general more specific in the guides for smaller businesses [24] [50]. From the interviews there were evidence that personnel security and training also are important topics for all the startups interviewed. The finding will be discussed in more detail below 5.2.

Regarding the validity of the results, it is important to emphasize that these categories and mappings were subjective, and that even though in this study they are mapped into a specific category, other studies might categorize them differently. Furthermore, the sample of the guides were also chosen on a basis of recommendations as presented in chapter 3.3, thus the validity of the results may have been affected. This is due to the fact that the researchers interpretation can affect the results [40].

In general, the frameworks and guides were not specifically designed for startups, and there was no exhaustive guide for information security in startups. However, parts of the different guides and frameworks included practices that were highly relevant for the startups. Since there were no guides and frameworks specifically designed to fit the startups needs for information security practices, and that guidelines for SMEs also lack some important topics which startups find highly relevant (e.g. roles and responsibilities), it could be suggested that there is a need to develop future guidelines that could be based on a range of the existing work.(referanser med de jeg liker)

## 5.2 Research question 2: What existing information security practices are found in Norwegian startups?

In this section, the results from hypotheses 14 and 8 are included in order to answer research question 2. In general, some information security practices were found in the startups. Some of these were found in all startup, while others were only found in the individual startups. Practices found were related to roles and responsibilities for security activities in the startups concluding that several persons were involved in these activities. In addition, the startups also included security in several steps of the development process and all startups also had some basic guidelines for security.

This section will not evaluate the quality of the practices and give advice to whether the practice itself could be considered as good enough for the security in the corresponding startup.

### 5.2.1 Organizational aspect

From the organizational aspect hypothesis 1 *Startup has a distribution of responsibilities and roles related to security* found that all startups had one main person responsible for the information security in the startup. The ISO 27001 [45] presents a framework for making a security management program and emphasizes the need to understand context, the organization and have different roles. Even though the startups did not have so strict role definitions as stated in ISO27001, they had a main person responsible and several persons involved. Hence, a distribution of the responsibility was evident. Startup A had for instance the CTO as the main responsible person regarding security, and he was hands on with the developers and teaching them to write quality code, while another from the marketing team was responsible for the less technical tasks such as creating the privacy policy and tasks relevant for being GDPR compliant. A similar distribution of tasks was also found in startup D. Here, there were the developers who were responsible for the code quality, while the interviewee being the data protection officer was working together with a lawyer on issues related to privacy and being GDPR compliant.

Startup C also had divided the tasks, and the DPO (Data protection officer) was responsible for the GDPR and security management and the developers were consulted for the technical considerations. It is not known whether it was the same sort of distribution for startup B, here the interviewee only reported that GDPR was important and they follow laws and regulations, but it was not expressed explicitly that they had different persons working with the privacy policies then the developers.

That all startups had several persons involved can suggest that several persons can involve security activities where they see them fit. Focusing on agile development and implementation of security activities has shown that it was necessary that every person in the project is involved in the security activities [27]. However, it can be speculated that if there are several persons involved as in the startups interviewed, that they can influence the others in the team as well.

Even though the startups have not stated that they have this policy and those practices in a structured and documented manner, the interviews showed that they had minor parts of these, or some related as stated in the background 2.1. Having a distribution of roles related to responsibility of information security was apparently experienced as important for all startups. However, distribution of roles could be more formalized and standardized as suggested by several guidelines [45] + flere. On the other hand, this may not be directly applicable in startups.

In the results from hypothesis 2 *Only one person in the startup is seeking information regarding security* it was found in table 4.2 #6 and #7 that the startups C and D used external parties. Startup C communicated that they seek persons who

knows the specific area in question rather than always seeking the information themselves. This could be a result of few resources since the startup had few employees. Similarly, Startup D also used external parties as presented in #7. In addition to the startup making a product that can include sensitive information resulting in taking in external persons to help with security activities.

Startups may be characterized by lack of resources [3], which can explain why they can seek external help instead of employing a security professional full time. In addition, the factor of involvement of a security expert in a project when implementing a secure software development practice was found to be an important factor [35]. Thus, when needing human resources for information security, seeking external help can be an approach.

The importance of developers skills and earlier experience was highlighted in hypothesis 3 *There is a requirement that you learn a lot yourself.* The startups presented that both earlier experience and that you can learn yourself was important for them. This also corresponds to an important factor when implementing a secure software development system were the factor *developer's skill, experience and knowledge* [35] as the most important factor. Thus, it is likely that this is not a startup specific characteristic.

In conclusion, for all the startups there were more than one person working with security, and they had a main person for security. In addition, there were different roles regarding security, and most, if not all, had divided responsibility between different persons regarding the technical and less technical tasks. In addition, they could engage external parties in their work.

### 5.2.2 Including security in the development process

Hypothesis 4 *Startups take steps to secure their product in several stages of a development process* resulted in several best practices for how they include security in the development process for their product. A development process can include different steps. However, to make it clear which part of the process that is being discussed for different security activities, the startups mentioned are connected to the development process from the Norwegian Data Protection Authority [53] consisting of *training, requirements, design, coding, testing, release and maintenance* 4.1.

The interview revealed that all startups had some thoughts and activities attributed to several stages of the development process, resulting in the hypothesis being confirmed. However, this hypothesis may have only included two activities in total, it may have been too easy to approve, since the statements could only include a similar theme to one of many steps in the corresponding guides. In addition, it is difficult to say that the steps and activities they presented were done every

time they were at that stage in the development process. The results differ slightly from previous research in this area, such as the research by Søhoel [16] that stated that startups did not have a systematic approach to ensure information security. Again this emphasizes the need for a systematic approach and guidelines involving information security practices in startups.

All startups reported how they have some activities for training the employees, as shown in in table 4.4 #1-4. Training of employees is also mentions of several of the guides and frameworks [45] [47] [53] [26]. However, training was not clearly described in the guides for smaller businesses [24] [50]. One of these states *help your staff cope with password overload* [24] without giving other specific examples of training. It could be suggested that there is a need to develop better training opportunities for personnel in startups. Who was involved in the training differed between startups. In startup A the CTO presented that he often sat down with the developers and taught them about different non-functional requirements including security. However, it is unknown if more people were involved and taught each other different principles. Hence, there was no organized training for the developers, but more an ad-hoc approach to the training. Risks with an ad-hoc approach may be that it is random which practices are taught and not, leading to uncertainty. At the same time, an ad-hoc approach can be specified for the actual need at the moment. The reported ad-hoc approach to training, calls for further attention to initiate platforms and activities for training startups personnel in information security.

This also seemed to be the case in Startup C as is presented in table 4.4 #3 the interviewee reported information about their awareness training. In contrast to Startup A, startup C's interviewee was a non-technical person. Thus, it is difficult to state whether the interviewee did not mention technical training because there were none, or because the interviewee was not involved in the developers training.

Startup D presented that they had a discussion fora where they could include security training. As stated in table 4.4 #4 they could have morning meeting and include different security topics. Interestingly, startup D also presented that their management were much involved in the security activities, and the interviewee presented in table 4.7 #15 that the once who had been working there for a long time cared about security and that they were role models. Startup B also had a discussion fora where one could address different technical topics as presented in table 4.1 #5. However, the interviewee had not attended such a meeting with the topic security. Still, there existed such a fora where one could potentially address security topics for discussion, and it could be used for training.

Regarding the steps in the development process, including requirements and design the startups had some different motivations to include security. While startup

A and B talked about that it was in general important that they followed the different laws and regulations which could affect the different requirements, startup C explicitly stated that every time they presented to make a change that could have a impact regarding information security they had to do a *risk and vulnerability analysis* which was required by their customer, as presented in table 4.4 #5-8. Comparatively, startup D also working with sensitive data stated that when planning for development they had to do research and also look at what were security requirements in the potentially new domain. This could imply that how they work with security in the requirement phase may be affected by the type of product they develop. This finding suggests that type of startup may influence how the startup actually addresses security issues, which needs to be taken into account when developing startup specific guidelines.

During the coding phase of the development process the startups had many thoughts about what they did regarding security as presented in table 4.4 #12-15. This phase also includes different approaches for having secure code such as choosing the right tools and processes [53]. Startup B talked about what different security tasks could be, startup A about their use of known frameworks and tools and startup D about their communication solution. Startup C, on the other hand, talked about security requirements and how their solution could not be tampered with. This was a result of how their product was made, and may say something about that the developers thought about security while coding. However, startup C did not explicitly talk about what the developers thought about when being in the coding phase. This might be a result of the fact that the interviewee did not have a technical background, and therefore talked about the process from its own perspective. Hence, it is not clear how the developers in startup C include security in the coding phase.

As Søhoel found in [16] some startups focused on security, and the ones that did not have so much focus had more severe security holes that needed to be fixed than those with more focus. She tested security in startups by using the top 10 vulnerabilities from OWASP [32], thus applying a more technical approach and actually testing how some startups were secure against common vulnerabilities, in contrast to the exploratory and descriptive approach of the present study. In the present thesis, it is unknown what startups security practices regarding secure coding were. Furthermore, since the startup in this thesis did not include a technical test it is unknown if the startup might have severe security holes as reported in Søhoels study [16].

For the release phase startups A and B mentioned the practice of code review 4.4 #20-21. This activity is also mentioned in the literature [31] as being one of the most used security activities for agile teams, where other from the team read through the code and comment on parts. When measuring security, code review is one of

the activities in BSIMM [51]. According to BSIMM one can devide a code review in several levels, and on level 1 one finds approaches such as *ad hoc review* and *Make code review mandatory for all projects* [54]. The startups had some similarities with these practices. However, as BSIMM is a measurement for measuring security for businesses and then comparing the results, it would be more interesting to test these specific activities and ways to perform them on several startups.

For the last part of the development process, the maintenance phase there were few statements that stated similar security practices. There might be several reasons for this. First this may be a results of not specifically asking about this stage. In the interview is was asked about if they had a development process and what it included, and then where security might be involved as shown in Appendix C. However, the other phases were not explicitly asked about, but were still mentioned in most interviews. With this in mind one may suggest that the maintenance phase received less focus than the other phases when talking about the development process. Moreover, the maintenance phase is highlighted as important in several guides and frameworks [45] [46] [51] [53]. A stronger focus on the maintenance phase could be suggested for future guidelines for information security in startups.

Regarding the development process, all startups followed more or less a agile development process for their product, with several iterations of their product. Startup D used the guidelines from the guide *Software development with Data Protection by Design and by Default* by The Norwegian Data Protection Authority [53]. Earlier research has suggested that agile is not easily adaptable with non-functional requirements such as security requirements [29]. However, even though it can be difficult, research has suggested that teams can integrate parts of security activities into their process [27]. This study found some similar results, the startups managed to involve steps regarding security in different steps of this process. It can be suggested that further inclusion of security practices in startups can be included through already existing process or activities. Moreover, startups can learn from each other how one can include these security activities, further suggesting the importance for arenas on which to share knowledge. However, this warrants further research about what a best practices for process in startups and following what should be included for security practices.

### 5.2.3 Basic guidelines for security

In hypothesis 8 the startups received yes/no questions with different security practices. All startups did at least two of the practices asked about. However, there were large variations towards what they did. All startups had routines for backup and access management, as shown in table 4.8.

How the practices are complied with was not answered through these questions.

The questions directed toward whether they have a practice, did not specify what was meant by practice. Furthermore, the questions did not take account for whether one startup had specified this practice in a written guideline or not. Hence, one startup may consider a common practice which is not written as a practice, while another might not. Subsequently, the answers may not be directly comparable. In addition, phrasing of the questions might also affect how the interviewee responded to the questions, and some questions could not easily answered with a strict yes or no answer. Conversely, one could say as a minimum that the startups having a positive response to the questions had some routines towards this topic.

There was also one practice that none of the startups had routines about and that was the question about whether they had guidelines towards the use of USB sticks. For all other guidelines at least two startups did the practice in question, but not for the USB practice. This practice was specifically included in guides for SMEs4.1. The guideline about USB can be considered as a very specific tips concerning "to do actions", rather then the more overall approach typical for other guides. This finding in the SME guides indicates that these guides for SMEs may include important tips for future information security guidelines for startups.

In some cases the startup showed variations, as in the guidelines about whether or not they had "asset management" and the guideline about "automated security tests". Startups C and D had similar answers regarding "asset management" and "automated security tests", and had both these guidelines implemented. As found in the guide by the Norwegian Data Protection Authority [53] - the Data protection by design and default these are guidelines corresponding to GDPR, and in order to be GDPR compliant when handling sensitive data they need to have these guideline in place.

In brief, all startups followed some guidelines from the checklist, but due to inaccurate definition of what is needed to be in place for it to be termed a practice, the results may not be reliable.

## 5.3 Research question 3: What motivational factors for information security are found among startups?

In this section, the different aspects of the motivational factors for working with security found in startups will be discussed in order to answer research question 3. Hypotheses 5, 6 and 7 explored different motivational factors for why startups worked with security.

Previous research have suggested that motivation is important for information security [18]. This was confirmed by the present study where internal and external

motivational factors seemed to be relevant for information security in startups. Several internal and external motivational factors were identifies through hypotheses 5, 6 and 7. Examples of external factors mentioned such as risks for startups. All startups said during the interviews that they were aware of risks, as presented in table 4.5 #14. However, while Startup C performed a risk analysis every time they developed something that needed it, startup D expressed concerns about risks and that they could not afford a major incident concerning information security. Startup A, had addressed the issue of safety when talking about risk. This might be affected by them producing a physical product. Startup B stated that they had an evaluation and could discuss matters regarding security risks. However, if was not always they first priority, but rather if they discussed and found out it could be a potential problem then they addressed it. This is corresponding to previous research which has found that for most companies using agile development, functionality was more important than security [27]. There might be other factors regarding whether the startups addressed risks or work with risk in a structured matter. Startup A and C had interviewees on a management level, and they also talked about their startup having an overall view of risks. Furthermore, the interviewee in startup D had worked with privacy and an external lawyer to help their startup work with privacy. In contrast, the interviewee in startups B worked with one part of their product and as stated in table 4.4 #13 talked more about product security when coding. However, having direct questions about risks may have affected how the startups answered. Additionally, risks are a general term, and may include other topics than security.

Through the interviews all startups expressed that they were concerned about their customers and that their requirements and trust was important. This was shown in table 4.6. All startups felt like they had to prove something for their customers, and that they could not afford to make any mistakes. As startup A stated in #1 *"we want to be taken seriously, as a new startup that do not have a large track record and so much trust."*. Startup B also expressed this concern that if their startup could be something they could not do any mistakes regarding security. Furthermore, he elaborated on that they had a responsibility towards their customers to handle their data right. Startup C also addressed the issue of responsibility in statement #3, but focused on it being more a social responsibility. This might be affected by the fact that even though their customer is buying their product, the end users are someone else. It seemed like the statement about their social responsibility was aimed towards the end user and the data that they had. Correspondingly, startup D also expressed that their end costumer was important. Interestingly, both startup C and D handled sensitive data for their end users, and this might also be why they addressed the issue of responsibility, not only towards their customer, but also end user.

Interestingly, many of the motivational factors found during the interviews were not only external motivational factors, but also internal. In table 4.7 the factors are

presented, and #5-7 includes statement were interviewees talked about their own reasons for wanting a good product. This was also found in a study for non-functional requirements in agile which identified that the practice *work with a quality mindset* could be a factor for better handling of information security in agile [29]. Startup A expressed that when making the product their own integrity was a motivational factor, because they wanted to make their product properly. Moreover, startup B also mentioned that there were a pride in making a good product, and the he did not like to make things that were not good. Likewise, startup D also mentioned that there was a common attitude towards making secure and safe products and that the developers care. Developers attitude and motivation was also stated as an important influencing factor in prior research [35], and a study has also suggested that employees in startups might have motivation for making secure products [36]. This corresponds to the interviews which seem like the employees in startups have strong feeling towards making good products, not only for their customers, but also for their own conscience.

Taken together, both internal and external motivational factors were found in the startups related to why they implement security activities. One can suggest that startups and companies knowing what their motivational factors are can also have implications for how they work with security, as suggested by earlier research comparing startups and freelancers [36]. Furthermore, they might focus on different aspect if only have external motivational factors. With the startups communicating that security was important for them and identifying internal motivational factors one can speculate that there could be a need for a tailormade security activities also focusing on this internal motivation.

## 5.4 Contextual considerations for interviews

In data collections there are pitfalls which may be due to environmental variations [40]. This section will examine some factors which may have affected the results from the interviews.

The background and role in startup of the interviewee may affect the answers from the different startup. From startup A and B technical persons were interviewed, one was CTO and the other was a developer. This resulted in more focus on technical measures. For instance when asked about the development process is was more focus on the technical measures such as how they used code review and git when developing. Startup C and D had more focus on privacy and organizational matters such as a privacy policy and risks.

Interestingly, the results clearly demonstrated that there are large variations on what the startups did regarding information security, and the type of the startup

can have affected how they work on security related issues. Startup C presented a whole security management framework and did almost all of the measures in the checklist (found in hypothesis 8). Startup D also had a focus on privacy by design and had several measures involved. Startup C and D did have some similarities, they were both in the health sector and both represented with their data protection officer. Hence, the startups sector or field of work may be a influencing factor when analysing how they work with security. Although the study did not evaluate what was sufficient security, it could be suggested that there is a need for tailor-made guides for different types of startups and startup sectors. It could for instance be suggested that tailormade guidelines specifically targeted at e.g. the health sector is needed.

The size of the startup varied. While one was less than 10 employees, others were 50-100 employees. The startups therefore had a very different structure with the larger ones having "subteams" as large as the smaller startup. This resulted in different solutions for taking part of the security work. While the smaller startups could have one to one conversations about security, the larger one had different arenas for addressing security. Startup B and D had more official fora for discussion were issues such as issues related to security could be discussed. Then the relevant persons could attend these discussions. For the smaller startups such an arena was not presented. Since knowledge transfer and training regarding security issues was highlighted by all startups, it is apparent that startups may benefit from group discussions, and it could be suggested that at least smaller startups need arenas or fora to meet and discuss. Although the startups specifically mentioned training only within their own startup, it could be suggested that there is a need for better knowledge transfer also between startups. Therefore, a discussion forum where startups can learn from others' experiences with the goal to improve best practices for information security in Norwegian startups would be beneficial.

In summary, three main contextual considerations may have affected the results. These were the interviewees background and role, the type of startup and the size of the startup. The need for better knowledge transfer in highlighted.

## 5.5 Methodological considerations and limitations

Using a review of literature and qualitative interviews has its advantages and disadvantages. This section will discuss the different methods and their corresponding advantages and disadvantages, in addition to present different limitations to the study.

Since there was little prior research in the field of security in startups, this case study was a exploratory case study [40]. An exploratory approach is often a preferred

method and chosen when *there is little to guide what one should be looking for, then your initial approach will be highly flexible* [40], and was therefore concluded to be a relevant method for the present study. With the goal of the study being exploring what are information security practices used today, and not if the startups were acting securely or not the interview guided needed to include some open questions. In contrast, a confirmatory study would have been confirming a theory based on previous exploratory results. With this being an exploratory case study, this affected the data selection. According to Robson, there is a tradeoff between selectivity and looseness of the data selection, which is affected when it is a exploratory case study [40]. As mention in the section about analysis, the whole interview needed to be transcribed. An advantage of this approach is that the one is open for new views and not blind to other views and results not directly connected to what one is confirming. However, anything might be important resulting in needing more time to filter out the results later.

There were difficulties in narrowing the research topic security in startup since this is such an unexplored topic. There was little research in this field, and the only paper found on security in startups [16] suggested that startups had little focus on security. So, the present study attempted to explore the field of security practices in startups using an exploratory approach. Hence, the exploratory case study was chosen [40].

Having an exploratory approach an important aspect for the research questions and hypotheses were to explore what they considered important, and not narrow down the topics. However, using hypotheses might also have narrowed conclusions for the results. In retrospective, the hypotheses might have a more negative view of what is expected then the security practices found in startups. While the startups in general were found to have a positive view and several thoughts and activities regarding security, the hypotheses were for instance *Startups are aware of risk and their risk appetite* and might be to vague and many answers could be considered relevant. Hence, having hypotheses might not be an optimal solution for identifying different nuances between the different startups. This might be an interesting approach when studying security practices in startups.

The startups interviewed were selected through some criteria that might be relevant for if the startups had some considerations about security. If this had been a confirmatory study with the goal to evaluate their security practices, a strategic selection would not have been appropriate. However, with this being an exploratory study to find some security practices used in startups, a strategic selection was considered appropriate. However, as stated in [1] strategic selection can be used to find respondents that can give reflective statements about a chosen topic.

Important considerations were that the researcher did not have a closed and prejudged view when deciding on the topic, since this is likely to affect the objectivity and trustworthiness of the research [40]. However, the researcher herself also brought views and own experiences to the research, so the way the research was conducted partly depended on the researcher, at least indirectly. Moreover, the research topic was also inspired from own direct experience, observation or discussions with others [40].

Having these open questions had their advantages and disadvantages. The goal of having such an approach was that all varieties could be explored during the interviews. This also affected the interview guide with having open questions and giving room for the startups to talk about what they did. Advantages with these open questions such as "do you have a development process" and then the follow up question "in the different steps of this process, do you include security?". The startups then got to talk about how they worked and did not get the question "do you think about security when coding?". With having open questions the startup may have been less affected by the interviewers' questions than if the interviewer had asked more direct questions. For future studies one can further explore practices found in this current study in a confirmatory way.

There are several challenges with using open questions in an interview guide [40]. First of all, with this approach the startups themselves decided what to talk about and present. When asked about their process they could talk about the areas they knew they actually did something, and may not present all steps of the development process. This may also affect the reliability of the results [40]. So, one does not necessarily get a full overall pictures of all the activities they do and in which they do not include security and thereby what are practices for information security. This issue was addressed in the interview guide through the use of follow up questions. These questions could be a summary of what the interviewee had answered as presented in4.3. This could lead to the interviewee being aware of what he/she had actually said, and the interviewee might add to its answer. However, asking good follow up questions needs a good interviewer [40], and not all questions had a follow up question to get instant response if the answer was analysed correctly.

The interviewers skill can also affect the results [40], and the interviews in the present thesis was conducted by only one interviewer. A better approach would have been to use two interviewers and reseachers to interview and transcribe in order to make the results more realiable [41]. The interviewers could compare notes, ask relevant follow up questions and make sure they agree on what was said in the interview. In addition, some interviews did not have perfect recorded sound, as shown in table . Some words were hard to identify, and this may affect the reliability of the results. Also regarding the interviewers, it might have been better to have two

interviewers in order to ask the right follow up questions and noticing when a follow up questions is needed. This was more difficult when being just one interviewer and having open questions.

Another disadvantage with interviews in general is that the interviewee might present that they do more then they actually do, affecting the validity of the results. Here, follow up questions asking "how they do this" and "why they do this" is important in order to find out if they actually do. Follow up questions were used to some extent to clarify what the interviewee meant.

Open questions also made if difficult to get very specific answers to the questions, this is a common disadvantage of open questions and also can make it more difficult to analyse [40]. Resulting in that one cannot directly compare the different startups since they have talked about different things in the interviews. Therefore the results are presented as subjects and trying to find themes that are in common. However, these results in giving the analyser much "power" and the results might therefore be biased of the analysers opinion [40].

Using interviews to ask about security practices is a method that is highly subject to subjective perceptions. Furthermore, the results are sensitive to subjective biases [40]. The risk of having the interviewee talking about what he or she wanted and therefore steer the conversation in what security activities they were actually doing was to use a checklist at the end of the interview. This checklist corresponding to hypothesis 8 was suppose to be answered as yes or no. However, some of the answers were that they were partially doing it. This method had the advantage that the interviewee was "forced" to answer short, and could in theory not steer the conversation on other topics. These questions can be categorized as *Direct questions* [41] and if not giving a specific answered was followed up with a *interperative question* [41] in order to get a specific answer. Several of the answers were that they did not do the different practices. For the first part of the interview they focused on what they were doing, but for this part they had a checklist which all interviewees had to answer the exact same answer, making the results more comparable. However, the questions turned out to not have strict yes or no answers. If they gave long answers they received follow up questions on order to formulate their answers as yes or no. This could have been avoided if the questions had been tested prior to the interviews using a test panel.

Ideally, more startups could have been included in the study, this in order to increase the trustworthiness of the study [40]. Only four startups were included in this study due to time and resource limitations. However, as presented in the Methodology 3, 3-5 startups can be projected as efficient in order to answer the research questions, as they did not require representative results. Disadvantages with

a small number of interviewees is according to Kvale [41] that it is not possible to conduct statistical generalisations or testing hypotheses about differences between different groups.

## 5.6 Suggestion for prototypes

The prototypes from section 4.4 were based on what startups presented in the interviews, and are suggestions for what could be done in the future to help startups improve their work with information security. However, these have not been validated by any means, and only represent suggestions.

Including motivational factors for motivation for future guidelines (4.4.1) have not been seen in the guides in the review. One can speculate that startups could find this relevant, and it might also inspire startups to include security when reading that other startups are motivated by their wish to make good products that they are proud of.

Including organizational aspects in guides were not found in the UK guides for SMEs [24] [25]. However, included in the NorSIS guide were ten recommended practices for companies starting with security as first presented by the Government in Norway[49], with one measure stating *Establish sufficient systematics for security management, and make sure that an expert in the field supports the management in this work.* [17]. The interviews identified that the startups typically had established some elements of systematics for security management, and made sure that a person (internal in the management or external expert) supported the management in security issues. It could therefore be suggested that this guideline has the potential of being a best practice, and should be further included in a guide to improve security in startups.

All startups included security in different stages of the development process, and one startup mentioned that they used the guidelines from the Norwegian Data Protection Authority [53]. It was therefore suggested that future guidelines should also include this practice. An future studies can further investigate what could be included in the different stages in the development process relevant for startups.

The startups all presented different ways of communicating security training and awareness to the employees, and prototype 2 4.4.2 addresses this need. While some had one-to-one tutoring about security practices, others had meetings where one could address security related issues. Different aspects of training and awareness was addressed in all frameworks and guides from the review [45] [26] [24] [50] [53] [51]. One startup emphasized that security was a part of their culture in the startup. The Norwegian Cyber Strategy has also expressed a need for a security culture

as the following practice *Map the companies security culture and identify what can be improved. Define the desired culture and carry out adapted annual training programmes to promote appropriate security culture.*[17]. One can speculate that if one can integrate security as important in the startups in Norway, making it a part of their culture to care about it, then one could improve security for existing and future startups. There are several challenges when discussing creating a security culture; startups are characterized with having lack of time and resources, focus on releasing functional requirements, earlier experience is important, culture change might take time and it is unknown what is a good security culture for startups. Prototype 2 suggests that one could create a platform for sharing security practices for information security specifically aimed for startups. One could further suggest that one could use profiled Norwegian startups for sharing some security practices, motivating smaller startups to focus on security. As mentioned in section 4.4.2, aspects important to consider would be to make it specific and relevant for startups and startups being able to share their security practices. In addition, learning from each others mistakes could be useful and may prevent other startups from making the same mistakes. One could further suggest that sharing negative related experiences could be of importance for startups.

## 5.7 Future knowledge needs

For future studies it would be very interesting to explore many aspects related to information security in startups in more detail. This was an initial exploratory case study, and has identified interesting aspects regarding security in startups. These initial findings opens up for future research necessary to improve information security in startups. In order to develop science based guidelines and recommendations for best practice for information security targeted at startups, several lines of research can be suggested:

**How to differentiate startups:** Results from this study indicated that the startups context and sector is important for their implementation of security measures, more than their number of employees. Thus, it would be interesting to identify factors that influence their security implementation, which has implications for future guidelines for security in startups. This in order to being able to develop tailor made guides for different kinds of startups.

**Comparing startups and businesses** and find out if there are things that actually differentiate them. In this study some aspects were highlighted from the startups point of view. They said things about not having enough resources and time for security activities, and that they had less bureaucracy and were less hierarchical than other non-startups. Further research is needed in order to

address this issue and identify what are different obstacles that different types of organizations experience that could affect their development of guidelines.

**Motivational factors for startups vs businesses** Testing motivational factors in two different organizational structures and see if there are similarities. This is order identify in more details motivational factors that are relevant for the implementation of information security recommendations. This could be done in interviews with the possibility of asking follow up question.

**Quantitative studies** of what security practices are present in startups would be interesting. If done on a quantitative level and larger scale one could get a representative sample and therefore be able to find out what is general security practices in the industry. The topics identified in the present thesis could aid to the development of a quantitative questionnaire needed in such a study.

**Development and testing of security guide for startups** would be very interesting to conduct and test out. During this study some interesting aspects and suggestions for prototypes were presented, and it would be interesting to further develop these and validate on startups.

**Action research** implementing and testing the effect of implemented security activities would be very interesting. Then one could actually evaluate how the specific activities would be received and what would be desired or unwanted consequences of this implementation.

**Action research** with the goal of testing out and further develop a information security guide for Norwegian startups. This could be done with the basis in the prototype presented in this thesis, and develop this further into a working guide. This guide could be tested on startups in the very beginning, such as the once at NTNU School of Entrepreneurship.

## 5.8 Future perspectives

The development of business ideas and forming these into a successful startup and later successful business may change entire sectors. Threats emerging from new technologies paired with poor information security practices in these businesses may be detrimental for their success. This thesis revealed that information security to some extent is taken seriously by startups, but there is a lack of a systematic approach, making the startups vulnerable to cyberattacks and data breaches. It is suggested that the development of applicable and guidelines or frameworks for information security tailor made for startups could contribute to a more systematic approach to better information security, thereby reducing vulnerability to e.g. cyberattacks and, hence, reduce the risk to loose good business ideas and costs connected with potential attacks. Therefore, the creation of security guidelines based on e.g. the

prototype suggestions in this thesis, and taking into account the motivational aspects of including security measures, could be crucial for the survival and success of a startup.

The interviews suggested that group activities and fora could be a practical solution to improve information security at least in the smaller startups with less budget and personnel. Based on the lack of systematic activity towards information security in startups today, paired with the growing need for secure solutions worldwide, and the apparent need for specially designed security solutions depending on the startups product and way of working, suggests that there may be huge business opportunities to produce tailor made security solutions for startups. This could for instance involve the development of applicable guidelines for individual startups, and promoting and organizing platforms and fora for training and sharing. It is likely that the implementation of valid security guidelines or frameworks could be used as an added value and for marketing purposes to sell products (as seen from adverts by Telia[1]), which may result in an added value for a variety of startup-businesses. A systematic approach to the field of information security in startups is of utmost importance, both for Norwegian industry and industry worldwide.

[1] Telia advertisement for secure internet solutions for SME http://presse.telia.no/pressreleases/telia-lanserer-sikkert-internett-en-verdensnyhet-for-smaa-og-mellomstore-bedrifter-2850127

# Chapter 6
# Conclusion

In this case study of information security in startup was explored. Previous research have identified information security practices in development processes, investigated how SMEs work with information security or have taken a technical approach to test some startup against known vulnerabilities. However, few studies have focused on startups in the context of information security. In particular, systematic information about how different Norwegian startups work with information security on an overall and specific level. In addition, previous studies have found that motivational factors can be of importance for the implementations of information security measures in organization. However, there has not been research on motivational factors for information security in startups. This study has explored what motivational factors are found for information security.

This exploratory case study used a review of frameworks and guide in addition to semistructured interview answered three research questions. First research question 1 *What are some existing knowledge and frameworks regarding information security with the potential of being relevant for Norwegian startups?* found out through a review that there were none frameworks specifically made for startups, and the relevant guides often focused on technical measures. However, the entire guides were not covering all topics reported as important by the startups. Much of their practical day to day work covered some of the important aspects mentioned in the guidelines or frameworks. Based on both existing guidelines and interview results from startups it was therefore suggested a prototype for work with future guidelines for information security specifically for startups. These future guidelines could be defined as best practices for information security practices in startups.

Research question 2 *What existing information security practices are found in Norwegian startups?* found through semi-structured interviews that there were several practices that startups did. The interviews identified that the startups typically had established some elements of systematics for security management, and made sure that a person (internal in the management or external expert) supported the

management in security issues. Interestingly, two of the startups also had external security personnel involved in their work. In addition, training and awareness around information security was of importance, but the startups varied in how the training of employees was conducted.

Research question 3 *What motivational factors for information security are found among startup?* identified, through semi-structured interviews, motivational factor for information security in startups. This study found that external factors (e.g. GDPR fines, reputational damage and customers trust), as well as internal motivational factors (e.g. entrepreneurial spirit,a belief in the product they are making) play important roles for how startups are working with security. Importantly, the employees' motivational factors need to be taken into account when developing new guidelines.

This thesis has brought some light to the little researched field of information security in startup. In addition, new technology and innovation are accompanied by new threats. The results indicate that there is a need for future studies. Hopefully, this study and futures studies in the field can identify and reduce vulnerabilities related to information security for existing and future startups.

# References


[1] A. Tjora, *Kvalitative forskningsmetoder i praksis*. Gyldendal, 2nd ed ed., 2012. Previous ed.: 2010.

[2] N. Levy, "Charts: Tech giants apple, google, microsoft, amazon and facebook are world's most valuable companies." https://www.geekwire.com/2017/charts-tech-giants-apple-google-microsoft-amazon-facebook-worlds-valuable-companies/.

[3] T. A. H. Tim Torvatn, Monica Rolfsen and R. Sørheim, *Teknologiledelse for ingeniørstudenter*. Kanalveien 51, Bergen, Norway: Fagbokforlaget, first edition ed., 2016.

[4] S. Blank, "What's a startup? first principles.." https://steveblank.com/2010/01/25/whats-a-startup-first-principles/.

[5] S. M. Sutton, "The role of process in software start-up," *IEEE Software*, vol. 17, pp. 33–39, July 2000.

[6] N. Robehmed, "What is a startup." https://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/.

[7] N. Murray, "The Norwegian h1 2018 (q1 and q2) funding analysis," *The Nordic web*, vol. 1, Aug. 2018. Accessed: 2018-10-10.

[8] P.-I. Nikolaisen, "Digitalministeren vil få det offentlige til å kjøpe av startups: «pisk og gulrot er det som skal til»." https://shifter.no/digitalministeren-vil-fa-det-offentlige-til-a-kjope-av-startups-pisk-og-gulrot-er-det-som-skal-til/.

[9] N. sikkerhetsråd, "Mørketallsundersøkelsen 2018: Informasjonssikkerhet, personvern og datakriminalitet," tech. rep., 01 2018.

[10] M. Team, "Customer guidance for wannacrypt attacks." https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

[11] R. Future, "Apt10 targeted norwegian msp and us companies in sustained campaign." https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf.

[12] N. Sikkerhetsmyndighet, "Innbrudd i datasystemene til helse sør-Øst." https://www.nsm.stat.no/aktuelt/datainnbrudd-helse-sor-ost/.

[13] S. Technologies, "Cybersecurity mistakes all small business employees make." https://lp.switchfast.com/smb-cybersecurity-report, 11 2018. Accessed: 2018-11-27.

[14] Cisco, "How small and midmarket businesses can fortify their defenses against todays threats." https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf.

[15] D. D. Cruzes, "Science of security for agile software development." https://www.sintef.no/en/digital/sos-agile-blog/aboutsos/.

[16] H. M. Søhoel, "Owasp top ten - what is the state of practice among start-ups," *NTNU master thesis*, p. 94, 2018.

[17] N. G. Security and S. Organisation, "National cyber security strategy for norway." https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.

[18] J. Stanton, P. Mastrangelo, K. Stam, and J. Jolton, "Behavioral information security: Two end user survey studies of motivation and security practices.," p. 175, 01 2004.

[19] M. E. Whitman and H. J. Mattord, *Management of information security.* 20 Channel Center Street, Boston, USA: Cengage Learning, fifth edition ed., 2017.

[20] E. Ries, *The lean startup how today's entrepreneurs use continuous innovation to create radically successful businesses.* New York : Crown Business, 2017.

[21] M. Beedle and colleagues, "Principles behind the agile manifesto." https://agilemanifesto.org/principles.html. Event date : 2018-08-24.

[22] E. Commision, "What is an sme?." https://web.archive.org/web/20150208090338/http://ec.europa.eu/enterprise/policies/sme/factsfiguresanalysis/sme-definition/index_en.htm.

[23] K. Renaud, "How smaller businesses struggle with security advice," *Computer Fraud & Security*, vol. 2016, no. 8, pp. 10 – 18, 2016.

[24] T. N. C. S. C. UK, "Cyber security: small business guide." https://ncsc-content.s3.eu-west-1.amazonaws.com/cyber_security_small_business_guide_1.3..pdf. Accessed: 2019-01-30.

[25] T. N. C. S. C. UK, "About the ncsc." https://www.ncsc.gov.uk/section/about-ncsc/what-we-do. Accessed: 2019-02-15.

[26] NorSIS, "Sikkerhet for bedrifter." https://nettvett.no/kurs/sikkerhet-for-bedrifter/. Accessed: 2019-01-20.

[27] S. R. L. M. B. J. M. G. Nicolaysen, T., "Agile software development: The straight and narrow path to secure software?," *International Journal of Secure Software Engineering (IJSSE), 1(3), 71-85*, p. 15, 2010.

[28] S. alliance, "What is scrum." https://www.scrumalliance.org/. Accessed: 2018-11-17.

[29] C. R. Camacho, S. Marczak, and D. S. Cruzes, "Agile team members perceptions on non-functional testing: Influencing factors from an empirical study," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 582–589, Aug 2016.

[30] D. Baca, M. Boldt, B. Carlsson, and A. Jacobsson, "A novel security-enhanced agile software development process applied in an industrial setting," in *2015 10th International Conference on Availability, Reliability and Security*, pp. 11–19, Aug 2015.

[31] T. D. Oyetoyan, M. G. Jaatun, and D. S. Cruzes, "A lightweight measurement of software security skills, usage and training needs in agile teams," *Int. J. Secur. Softw. Eng.*, vol. 8, pp. 1–27, Jan. 2017.

[32] OWASP, "About the open web application security project." https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project. Accessed: 2018-10-25.

[33] OWASP, "Owasp application security verification standard." https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Accessed: 2018-10-25.

[34] R. M. Ryan and E. L. Deci, "Intrinsic and extrinsic motivations: Classic definitions and new directions," *Contemporary Educational Psychology*, vol. 25, no. 1, pp. 54 – 67, 2000.

[35] S. L. Kanniah and M. N. Mahrin, "A review on factors influencing implementation of secure software development practices," *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 10, no. 8, pp. 3032 – 3039, 2016.

[36] J. Bau, F. Wang, E. Bursztein, P. Mutchler, and J. C. Mitchell, "Vulnerability factors in new web applications: Audit tools, developer selection & languages," *Stanford, Tech. Rep*, 2012.

[37] Z. Xian (Sean) Ng, A. Ahmad, and S. Maynard, "Information security management: Factors that influence security investments in smes," 12 2013.

[38] N. Tripathi, P. Seppänen, G. Boominathan, M. Oivo, and K. Liukkunen, "Insights into startup ecosystems through exploration of multi-vocal literature," *Information and Software Technology*, vol. 105, pp. 56 – 77, 2019.

[39] S. E. Chang and C.-S. Lin, "Exploring organizational culture for information security management," *Industrial Management and Data Systems*, vol. 107, pp. 438–458, 04 2007.

[40] C. Robson and .-a. McCartan, Kieran, *Real world research : a resource for users of social research methods in applied settings*. Chichester, West Sussex ; Hoboken, N.J. : Wiley-Blackwell, 4rd ed ed., 2016. Previous ed.: 2011.

[41] S. Kvale, *Det kvalitative forskningsintervju*. Gyldendal, 8th ed ed., 2006.

[42] N. Futsaeter, "Security in startups - a preproject," *NTNU Preproject*, pp. 1–10, 2018.

[43] R. J. Wieringa, *Design Science Methodology for Information Systems and Software Engineering*. Springer, 2014.

[44] NSD, "Norwegian privacy services for research data." http://www.nsd.uib.no/personvernombud/en/notify/meldeskjema?eng. Accessed: 2018-10-27.

[45] I. t. I. E. C. ISO (International Organization for Standardization), "Information technology — security techniques — information security management systems — requirements," standard, International Organization for Standardization, Geneva, CH, Oct. 2013.

[46] NSM, "Nasjonal sikkerhetsmyndighet." https://www.nsm.stat.no/english/. Accessed: 2019-01-21.

[47] Norsis, "Nsms grunnprinsipper for iktsikkerhet." https://nettvett.no/wp-content/uploads/sites/2/2019/01/Sikkerhet_for_bedrifter_-_Nasjonal_sikkerhetsmyndighets_grunnprinsipper_for_IKT-sikkerhet.pdf. Accessed: 2019-01-22.

[48] NorSIS, "The norwegian center for information security." https://norsis.no/english/. Accessed: 2019-01-15.

[49] NorSIS, "10 anbefalte tiltak." https://norsis.no/wp-content/uploads/2019/03/Sikkerhet_for_bedrifter_-_10_anbefalte_tiltak.pdf.

[50] T. N. C. S. C. UK, "Cyber security: small business guide actions." https://ncsc-content.s3.eu-west-1.amazonaws.com/small_business_guide_actions.pdf. Accessed: 2019-01-30.

[51] BSIMM, "Bsimm." https://www.bsimm.com/about.html. Accessed: 2019-01-25.

[52] E. Union, "Regulation (eu) 2016/679 of the european parliament and of the council." https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

[53] T. N. D. P. Authority, "Guide software development with data protection by design and by default." https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/. Accessed: 2019-01-23.

[54] BSIMM, "Bsimm code review." https://www.bsimm.com/framework/software-security-development-lifecycle/code-review.html.

Appendix A

# Research application to NSD

for behandling av personopplysninger.png for behandling av personopplysninger.png

NSD NORSK SENTER FOR FORSKNINGSDATA

**Meldeskjema 994362**

**Sist oppdatert**

28.01.2019

**Hvilke personopplysninger skal du behandle?**

---

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer

**Type opplysninger**

---

**Skal du behandle særlige kategorier personopplysninger eller personopplysninger om straffedommer eller lovovertredelser?**

Nei

**Prosjektinformasjon**

---

**Prosjekttittel**

Security in startups

**Begrunn behovet for å behandle personopplysningene**

For å følge opp intervjuobjektene trenger jeg å lagre deres navn og mailadresse til intervjuene er fullført. Deretter kan dette slettes. Navnene på startupsene vil også bli anonymisert i oppgaven.

**Ekstern finansiering**

**Type prosjekt**

Studentprosjekt, masterstudium

**Kontaktinformasjon, student**

Nora Futsæter, nora.futsaeter@gmail.com, tlf: 93269440

**Behandlingsansvar**

---

**Behandlingsansvarlig institusjon**

# for behandling av personopplysninger copy.png for behandling av personopplysninger copy.png

NTNU Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Karin Bernsmed, karin.bernsmed@sintef.no, tlf: 4748215585

**Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?**

Nei

**Utvalg 1**

---

**Beskriv utvalget**

Ansatte i startups

**Rekruttering eller trekking av utvalget**

Ble kjent med kontaktpersoner gjennom stands og startupevents.

**Alder**

18 - 62

**Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?**

Nei

**Personopplysninger for utvalg 1**

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer

**Hvordan samler du inn data fra utvalg 1?**

**Personlig intervju**

**Grunnlag for å behandle alminnelige kategorier av personopplysninger**

Samtykke (art. 6 nr. 1 bokstav a)

**Informasjon for utvalg 1**

**Informerer du utvalget om behandlingen av opplysningene?**

Ja

**Hvordan?**

Skriftlig informasjon (papir eller elektronisk)

**Tredjepersoner**

for behandling av personopplysninger copy 2.png for behandling av personopplysninger copy 2.png

---

**Skal du behandle personopplysninger om tredjepersoner?**

Nei

**Dokumentasjon**

---

**Hvordan dokumenteres samtykkene?**

- Manuelt (papir)

**Hvordan kan samtykket trekkes tilbake?**

Gjennom kontakt på mail eller tlf

**Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?**

Gjennom kontakt på mail eller tlf

**Totalt antall registrerte i prosjektet**

1-99

**Tillatelser**

---

**Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?**

**Behandling**

---

**Hvor behandles opplysningene?**

- Private enheter

**Hvem behandler/har tilgang til opplysningene?**

- Prosjektansvarlig
- Student (studentprosjekt)
- Interne medarbeidere

**Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?**

Nei

**Sikkerhet**

---

**Oppbevares personopplysningene atskilt fra øvrige data (kodenøkkel)?**

Ja

for behandling av personopplysninger copy 3.png for behandling av personopplysninger copy 3.png

**Hvilke tekniske og fysiske tiltak sikrer personopplysningene?**

- Opplysningene anonymiseres
- Opplysningene krypteres under forsendelse
- Opplysningen krypteres under lagring
- Endringslogg
- Flerfaktorautentisering
- Adgangsbegrensning
- Adgangslogg

**Varighet**

---

**Prosjektperiode**

11.01.2019 - 07.06.2019

**Skal data med personopplysninger oppbevares utover prosjektperioden?**

Nei, data vil bli oppbevart uten personopplysninger

**Hvilke anonymiseringstiltak vil bli foretatt?**

**Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?**

Nei

**Tilleggsopplysninger**

---

# Appendix B
# Information sheet

copy.png copy.png

## Vil du delta i forskningsprosjektet

## *"Security in startups"*?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se på hvordan startups jobber og kan jobbe med informasjonssikkerhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

**Formål**
Dette er en masteroppgave gjennom Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU. Masteroppgaven tar for seg spørsmålet om hvordan informasjonssikkerhet blir jobbet med i noen startups. Det overordnede målet med oppgaven er å se på hva som kan forbedre hvordan startups jobber med sikkerhet fremover. Derfor vil jeg se på hva som finnes i dag av måter å jobbe med informasjonssikkerhet. Her vil fokuset være på prosessene og arbeidsmåten startupsene jobber på, og deretter se om og hvordan de får inkludert sikkerhetstiltak.

Dette vil bli jobbet med gjennom å svare på følgende forskningsspørsmål
- Hva er best practices for informasjonssikkerhet som kunne vært relevante for startups?
- Hvilke best practices finnes for informasjonssikkerhet i noen norske startups?
- Hva kunne vært sikkerhet practices for norske startups?

Første forskningsspørsmål vil bli svart på gjennom en litteraturstudie av noen rammeverk og guider. Andre spørsmål vil bli besvart på gjennom intervju med noen startups. Basert på svarene her vil forsøke å lage et forslag til hva andre startups kan gjøre, og dermed besvare det siste forskningsspørsmålet.

**Hvem er ansvarlig for forskningsprosjektet?**
SINTEF og NTNU er ansvarlige for dette forskningsprosjektet.

**Hvorfor får du spørsmål om å delta?**
Prosjektet vil undersøke hvordan ulike startups jobber, og hva slags prosesser de bruker. Deretter vil jeg se på hvordan sikkerhetstiltak kan passe inn i disse prosessene. Derfor er det ønskelig at ansatte i startups deltar i denne studien. Jeg skal intervju 3-5 startups.

**Hva innebærer det for deg å delta?**
Dersom du velger å delta i prosjektet, innebærer det at du må delta på et intervju. Det vil ta ca. 1 time. Du må oppgi opplysninger om stilling, arbeidsoppgaver og arbeidsprosesser. I tillegg vil det være spørsmål knyttet til hvordan bedriften generelt jobber, og om ulike stillinger og ansvarsoppgaver dere innehar.

**Det er frivillig å delta**
Det er frivillig å delta i prosjektet. Alle opplysninger om deg vil bli anonymisert. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

copy 2.png copy 2.png

**Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. De som vil ha tilgang til data tilknyttet prosjektet er masterstudenten, SINTEF og NTNU. Ditt navn eller annet personidentifiserende
data vil ikke bli registrert, kun stilling og arbeidsoppgaver. Du vil bli registrert et anonymt identifikasjonsnummer.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**
Prosjektet skal etter planen avsluttes 7.juni 2019. Anonymiserte data og lydopptak vil ved prosjektslutt bli slettet permanent.

**Dine rettigheter**
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

**Hva gir oss rett til å behandle personopplysninger om deg?**
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra SINTEF og NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

**Hvor kan jeg finne ut mer?**
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- *SINTEF* ved *Karin Bernsmed (karin.bernsmed@sintef.no +47 482 15 585)*
- Vårt personvernombud: *NSD*
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig

*Eventuelt student*

(Forsker/veileder)

---

copy 3.png copy 3.png

## Samtykkeerklæring

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

- □ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 7.juni

---

(Signert av prosjektdeltaker, dato)

# Appendix C
# Interview guide

| Questions | Follow up | |
|---|---|---|
| **Part 1 - context** | | |
| **Context** | | |
| Kan du fortelle litt innledningsvis hva dere jobber med? | Hvorfor kaller dere dere en startup? | |
| | Når ble første versjon av produktet lansert? | |
| Hva jobber du med til vanlig? | | |
| *Vi har delt inn noen fokusområder som vi vil snakke nærmere om. Det går på personene i startupen deres, prosessene dere jobber med og motivas* | | |
| | | |
| **Part 2 - Organizational level security** | | |
| **Persons** | **Trenger ikke stille alle om de er besvart** | **Hypotese** |
| Hvordan er dere organisert eller inndelt i startupen? | | |
| | Hvor mange personer er i hver gruppe/flyt/område? Hvorfor er det evt mange et sted? | |
| | Hvor mange jobber med utvikling? | |
| | Implementerer dere og drifter også? | |
| | Hva skiller dere fra hvordan en vanlig bedrift er organisert? | |
| Hvem er det som jobber med sikkerhet i deres startup? | | **Startups har en ansvarfordelingen og roller knyttet til sikkerhetsarbeidet** |
| | Hvilke aktiviteter er de ulike involvert i? følge opp med spørsmål om hva de enkelte gjør | |
| | Har dere flere som jobber med sikkerhet eller har oppgaver som er nærliggende? | |
| Hvordan avklarer dere hvem som har ansvaret for hva? | | |
| | Står det nedskrevet noe sted? | **Aktivitetene knyttet til sikkerhet er avklart muntlig og ikke skrevet ned.** |
| | | |
| Er det noen av de nevnte som har vært initiativtaker for arbeidet med sikkerhet? | | **Det er en person som er hovedkompetansesøker for sikkerheten i startupen** |
| | Hvorfor er det slik at det kun er en person / flere personer? | |
| | Hvor er det denne personen søker kompetanse? | |
| | Er det andre som aktivt søker kompetanse? | |
| | | |
| Av de som har sikkerhetsrelaterte oppgaver - Hvordan lærer disse om sikkerhet? | | **Det stilles krav til at man lærer mye selv** |
| | Har dere intern eller ekstern kursing? | |
| | Er dette kursing for alle typ awereness training program, eller spesifikt for de som trenger noe? | |
| | Har dere noe opplæring av andre ansatte om sikkerhet? | |
| | Hvordan gjør dere det med opplæring av disse? | |
| | I hvilken grad har bakgrunn innen sikkerhet noe prioritering når dere ansetter? | |
| Har det endret seg hvem som jobber med sikkerhet gjennom årene? | | **Organisering av sikkerhetsarbeidet endrer seg etter hvert som startupen vokser** |
| | Hvordan har det endret seg? | |
| | Hvor tidlig startet dere å fokusere på sikkerhet | |
| | Hvordan er arbeidet dere gjør med sikkerhet påvirket at dere er en startup? | |
| | | |
| | | |
| **Development prosess** | | |
| Har dere noe prosess rundt hvordan dere jobber med /utvikler deres produkt? | | |
| | Hva innebærer denne prosessene? | |
| | Har dere noen ulike steg/faser dere følger? | |
| | | |
| Hvordan jobber dere med sikkerhet i ulike steg/faser av prosessen? | | **De gjør tiltak for å sikre produktet sitt i flere steg av en utviklingsprosess.** |
| | Hvorfor velger dere disse stegene eller fasene? | (kravspek, design/arkitektur, koding, test, prodsetting, forvaltning) |
| | Er det noen faser dere ikke jobber med sikkerhet, eller faser hvor sikkerhet blir nedprioritert? | |
| | Hvorfor gjør de ikke noe her? | |
| | Hvem bestemmer hva dere skal inkludere i prosessene? (en person vs kollektiv beslutning) | |
| | Hvorfor er det denne/disse personen/(e)? | |
| | Om dere ikke hadde vært en startup, tror du det hadde vært annerledes prioriteringer? | |
| | Hvilke faktorer spiller inn når dere prioriterer? | |
| | | |
| Har dere gjennomført sikkerhetstesting/inntrengingstester? | | |

| | | |
|---|---|---|
| | Hvordan gjør dere dette? | |
| Hvorfor la dere inn de ulike sikkerhetstiltakene i utviklingsprosessen? | | **Fokuset på sikkerhet har endret seg ettersom produktet har blitt mer stabilt** |
| Hvordan blir rutinene håndhevet? | | |
| | | |
| I hvilken grad styrer risiko eller negative konsekvenser hvordan dere lager produktet? | | **Startups er bevisste på risiko og deres egen risikoappetit** |
| | Hvordan kommer dette til uttrykk? | |
| | Hvorfor blir det ikke styrt? | |
| | Om dere ikke hadde vært en startup, hadde dere prioritert annerledes? | |
| | Hvorfor det? | |
| **Motivasjon** | | |
| | | |
| Du har nevnt at dere jobber med sikkerhet xx, hva er dere motivasjon for å jobbe med sikkerhet? | | |
| | Hvem er det som påvirker hvordan dere jobber med sikkerhet? | |
| | | **Tillit og krav fra kunden er viktig for deres prioriteringer** |
| | | |
| | | |
| Har dere eksterne påvirkningsfaktorer for hvordan dere jobber med sikkerhet? | | |
| | I hvilken grad påvirker lover og regler arbeidet? | **GDPR er en primær pådriver for compliance** |
| | Spør kundene etter noe? evt hva? | |
| | Hvorfor er det viktig/ikke viktig å høre på kunden? | |
| | Har dere andre som kunder, investorer, osv? | **Eksterne faktorer er mer effektive som pådriftskraft enn interne** |
| | Har dere interne påvirkningskraft for hvordan dere jobber med sikkerhet? | |
| | Hva vektlegger dere mest? | |
| | Er det noen av de forrige faktorene som blir påvirket av at dere er en startup? | |
| Har dere noen interne motivasjonsfaktorer for å jobbe med sikkerhet? | | |
| *noen raske spørsmål om sikkerhet* | | |
| **Checklist** | | |
| Får ansatte tips om hvordan lage passord? | | **Startups har noen grunnleggende retningslinjer for hvordan ansatte skal jobbe sikkert** |
| Har ansatte krav om 2F? | På hvilke kontoer? noen håndheving? | |
| Har dere retningslinjer for bruk av tilkoblede enheter som USB? | | |
| Har dere noe policy for låsing av maskinen? | | |
| Bruker dere diskkryptering? | | |
| Har dere rutiner for backup? | | |
| Bruker dere noe fildelingstjeneste? | Hvilke? | |
| Har dere en oversikt over hvilke maskiner, utstyr og brukerkontoer dere har? | | |
| | Når noen slutter, hvordan blir dette håndtert? | |
| Har dere gjennomgang når folk begynner? | | |
| Har alle tilgang på alt, eller har noen flere tilganger? | | |
| Har dere noen automatiserte sikkerhetssjekker? | | |
| | | |
| | | |
| | | |
| | | |
| **styringsrammeverk** | | |
| Hvor får xx eller flere inspirasjon fra når dere jobber med sikkerhet? | | |
| | Typ owasp, norsis, iso andre steder | |
| Bruker dere noe rammeverk/guider annet? | | |
| Har dere noen rammeverk / guider dere anbefaler andre startups? | | |
| Små startups som vokser, noen tips til hva de burde gjøre? | | |
| | Og hva kan være eventuelle fallgruver for dem? | |
| | | |
| | | |
| | | |
| | | |

Appendix D

# Research approval NSD

NSD NORSK SENTER FOR FORSKNINGSDATA

**NSD sin vurdering**

**Prosjekttittel**

Security in startups

**Referansenummer**

994362

**Registrert**

28.01.2019 av Nora Futsæter - norakf@stud.ntnu.no

**Behandlingsansvarlig institusjon**

NTNU Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Karin Bernsmed, karin.bernsmed@sintef.no, tlf: 4748215585

**Type prosjekt**

Studentprosjekt, masterstudium

**Kontaktinformasjon, student**

Nora Futsæter, nora.futsaeter@gmail.com, tlf: 93269440

**Prosjektperiode**

11.01.2019 - 07.06.2019

**Status**

28.01.2019 - Vurdert

**Vurdering (1)**

---

**28.01.2019 - Vurdert**

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 28.01.2019. Behandlingen kan starte.

MELD ENDRINGER
Dersom behandlingen av personopplysninger endrer seg, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. På våre nettsider informerer vi om hvilke endringer som må meldes. Vent på svar før endringer gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 07.06.2019.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!
Tlf. Personverntjenester: 55 58 21 17 (tast 1)