NTNU – Trondheim
Norwegian University of
Science and Technology

Utilisation of the perceived benefits of training new employees in information security

Jonas Tysdahl Gedde-Dahl

Submission date: June 2019
Responsible professor: Maria Bartnes, IIK
Supervisor: Erlend Andreas Gjære, Secure Practice

Norwegian University of Science and Technology
Department of Telematics

Title:	Utilisation of the perceived benefits of training new employees in information security
Student:	Jonas Tysdahl Gedde-Dahl

Problem description: Users of information systems are often seen as the weakest link in the security chain. Often users do not follow security advice and procedures. A good information security culture is proven to be a working solution. Education and training of employees is one measure to increase the information security culture. Education and training are already an essential part of the onboarding of new employees. Teaching information security from the beginning utilizes the new employee's eagerness and will to learn. Additionally, it eliminates the need to relearn tasks in a secure manner and removes the potential security hole of new employees, pre-information security training.

The Norwegian center for Information security (NorSIS) has released several reports on the state of the general Norwegian information security culture. They state that roughly only one in five has received any form of information security training, businesses are becoming more likely targets, and; "The government is not taking proper responsibility to educate its citizens, hence it is left to the businesses." This means that businesses are the first places many people learn about information security and that the training provided becomes even more important. We hypothesize that businesses do not educate new employees sufficiently and do not utilize the advantage of doing so.

The aim of this project is hence to find out how, why, and to what extent businesses train new employees in information security. This will be researched through a case-study of different organizations where data will be collected through interviews and surveys.

Responsible professor:	Maria Bartnes, IIK
Supervisor:	Erlend Andreas Gjære, Secure Practice

Abstract

Knowledge and training are crucial parts of obtaining an Information Security (InfoSec) awareness and creating a behavioral change. In Norway, no InfoSec training or education is done at school or in other ways targeting the younger population. This means that when they get hired by a company, the new employees stand without any InfoSec experience and pose a potential risk towards the company. The solution to this problem is simply training the new employees in InfoSec when they start working. This solution also provides benefits in that the new employees can learn their tasks in a secure way from the start, and do not need to relearn their tasks. The new employees can be introduced into the InfoSec culture from the start and molded to this effect. Even with all the advantages, and information pointing to early InfoSec training of new employees as a critical point, not every company does so. This research project aims to uncover not only how and why new employees are trained in InfoSec, but also potential faults in the training, and potentially why the InfoSec training is missing. In order to find the answers, there were three rounds of information gathering. Firstly, a case study was conduced on the learning material different companies used when training their new employees in InfoSec. This case study aimed mostly at finding the answers to the question of "how new employees are trained in InfoSec?" Secondly, an interview with the people who developed the InfoSec training program and who supervised the execution of the training program was conducted. The interview focused at answering the question "why new employees are trained in InfoSec, or potentially why not?" Lastly, a questionnaire was used to strengthen the findings of the case study and interviews. The first of the findings tell that all InfoSec training done by the companies, is in the form of online courses done individually by the new employees. The reason for this was the resource usage for any other solution being high, and limitations to the time allocated for InfoSec training of the regular employees. The second finding is that the InfoSec personnel develop the InfoSec training program, without educational resources. In practice, this means that the content and topics of the InfoSec training are good, but the methods and techniques used to impart knowledge to, and change the behavior of the new employees are somewhat lacking. The last finding is towards the companies who do not train their new employees in InfoSec. This problem does not come from a lack of interest from the InfoSec department, but from the company in general. More specifically the InfoSec department had problems with jurisdiction and authority outside of their own department. The problem had existed in all the companies

but was solved using written contracts between the InfoSec department and the top management.

Sammendrag

Kunnskap og opplæring er en avgjørende del av å skape en bevissthet rundt informasjonssikkerhet og å skape atferdsendring. I Norge er det ingen opplæring eller utdanning i informasjonssikkerhet på skolen eller som på andre måter er rettet mot den yngre befolkningen. Dette betyr at når de blir ansatt i en bedrift, står de nyansatte uten erfaring i informasjonssikkerhet og utgjør en potensiell risiko mot bedriften. Løsningen på dette problemet er ganske enkelt å trene de nyansatte i informasjonssikkerhet når de starter. Denne løsningen gir også fordeler ved at de nyansatte kan læres opp i oppgavene på en sikker måte fra starten, og trenger ikke læres opp på nytt i etterkant. De nyansatte kan bli introdusert i informasjonssikkerhetskulturen fra starten og kan formes deretter. Selv med alle fordelene, og informasjon som peker på tidlig trening i informasjonssikkerhet for nyansatte som et kritisk punkt, gjør ikke alle bedrifter det. Dette forskningsprosjektet tar sikte på å avdekke hvordan og hvorfor nyansatte blir opplært i informasjonssikkerhet, hvilke mangler opplæringen eventuelt har, og hvorfor de nyansatte eventuelt ikke blir opplært i informasjonssikkerhet. For å finne svarene ble det gjennomført tre runder med informasjonsinnsamling. Første runde var en case-studie på læringsmateriellet ulike selskaper brukte når de lærte opp nyansatte i informasjonssikkerhet. Denne case-studien er i hovedsak rettet mot å finne svar på spørsmålet om "hvordan nyansatte er opplært i informasjonssikkerhet"? Den andre runden var intervju med utviklerne av opplæringsprogrammet i informasjonssikkerhet og de som administrerte gjennomføringen av opplæringsprogrammet. Intervjuene fokuserte på å få svar på spørsmålet "hvorfor nyansatte er opplært i informasjonssikkerhet, eventuelt hvorfor ikke"? Til slutt ble en spørreundersøkelse brukt til å styrke funnene fra case-studien og intervjuene. Det første av funnene er at all opplæring i informasjonssikkerhet utført av bedriftene var i form av nettbaserte kurs utført individuelt av de nyansatte. Årsaken til dette var at ressursbruken for andre løsninger var høy, og det var begrensninger på den tildelte tiden for opplæring i informasjonssikkerhet for de ansatte. Det andre funnet er at informasjonssikkerhetspersonellet utviklet opplæringsprogrammet i informasjonssikkerhet uten pedagogiske ressurser. I praksis betyr dette at innholdet og emnene i informasjonssikkerhetsopplæringen er god, men at metodene og teknikkene som brukes til å formidle kunnskap, og endre oppførselen, til de nyansatte var mindre effektive. Det siste funnet er mot selskapene som ikke lærer opp sine nyansatte i informasjonssikkerhet. Dette problemet kommer ikke fra mangler hos informasjonssikkerhetsavdelingen, men fra selskapet generelt. Nærmere

bestemt hadde informasjonssikkerhetsavdelingen problemer med ressursbruk og autoritet utenfor egen avdeling. Problemet hadde eksistert i alle selskapene, men hadde blitt løst ved hjelp av skriftlige avtaler mellom informasjonssikkerhet avdelingen og toppledelsen.

Preface

This research project is the master theses that finish my Master of Science degree in Communication Technology at the Norwegian University of Science and Technology (NTNU). As a part of the degree the author chose to specialise in InfoSec at the Department of Information Security and Communication Technology (IIK) at the Faculty of Information Technology and Electrical Engineering (IE).

Very first I would like to thank Erlend Andreas Gjære and professor Maria Bartnes at IIK who have been my supervisors. You have both been an incredible help.

I would also like to thank the organizations who chose to join this research project and to all who answered the questionnaire.

Lastly, I would like to thank my wonderful girlfriend, friends, and family who have helped with things like proofreading, discussions, and ideas throughout the semester.

Jonas Tysdahl Gedde-Dahl
Trondheim, June 2019

Contents

List of Figures

List of Tables

List of Acronyms

CET Cognitive Evaluation Theory.

CISO Chief Information Security Officer.

GDPR General Data Protection Regulation.

HR Human Resources.

IE Faculty of Information Technology and Electrical Engineering.

IIK Department of Information Security and Communication Technology.

InfoSec Information Security.

IT Information Technology.

NIST National Institute of Standards and Technology.

NorSIS Norwegian Center for Information Security.

NTNU Norwegian University of Science and Technology.

PHD Philosophiae Doctor.

PMT Protection Motivation Theory.

TRA Theory of Reasoned Action.

Chapter 1
Introduction

This chapter aims to inform the reader on the history, current state, and motivation for this research project. The intention is to give the reader the same baseline this research project builds upon and support the arguments given.

1.1 History and Motivation

Any organization with digital assets or obligations need to protect these. In the process to do so, it is impossible not to involve humans. In modern InfoSec, humans are generally considered the weakest link in any InfoSec chain. The reason is that users do not follow policies or rules regarding InfoSec. This has been a problem for several years. The reason users do not follow policies, rules, or generally make mistakes is associated with a general lack of InfoSec culture, which again is caused by lack of InfoSec awareness and understanding. InfoSec awareness is the perception, evaluation, and understanding of InfoSec, and builds on knowledge. The first step to improve users behavior towards InfoSec policies and rules is to improve their knowledge and understanding of the subject [NSSF16].

Another fact is that organizations who aim to continue normal operations need to hire new employees. New employees may come from a variety of different backgrounds and will work in a variety of different jobs, all in the same organization. What is the best method to educate a group of people in InfoSec, when all in the group have different pre-knowledge and expectations? New employees starts a new job with a commitment that decreases some over a time period [OC81, PJ91]. Is this utilized when educating the new employees in InfoSec? From the new employee's point of view InfoSec may be one of many topics mentioned to them in their new work environment, but not something that they actually use or see as relevant to there task. Training new employees in InfoSec is not something that generates a profit for the organization from the management point of view. How to overcome problems with management? How to educate an interested group? How to change

the behavior of the employees? Finding a solution to all these potential problems and customizing them for a specific organization is a complex task.

Norwegian Center for Information Security (NorSIS) have for the last three years made an annual survey of the general InfoSec culture in Norway. The first report from 2016 stated that "The government is not taking proper responsibility to educate its citizens, hence it is left to the businesses." With no InfoSec education or training prior to getting hired, the training or education received from the employer becomes even more crucial. The 2017 report found that only 21% of the population had any form of training or education at all. The 2018 report mentioned higher fears and rising threats towards the digital life [MR16, sfi17, MR18].

The new employees will most likely have their first encounter with InfoSec when they start their first job. The new employees show a higher commitment and are easier to influence at the start of a new job. The organizations are better off with InfoSec being used and utilized from the beginning. These arguments are singling out the education of new employees as a critical point for initializing and maintaining a good InfoSec awareness and culture.

The research questions (RQ) for this thesis are then as follows.

- RQ1: How are new employees trained in InfoSec, and are there any differences compared to other employees?
- RQ2: What is the content of the InfoSec training for new employees?
- RQ3: Why are new employees trained or not trained in InfoSec?
- RQ4: Do companies utilize the benefits of training new employees in InfoSec, possibly why not?

1.2 cope and Limitations

This thesis is the final part of a Master of Science degree in Communication Technology at NTNU. The thesis and its work are weighted at 30 points and estimated to take 21 weeks of work to finish. Before the thesis, there was done a pre-project weighted at 7,5 points. The pre-project and thesis was done on the same topic and by the same author.

As this research project is based in Norway, any research done with a physical location requirement will hence be limited. The research project will also be limited by the time allocated, and that re-use from the pre-project is not allowed.

Chapter 2
Related Work

In this chapter, there will first be presented some definitions followed by a review of several studies and previous work on the topic of training and education in regards to InfoSec.

2.1 Definitions

The use of different terms may change depending on the person using them, the context, or other variables. In order to remove doubt and the possibility of misunderstandings, this part will define the meaning of the main terms used in this project.

2.1.1 Information Security Awareness

Information security awareness has previously been used with varying definitions. These definitions all had the main part in common, containing behavior and knowledge to different degrees. Some examples are Wolf, Haworth, and Pietron [WML11]. Whom states that:

"It is the effort to impart knowledge of or about factors in information security to the degree that it influences users' behavior to conform to policy."

While Shaw, Chen, Harris, and Huang [RH09] defines InfoSec awareness as:

"The degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks."

For this project, Shaw, Chen, Harris, and Huang's definition will be the correct one. While Wolf, Haworth, and Pietron's definition is a good definition, the formulation

of the definition was made in the context of its study. One example is that it includes "the effort to impart knowledge," which may not always be the case in different contexts. Shaw, Chen, Harris, and Huang's definition refer to the knowledge, behavior, and motivational aspects on different levels towards the protection of the organization's information assets.

2.1.2 Information Security Culture

Similar to the definition of InfoSec awareness the definition of information security culture seem to have varied some dependent on the person using it and the context. The main theme of the InfoSec culture definitions is that they refer to the definition of culture in the context of an organization, combined with InfoSec. Veiga and Eloff [VJ10] suggest InfoSec culture can be defined as:

"The way things are done in the organization to protect information assets"

Martins and Elofe [AJ02] also comes with an definition, but similar to Wolf, Haworth and Pietron's [WML11] its formulation is to related to its context. Other definitions also exist [Lar18], but from lack of access to the source, the definition to be used in this project will be what Veiga and Eloff suggest. This definition also aligns with the definition of organizational culture that Martins and Elofe use and refers.

2.2 Education

This section is meant to clarify and support other research that is discussed in section 2.3.

Education is the process of receiving or giving systematic instruction or knowledge. In order to make this process as effective as possible, research has aimed to understand and utilize it [Hob60].

2.2.1 Protection Motivation Theory

The Protection Motivation Theory (PMT) deconstructs how fearful something appears to be into three parts. The first is how dangerous or potentially harmful the situation is perceived to be. The second is the perceived likelihood of the event occurring. The third is the effectiveness of the response. All of these parts rely on the observation of, or communication to, the individual and trigger individual appraisals. These appraisals may result in attitude or behavior change or both [W75].

In the end, this is all about how the individual perceives and processes threats, and selects a response. This Theory is well supported and accepted in later research. Some of the research done on the PMT is how the individual may be influenced to choose different responses [JFTJC89]. The same research also indicates that fear appeals become less effective at inducing an attitude or behavior change, when not combined with information about the response.

2.2.2 Theory of Reasoned Action

The Theory of Reasoned Action (TRA) is a model that can be used to predict how individuals will behave. The model uses the intentions and attitudes of the individual before the situation in order to predict the result. The theory has been revised and extended by other researchers, especially in the 1970s and 1980s. The current version of the theory is widely accepted. It is simple in its application and gives good results [BHSW88].

2.2.3 Cognitive Evaluation Theory

In short terms, the Cognitive Evaluation Theory (CET) tries to explain the connection between external events and internal motivation. The theory suggests motivation is affected negatively by expected rewards, and that unexpected rewards not perceived to be a part of the task, does not have any effect on the motivation at all [RMRK83]. Though not specified the CET defines rewards quite loosely including different forms of feedback. The theory is widely accepted and covers a broad area, but is mostly applied to motivation [M.82].

2.2.4 Universal Constructive Instructional Theory

The universal constructive instructional theory is a framework developed in 1997. The framework is based on the instructional theories of its time and aimed to promote discussion in the field of instructional theory. The goal of the framework itself was to customize instructions for the topic and the receiving users. Even though the original framework was generalized, it was found to be accurate and give positive results [FP97, PS10].

2.2.5 Situational Awareness

Situational awareness is defined as, "the perception of the elements in the environment within volumes of time and space, the comprehension of their meaning, and the projection of their status in the near future." This definition was described in 1995 by Mica R. Endsley, who explained the needs of different levels of situational awareness [END95]. She divided situational awareness into three levels. The first level is the perception of the current status, monitoring, and detection of a change in the

situation. The second level is the comprehension of situations and determining the meanings of and reasons for changes to the situation. The third level is the ability to predict future situations from the current situation and its meanings.

2.3 Information Security

Information security and the protection of information assets have existed for a long time. Encryption of information has been in use from as early as 1500 bce [Kah96]. From then and forwards the progress has been massive, especially with the use of computers. With the influx of computers and the internet, information has become a more sought and needed asset. In modern times the main problem is no longer the lack or weakness of encryption or safe transfer of information. The problem is the lack of use, or misuse of these features, as well as poor management of the systems [Spu95, TvS98, Gau98]. In order to find an effective countermeasure to these problems, several studies have focused on it.

2.3.1 The Norwegian Situation

NorSIS is an organization whose goal is to influence the Norwegian private and public sectors positively in regards to InfoSec. NorSIS have published a report each year since 2016 based on their research into InfoSec in the Norwegian society.

The conclusions from the initial report are that the general population lacks in general InfoSec knowledge and that there is a great potential for improvement. The report mentions measures like education, business InfoSec policies and commitment all affect the general InfoSec culture positively, but that they alone are not enough. The report also goes into details on what part of the society is covered by different initiatives,

"The government is not taking proper responsibility to educate its citizens, hence it is left to the businesses."

Those outside the workforce is left without any initiatives [MR16].

The NorSIS report from 2017 mentions that less than 22% of the Norwegian population has received any form of education or training in InfoSec. The report urges the government as well as private and public companies to facilitate for a better InfoSec culture, through training, education, and commitment, but also mentions that this probably will not be enough. Finally, the report mentions rising fear and mistrust towards digitalization from the population [sfi17].

The NorSIS report form 2018 states that the fear towards the digital life is rising, more people expose themselves online, and the global threats are rising. The rising

threats are towards individuals as well as companies. The general population's InfoSec competence and culture does not seem to be rising [MR18].

2.3.2 Information Security Training

From the beginning, all research on InfoSec awareness has agreed that training and education is a key point in order to change behavior and create the awareness itself. [Spu95, dVM15, NSSF16]. InfoSec training is as other forms of training only a tool in order to reach a goal. Training is the act of teaching a particular skill or type of behavior. The goal of InfoSec training is then to educate and stimulate the recipient to perform at a higher level in regards to InfoSec. Project and articles on how to train and educate employees in InfoSec started appearing in 2002. Some of these articles focused on potential tools and methods of InfoSec training [SFD02], and some on a larger scale. In 2003 National Institute of Standards and Technology (NIST) released a publication on how to build a InfoSec training program [WH03]. These solutions where implemented and tested during the years after, but where found lacking in some aspects as users still presented a major threat.

The first research to focus on users part of the InfoSec relied heavily on physiology to understand why users misused systems, deliberately or unintentionally. The main theory explored was the PMT (2.2.1). The first research to use this theory found that there was a large discrepancy between the users and the experts on all three main points of the theory. Users did not find the situations potentially harmful, did not find it likely that they were targeted and did not see the benefits or effects the responses put in place by the experts [MWS08]. This same article also points to the complexity of the measures taken felt by the users. Further, it uses this as an additional argument of the failure of the third point of the PMT.

Cormac Herley [Her09] also brings up users deliberately ignoring measures put in place. His article takes a logical review of the most common policies and measures from the user's point of view. In the article, he argues that users rationally ignore the measures put in place because of the general cost compared to the rest of the context. The conclusion of his article states that, the service of InfoSec provided should not come at a cost to the user and that the service needs to take the user and the users context into account when being developed.

Because users seemed to be overwhelmed by complex or costing InfoSec policies, these needed to be explained and customized. Mete Eminağaoğlu, Erdem Uçar and Şaban Erenc [ME09] did a case study on a company trying to increase the policy compliance. This study was done through initial training and a follow-up campaign within the company. The results show similar to the other articles that simplified and cost-efficient advice given to the users was being followed, even though it based on the same policies previously. The article specifies a need for an understanding and

cooperation with the user, rather than a one-way flow of information and requests. Additionally, in the iterations done on the process of the case study, the article finds that campaigns that aim to remind are preferable to campaigns that aim to reeducate.

R.S. Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang [RH09] mentions three main problems of their time concerning InfoSec. General InfoSec awareness, budgets, and users low computer skills. In their article, they explore the use of computers to solve all of these problems. They found that this helped against the second and third problems. The first problem was found to be reliant on the type and forms of media used. To which they found that media like pure text help to perceive the information, and mixed media like images, video, and sounds was found to be best at the comprehension part. Both comprehension and perception were needed in order to use the knowledge correctly.

More studies where done on InfoSec training to increase the InfoSec policy compliance, as this was the main problem observed. This research was argued to be theory based and to be empirically evaluated. In their article, Petri Puhakainen and Mikko Siponen [PS10] uses educational, instructional, and psychological theories in order to find how the InfoSec training could be as effective as possible. The main finding was that customizing the training to the relevance of the typical tasks users performed was a significant success. Customizing the training based on the user's previous knowledge also gave positive results. In the organization of the training, in the context of the relevance to the typical tasks, InfoSec training should be combined with the other forms of training the users did. Additionally, they suggest that InfoSec training should be continuous. Lastly, their findings indicate that visible support from the top management was necessary in order to ensure users compliance with the policies.

Still trying to find a solution to the problem of users not complying with InfoSec policies, Mari Karjalainen and Mikko Siponen [KS11] made a new meta-theory for designing InfoSec training. Building on previous articles, they argue that the theory for other forms of training and education is not viable for use in the context of InfoSec. The new meta-theory has four main phases to InfoSec training: Involve concrete experiences, Engage reflective observations, Support formation of abstract concepts and generalizations, and Enable active experimentation. All the four phases are backed in previous research and used as pedagogical requirements for an effective InfoSec training approach.

Having found a viable solution to the problem of how to educate users in the context of InfoSec, the main problem still was found to be users misusing the system, intentionally or unintentionally. The focus of the general research in InfoSec returned

to the physiology in the context of InfoSec education. Meso, Ding and Xu [PMX14] applied the PMT (2.2.1) to InfoSec training in school. This study provided even more evidence to the theory of relevance to normal tasks being a positive trait in the InfoSec training.

Mikko Siponen, M.Adam Mahmood and Seppo Pahnila [MSP14] combined the PMT (2.2.1), the TRA (2.2.2) and the CET (2.2.3) as the base for a new model trying to explain employees' adherence to InfoSec policies. Their findings include the following; The higher the perceived severity and vulnerability of potential threats become, the more likely users are to comply. The user's belief as to whether they are able to comply and the user's attitude towards complying, both affect the motivation to comply positively. Lastly, positive social norms towards compliance gave a positive motivation to the individual users to comply. All of these affected the user's motivation, which affected the user's actual compliance as well as the training.

Research has also been conducted on compliance of InfoSec policies in the context of an organization. Similar to Mikko Siponen, M.Adam Mahmood and Seppo Pahnila, involvement, commitment, and norms were found to affect motivation positively and indirectly the InfoSec policy compliance. Attachment was found to have a negative effect on InfoSec policy compliance [NSSF16].

Chapter 3
Methodology

This research project goes into the topics of social science and management while briefly touching on other topics as support. The social science is through the research of how the training of new employees are trained in InfoSec, while the management is through how the InfoSec training of new employees are performed. This research is done as a case study, followed by an interview, followed by a questionnaire. The case study and interview uses qualitative methods for the analysis. This method is by Robert K. Yin [Yin09] argued as the best analysis method, based on the type of material that probably will be available for the case study and the nature of the spoken words used in interviews. The questionnaire uses a quantitative method for the analysis. This is an excellent and well-tested method for large amounts of responses and simplifies the analysis process. Because the research project will make use of both qualitative and quantitative methods, it will fall into the category of a so-called mixed research method or multi-strategy research [RM11].

There has previously been a discussion on whether the two methods, qualitative and quantitative, could be used together in social science. The discussion was mostly based on Egon G. Guba [Gub87] who argued "no possibility exists that there can be an accommodation at the paradigm level.", hence "naturalistic evaluation of the second kind is necessarily bounded by the assumptions of the naturalistic paradigm." with "naturalistic evaluation of the second kind" referring to the naturalistic approach of a "wholly different way of viewing the world". Egon G. Guba does however, agree that a mixed research method is entirely possible in the naturalistic approach of using qualitative and quantitative methods as tools. This research project will use the qualitative and quantitative methods as tools, hence falling in the first category and evading this potential problem. This also allows for the utilization of the advantage of the mixed research method by using triangulation to further support the findings [RM11].

Information security	Training
	Awareness
	compliance
	Education
	Guidelines
	Teaching

Table 3.1: Systematic literature review search terms.

3.1 Systematic Literature Search and Review

A systematic literature review is a systematic and thorough mean to find, categorize, evaluate, and interpret literature that may be relevant to the study. The purpose of the literature review is to evaluate the current state of the research in order to find evidence to be used as a baseline for new research or possible faults or gaps that should be covered [Kit04]. The results from the literature review are found in chapter 2.

In this study, the primarily used search engine was Google Scholar. Google Scholar has located, categorized, and indexed large amounts of journals and other scientific papers. When using Google Scholar, the starting search term used was "Information security training," this was followed up by several variations. All variations used in the literature search is listed in table 3.1. The literature search was not perfect, and so all articles and papers found were filtered. The first filtering criteria were relevance to this research project. This was determined after reading the abstract and conclusion. If, after reading the abstract and conclusion, the relevance was still in doubt, the whole paper was read. The second filtering criterion was credibility. To ensure this, all the papers had to be peer-reviewed. ScienceDirect, Taylor & Francis, ProQuest, Association for Information Systems, EmeraldInsight, IEEE Xplore, Microsoft Research, SpringerLink and Jstor are all platforms with databases of academic papers. These platforms allow for publication of peer-reviewed research and have strict standards. This process was iterated overall search term variations, with the 30 top results being filtered. Some articles were located through the citations of the articles found in the search, and some were found through word of mouth. All the articles found were still put through the criteria in order to be useful to this project.

Outside of the results from the Google Scholar searching process, some other literature was found to match the criteria. This includes reports from NorSIS, previous master projects, and books from the curriculum of related courses at NTNU.

3.2 Information Gathering

The gathering of information consists of three steps. The first step is a case study of the information security learning material that each company uses. The case study gives an initial overview of how and what the companies information security training contains. The second step is a semi-structured interview. While the interview will primarily function to gather more in-depth data, it provides an excellent opportunity to follow up on missing or additional information from the case study. The last step is a questionnaire for new employees. The questionnaires primary function in this study is as a third point in order to triangulate and validate the findings.

3.2.1 Case Study

A case study is a research method that focuses on observing the research object in the natural environment it occurs. The object of the case study will be the learning and teaching materials that each company provides. The purpose is to find how information security is taught, how the learning process is implemented, what topics, how much of the different topics are taught, and how the teaching process tries to affect the learner. According to [Yin09], case studies are one of the most laborious research methods to master, and he recommends apprenticing under a senior researcher. It will be unpractical to be in an apprenticing position during the whole project, so the supervising researcher will follow the case study carefully and consulted when needed. Case studies work best when the question to be answered is *how* or *why* based, and the research object is observed without control of the environment it exists in [Yin09]. The questions asked in the case study are how-based, and the research object may be on several formats, including paper, audio, video, and more. This matches the requirements for the case studies. The analysis of a case study does not have any pre-defined method for completion. This is why [Yin09] means it is the most laborious research method to master.

The analysis for the case study in this research project will base on the pattern matching technique on the qualitative data where the pattern should be compared up to expert recommendations.

3.2.2 Semi-Structured Interview

Semi-structured interviews are a combination of structured and unstructured interviews. The semi-structured interview can be a combination of any grade between the two. Semi-structured interviews are the most used method out of the three. The advantages of semi-structured are that it maintains a structure and outline to its form while being flexible to ask followup questions or new questions based on the interviewer's intuition [RM11]. Structured interviews have the advantage of questions being asked with the same phrasing, making analyzing the answers easier.

Semi-structured interviews may combine this with the freedom of the followup or new question, generally making it easier to analyze the main parts [RM11].

In this research project, the interviews will be classified as semi-structured interviews, making use of its advantages. The main goal of the interviews is to gather information around the information security training that is not on the training material itself. It then also becomes natural to have followup questions to the case study material. The interviews will also provide in-depth information on the particular solutions each company applies. Most of the questions will be open, promoting in-depth answers and explanations from the interviewed party. Regardless of the interview type, an interview guide will be of great help. The interview guide may contain questions, guidelines to different topics, or a general notation for what directions the interviewer would like the interview to take. This is not the only purpose of the interview guide. The interview guide should also contain notes on how to phrase questions, possible biases, and general tips and tricks [RM11, oS]. This project's interview guide will contain the main questions, possible followup questions, and tips to the interviewer. The interview guide can be found in appendix A.

3.2.3 Questionnaire

A questionnaire is a survey with a fixed set of questions. Questionnaires may vary in their length, depth of questions, whom they target and how they are distributed. A questionnaire excels at targeting larger groups of people and low-cost of information gathering. An online questionnaire is one way of distributing the questionnaire. Other forms of questionnaires include interviews, postal, or telephone calls. When compared to its counterparts, online questionnaires excel at lower cost, shorter collection period, and use of aid tools visual or otherwise[RM11]. The downsides of online questionnaires are the dependency on the respondent. The most common problem is that too few recipients respond, which in turn may affect the validity of the analyzed results. Lack of control is also a known problem that may cause the respondent to answer the questions in a different order than intended, misunderstandings while answering or interpreting the results or there may be unknown biases of the respondent [RM11].

The questionnaire was chosen as the method for this task as it matches the best with the requirements. This research project will gather information from the new employees in the companies interviewed. The purpose of the information sought is to triangulate the information from the case study and interview. The questions in the questionnaire need to be formulated in such a way that, they follow guidelines, are easy to understand, cannot be misunderstood and are the same for all companies regardless of the training method used. The questions will be close-ended, this requires that the answer alternatives are mutually exclusive and exhaustive [RM11]. Making the questions is an iterative process that will be repeated until all these

requirements are fulfilled. The final version of the questionnaire can be found in appendix A.

The group of potential responders in these companies is already considered low, as the companies do not recruit many new employees on a regular basis. This makes it even more important to get the possible respondents to answer the questionnaire. In order to get as many respondents as possible, the following steps will be taken: The questionnaire will be made so that it is easy to complete and takes short time. A random participant in the questionnaire will receive a price. Because the company is involved as a hole, answering the questionnaire may be done at work. This will need to be cleared with each company individually. When sent to the new employees, the questionnaire will be sent to their work e-mail. This will be done in an exchange of e-mails where they first have to give permission before receiving the actual questionnaire.

3.3 Data Analysis

Analyzing and processing data and information is a large portion of research work. In order to not affect the information or any conclusions that may be drawn from it, the analyzing process needs to be strict. Preventing that without proper guidelines or experiences analyzing data can allow for bias or faults to contaminate the work.

3.3.1 Quantitative Analysis

Before a quantitative analysis can be done, the data to be analyzed needs to be prepared. Most of the qualitative analysis done is currently being done on computers. Computers help organize, structure, and present the data. This is especially helpful when dealing with large amounts of data. When the data is prepared, cleaned, and checked for mistakes, the analyzing process can start. Quantitative analyses can be done in two ways, exploratory or confirmatory. Exploratory means to rearrange the data in new ways trying or testing, in order to find possible connections or correlations. Confirmatory analysis bases off a hypothesis and seeks to disprove or strengthen that hypothesis [RM11]. This research project will use quantitative analysis mainly on the results of the questionnaire. The reason for this is that it is the only results that will be based solely on numbers, as the questionnaire mainly have closed-ended questions. By using different analyzing methods, a better result will come from the triangulation. The quantitative analysis will be confirmatory in nature, with the findings in the case study and interview as the hypothesis it seeks to strengthen. Using the analysis in this way has a possibility of confirmatory bias. In order to prevent this, the person doing the analysis will be aware of the possible problem, and the supervisor of this research project will be in close contact in order to discuss the process during this part.

3.3.2 Qualitative Analysis

Qualitative analysis is mostly based on language, either spoken or written. It can also base on other forms of information, presented in a way that is subject to unsystematic subtle variations or biases from the source that is also hard to discern. There are three approaches to qualitative analysis, quasi-statistical, thematic coding, and the grounded theory approach. The first is a method that uses either the frequency or inter-correlation of words or phrases, in order to determine the importance and relevance. The second approach is similar to the first in that it splits the information, puts it back together, and looks at it in new forms. The splitting process gives codes or labels to all parts of data determined by the content. When put back together, the codes and labels are put under different themes. This approach is generic but not linked to a specific theory. The last approach is the grounded approach. The grounded approach is grounded in the data it bases off. It still uses thematic coding, but the codes and themes come from interacting with the data, rather than being made and categorized forehand [RM11].

This research project will utilize the grounded approach to analyzing the interviews. A thematic coding approach could have been used, but the codes and themes would be made with the material from the case study allowing for possible bias. Real World Research [RM11], have two assumptions for doing qualitative analysis at all: With a large amount of qualitative data, software should be used to handle it. And, unless the analyzing part is experienced, someone to help or advice during this part is needed. Apprenticeship has been the primary model for such work previously. In order to make the best use of the information offered by Colin Robson and Kieran McCartans book [RM11] and the resources available to the project, this apprenticeship will be handled similarly to that of the case study in section 3.2.1.

3.3.3 Triangulation

The word triangulation ordinates from the geographical field, where it represents the method of measuring distances and relative positions. In research, the triangulation method is the process of using several measurements from different points of origin onto the same area of research. This process allows for more certainty by reducing the area of possible outcomes. Triangulation is mostly done in qualitative research. This is linked to variations and possible bias in qualitative research [CNJ14].

3.4 Privacy and Neutrality Issues

This research project will handle information from both individual people and companies. Some of the information may be damaging to the people, the company, or both. This research project seeks to gather information without affecting the companies or people. The steps taken to ensure that this research project does not

affect the people or companies involved are as follows: The project has been reported to the Norwegian center for research, who have reviewed the methods of information handling and information given to participants so that everything follows laws and requirements. All information will be stored, handled, and transferred safely. No identifying information for people or companies will be in the final report, and no single individual will be mentioned in the final report.

3.5 Project Limitations and Risk Assessment

Doing a research project always carries the possibility of failing for different reasons. The research may also be limited by different factors that may affect the data gathered or the project in general. Here these points are discussed and what measures are used to counter them.

3.5.1 Limitations

A limitation is a tool used to narrow down the possibilities of something. This research project contains some limitations for different reasons. In this part, it explains what the limitations are and why they are used.

New Employees

In most cases, new employees will get training, information, and an overall impression just after starting a new job. In a work environment, the employee works to complete their tasks in a time and effort efficient manner. Information security training will seek to inform and change the way the employees behave and how they do specific tasks. The difference between new and old employees, other than the time employed, lies in that new employees have the possibility of learning the secure way of their job from the beginning. This is compared to regular employees who have to relearn or change the way of their work at a later time. New employees are also more committed to there job, are easier to influence [OC81, PJ91], and have not been subjected to the company security culture. These are all good reasons why information security should be applied to new employees as early as possible, and this is also why this research project focuses on new employees.

By the phrasing, the definition of new employees is that they are new to their current job. A new employee will transition towards the status of regular employee as their knowledge of the social norms, work ethic and how to perform their tasks approaches that of a regular employee, additionally their initial commitment will change [PJ91, OC81]. The time needed for this transition may vary dependent on the topic and how much it is applied. Social norms and work ethics have more variables to their estimated transition due to the interactions required, hence the time it takes

to know how to perform their own tasks is more reliable, but still it varies. Charles A. O'Reilly and David F. Caldwell [OC81] used a time period of 24 months in their project. In this research project, the definition of new employees is those who have worked 12 months or less. This matches with the influx of employees directly from school, provide time to transition towards a normal employee status to a degree, and will be relevant in a InfoSec relevant context.

Companies

The criteria for choosing what companies invited to this research project's surveys were: Being considered as a medium or above company with 50+ employees. This limitation was to remove small companies who do not necessarily employ enough new employees in a year to be use-full to the survey. Additionally, small companies do not necessarily have any internal information security program. The second criterion is that the company's main task is not IT related in terms of development, operating, or security through IT. This was to remove statistical outliers where the employees have specialized training or generally a much higher knowledge than the rest of the population. Combined with the size requirement outliers on both sides will be removed. The last criterion is for the company's employees to handle critical information. Critical information can be but is not limited to, personal, financial, cutting edge research, military, or medical information. Any company that fulfilled these criteria was qualified to join the survey.

3.5.2 Risk Assessment

In order to minimize the likelihood of failure for this project, a risk assessment is made. Here possible problems from different design choose done in this research project, will be discussed.

Information Gathering

One of the potentially most harming risks to this research project was if the information gathering failed. Without any information, no results may be achieved. Without any results, this project has nothing to show and nothing to discuss or conclude. As the project has three main steps all requiring different forms of information, they all carry some threat of not being able to gather information, but the risk of total failure is reduced. The common factor for all three steps is that they need companies to join the research project. Without any willing companies, the research project can not be completed. The risk for individual companies not wanting to join the project is quite high. This risk is typically countered by inviting a larger amount of companies. Due to the steps needed to be completed on all companies who join, and the work anticipated with each step, the goal is to get four or five participating companies. In order to further reduce the likelihood of companies declining to join, the companies

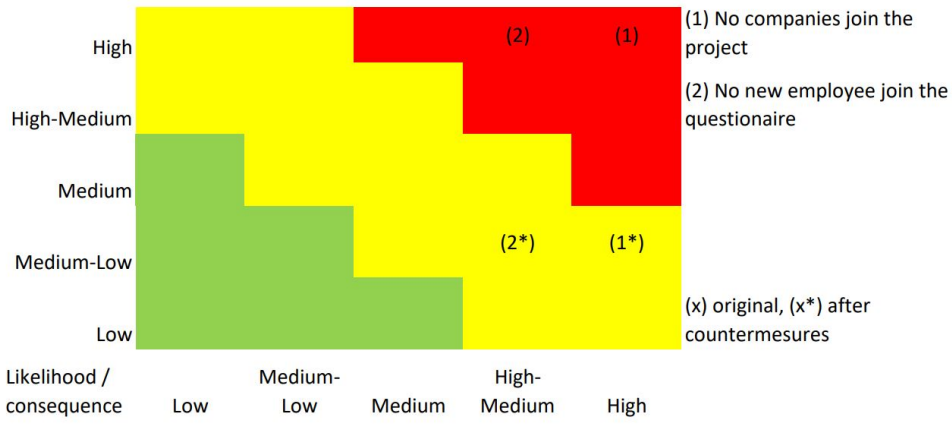

Figure 3.1: Risk matrix over the specific threats to this research project.

will be provided with the result from their own companies and comments referring to research and practices that may be improved or further focus is needed. This is as a trade for the resources they will use in joining this research project. When contacting the companies, a focused and direct approach will be used by contacting the Chief Information Security Officer (CISO) of the companies directly through different means. With these countermeasures, the likelihood of not getting enough companies is lowered from a high to medium-low as seen in 3.1.

With companies willing to join, the risk for the case study and interviews are handled. The questionnaire is also reliant on the new employees in the companies. With the goal of the questionnaire being to confirm or deny findings in the case study and interview the consequences is not as high. This research project can still be completed without any answers from the questionnaire, but it would be somewhat lacking. The likelihood of not getting any answers is considered high-medium. Because the companies will be a part of the distribution, and the number of answers needed to strengthen or weaken the findings is not that high, the likelihood is lower than usual. As for measures to lower the risk, prises can be given out as another incentive for the new employees to answer the questionnaire, this is a known and well-used method. Additionally, the questionnaire will be made in such a way that it does not take an unreasonable amount of time or hinder the recipients in any way. The risk of not getting any answers on the questionnaires is hence lowered to medium-low.

Other Risks

There are a couple of other risks associated with this type of research. These risks do not affect the likelihood of completing the research project, but rather the results and conclusion. Firstly as the project uses a sample of the total companies, there is a chance that the companies who join the project do not represent the average of the total companies. The reason for the risk is complicated, but the distribution, followup, and assumptions for the limitations are possible culprits. Some measures have been taken to avoid this (3.5.1), but the risk is still present at medium-low. A second risk to the results is faulty, inaccurate, or in other ways, information that does not represent the actual truth. There is also the inherent risk in some of the methods used, and so on. Most of these minor risks are meant to be countered by the methods described in this chapter, or from peer-review of the finished report.

Chapter 4
Results

This chapter is dedicated to the presentations of the raw results from the information gathering. The results are presented in a down-up view as the companies appear the most similar at the bottom levels.

In addition to the results gathered from companies who chose to be a part of this research project, several other companies were invited. Out of those who were invited and chose not to participate, three gave the reason that they did not have any training or education of InfoSec at all. One of these also stated that they had no organized protection for their machines, equipment or employees, treating all employees as a "3rd party". All these three companies, in addition to the four who joined the research project, were interested in improving their information security. Out of the total seven companies, six of them had problems acquiring human resources with InfoSec competence.

There where four companies who joined this research project by providing material and information about their InfoSec training of new employees. Further on in this report, they will be named A, B, C, and D respectively. In order to provide some information for their daily operations, some context will be given. Company A and B operate within the service industry, especially around humans. They are regulated through safety laws and work environment laws. Information Technology (IT) based tools are in daily use and are critical for daily operations. Company B also extends to other industries, so more laws or regulations may also influence them. Company C and D operate in the finance industry. They are regulated with several different laws, but also by contract between peer companies in the industry. For the finance industry in general IT is heavily used as a critical tool in daily operations.

4.1 Case Study

The case studies completed used the available material that the different companies used when training and educating their new employees in InfoSec. The material

available varied from company to company depending on the type, methods used, and the content of the training.

4.1.1 Methods Of The Training

To start off, Company A, B, and C mainly used online courses, while Company D used mainly classroom teaching.

The online courses were mainly based on videos, pictures, and text, but they all differed in what amount of which. Company A used videos as the primary form of media. The videos were mostly information based and focused on informing the new employees. Some of the videos had a narrator who read the text on the screen and supplemented with additional information not presented on the screen, while other videos did not use audio at all. The videos also contained still images or minor animations. The still images were presented beside the text as minor examples, or in combination with the minor animations when educating on separate examples. The examples used in the videos were mostly specific guidance on different operations in systems used. In addition to the specific examples, some generalized examples were given on different sub-topics, but not consistently. In order to involve the users, the courses required different interactions from the new employees. Some courses were made to have tasks embedded so that the new employees could do the examples outside of the video format. Other courses used simple quizzes. The language used in the courses was phrased to inform and instruct the new employees on how to utilize the InfoSec they were being trained in. The courses did not use fear as a tool to change the behavior of the new employee. Instead, the courses presented instructions on what to do and how to do it. There was no indication that the new employee would be responsible in the case of an event, but the courses told the new employee that they were expected to react and tell of any event to the closest leader.

Company B also utilized online courses but did not have a single primary form of media in their courses. Each course company B provided to the new employees used different forms of primary media. The primary media forms used were video, slide show, and a video-slideshow hybrid. The courses that based of video of two different types, the first was recording of a classroom session done by a 3rd party, the second type used text, pictures and animations similar to the courses of company A. The second type of video media based courses by company B did use a narrator to read the text presented on screen, but the narrator did not provide additional information and was used more to the effect of universal design for those with problem reading. The courses with slide show did not use audio at all, nor did it use animations, both in contrast with the other courses. The slide show courses were more interactive and had quizzes embedded in several parts. The video-slideshow hybrid was a slideshow where all the slides were in video format, this included slides with only a topic header

or a picture. The new employee also had to navigate to the next video in line through embedded buttons in the videos. The video-slides with text or example content worked similar to the video courses of the second type. Video-slides of headers, images, or menus were only one to two seconds long. The courses from company B did vary in how interactive they were. Common for all the courses where that they sought to inform the new employees and make them understand. All the courses provided in-depth information. The courses did use fear as a tool to change behavior, but also provided solutions, so the courses of company B was both cautionary and instructive, but most of all, informative. The courses brought up responsibility in the context of expected behavior in the case of an event but did not go into further detail.

The courses from company C was in the form of slide-shows. The courses were well structured, starting with the goal of the course, a motivational part, the main content, an interactive quiz, and lastly a summary, all in that order. The slides varied in content, but each slide had a single aim. In general, text slides aimed to inform, picture slides aimed to explain and create understanding, video slides aimed to give motivation and give context and interactive slides aimed to provide feedback to the new employees on their understanding of the topic. The courses from company C were all informative, instructive and cautionary, of about the same level. None of the categories stuck out from the others and no was underused or missing. From the beginning of all company C's courses, the focus was on the new employees as individuals rather than employees in the work environment. All but one of the examples related to the work environment had a personal example as a counterpart, and several examples of personal protection had no work-related counterpart. This focus on the personal aspect was also present in the presentation of responsibilities. The courses conveyed that each individual was responsible for their protection and for the protection of the work they ware responsible for. The courses also stated that the InfoSec department existed to facilitate and help in the protection.

For the online courses in general, the text part of the was used to inform the recipient and provide knowledge, while the video and pictures were used to explain and provide understanding. One of the companies also used audio additionally to the text presented in their courses. The online courses also included minor elements of interactive sections. The interactive sections consisted of simple questions, or in the case of one of the companies actual tasks. The online courses were designed to take short amounts of time, the time varied done to individual courses but was aimed to take between two to ten minutes.

Company D used classroom teaching as their primary form of teaching. The training consisted of two different parts, the first part was a general 3-minute presentation, and the second part was a 4-hour session on specific topics in regards

to the department the new employee would be working in. The first session was a general introduction the teacher used a slide show for supplementary information, images, explanations, and cases, but the primary information and focus was towards the teacher. For the first half, the presentation was structured, meant to motivate, provide baseline knowledge, and to create an understanding within the new employees of the importance of InfoSec. The second half focused on information and explanation of different topics all related to the work environment. Because of the limited time, the teacher used images or headers as the only content of the presentation slides. Similarly, the teacher introduced elements of humor and entertainment in order to help the new employees remember. This entertainment was as a counter to the time limitation and the speed of the presentation. The second session was of varying length based on the department and the content, this was estimated to be 4-hours and was a combination of classroom and discussion groups. The second session had a slower pace than the first session and was aimed heavily towards concrete work-related information and understanding. Some general instructions where given, but the new employees were supposed to use the knowledge presented in their daily operations. These expectations were stated to them, but also that they should contact the InfoSec personnel about any problems. The teacher interacted with the new employees throughout the classroom part by asking questions during the first half and encouraged discussion with peers and in groups in the second half.

Company C and D also provided additional training meant for specific roles employees could have. Common for the specialized training was that they followed more of a traditional method of teaching. This training consisted of more practical and interactive methods rather than online courses. Classrooms, discussions, workshops, hands-on learning sessions were the most used methods in the specialized training. Online courses were also used in specialized training, but to a much less degree and mostly as a supportive method.

4.1.2 Contents Of The Training

The content and depth of the training provided varied widely. All the companies provided training in General Data Protection Regulation (GDPR), covering several aspects and from both user and company viewpoints. For company B, GDPR training also included user privacy outside the coverage of GDPR. In the case of the other companies, company A, C, and D privacy was covered as a separate topic with separate sessions. For company A this was the only InfoSec training provided. They did provide training and courses in a variety of topics they had labeled as non-InfoSec topics. Two of these courses labeled as non-InfoSec was it-security focused but went under the definition of financial and user handling.

The other companies, companies B, C, and D all covered the topics of passwords,

phishing, and threats to the workplace. For both passwords and phishing the problems, the reason behind problems, possible solutions, and reasons for specific solutions were explained in detail. The threats to the workplace were the most varying of the three topics. Company B focused more on the company and the employees as responsible parties, while company C focused both on the company and the employees individually. The focus on individuals extended to some courses which were provided, solely to be of use while of work. Company D focused on the users in the company when presenting the threats to the workplace. With the different focuses, the information presented varied to some degree.

Other topics were also covered, this includes social engineering, behavior outside of the workplace, general do's and do not on the internet, and measures and responding to an event. None of the companies covered all of these topics. The social engineering was by company B covered as a part of the phishing topic, while the remaining company C and D used separate sessions on the topic in different settings and methods. The same two companies, C and D, also included the topic of behavior outside of the workplace. General do's and do not on the internet were in some way included in all the three companies, but only Company B and C had it as a separate topic. Only company D went into depth on measures both preventive and responding.

All four companies made efforts to make the training relevant to the employees. This effort was either made as separate training in specific topics or as generalized examples in the regular training. Company C and D used specific training used these as additional training for employees with specific responsibilities or employees in roles with specific risks. The content and topics of the specific training varied widely with the need and focus of the specific companies. The specific training topics that were available during this project was; several versions of specific systems, several versions of system development, user and customer problems, several versions of InfoSec for leaders. Other specific training topics where mentioned, but not with specifics.

4.1.3 Organization Of The Training

The organization of the training was in one of two different ways depending on the training method used. For the online courses, the norm was that the new employees would be informed of the online platform and was themselves responsible for taking the required courses in a timely manner. On the online platform, the courses are also repeatable and continually available for the employees. In companies A and C, with online courses, the responsible party, boss or department could follow the progress of employees on the platform.

The classroom training of company D was set up when needed. The first part of the classroom training was, on average, held once every month. This presentation

was one of several lectures in a series of different topics. The second part was held by the different departments when needed. This second part was, on average, held once every second month. The topics of the second part were held separately from any other topics. Neither the first or second part of the classroom training was available to the employees at a later time.

The different companies had very different guidelines for what was obligatory, recommended, or only available. For company D, who used classroom training, everything was obligatory. Company A had no required courses, only recommended courses. Company B had required courses and some available videos. Company C had a mix of required and available courses. The online courses also followed the pattern that general courses and specialized courses employees qualified for was obligatory, additional content to the general courses where recommended, and specific courses, in general, was only available. The specific courses that were not online varied in whether they were available to all or needed registration from a boss or supervisor.

The decisions on what employees roles who qualified for specific courses were similar in all the companies who used it. The process locked at what responsibilities the employees would have in different roles combined with reassessments on the different threats. If an employee had a role linked to a risk, and that risk had a course as a countermeasure. That specific course became obligatory or recommended to that employee.

The companies who used online courses varied widely in the number of courses offered. The time needed in order to complete the required or recommended courses for the different companies was 15 minutes for company A, 55 minutes for company B, and 2 hours 10 minutes for company C. The time needed to complete a single specific course was between 15 minutes and 8 hours. The number of different specific courses obligatory or recommended to an employee was also highly variable.

4.2 Interview

The interviews were done with representatives from the companies who were responsible for the education of employees in InfoSec. The interviews gave a deeper understanding and showed the differences between the companies on a higher level.

4.2.1 Confirmation Of The Case Study

The first question of the interview was how the interview object would describe the current InfoSec training for new employees and regular employees. Company A answered that they had very little in terms of InfoSec training in general. What

little they had was meant for both new employees and regular employees. In terms of general security, company A claimed to have quite a lot, most of which were required by law. The company used 5-15 minutes long courses for both InfoSec related and non-InfoSec related, all gathered in an online platform. All of the courses they had on the online platform where developed in-house and the only use of any third party was with animations or actual hosting of the platform. Further, they stated that the whole process around the content, registration, completion, and follow-up of courses was well documented, partly because of what the online platform enabled.

Company B stated that they used courses on an online platform. They had previously relied heavily on third-party InfoSec providers for courses and content, but was in the process of in-sourcing the courses in order to have ownership, better control and became less reliant on the third party providers. The courses and content provided by the third parties were a mix of recorded classroom sessions, a few online courses, and slide shows. The courses developed in-house were online courses of 5-10 minutes in length. The topics and content of the in-house courses were told to be of high quality, but there were problems with imparting this knowledge to the new employees. The company had tried out different combinations of types of media, no specifics where mentioned, but were still dissatisfied. Company B also mentioned testing and InfoSec events throughout the year. These secondary InfoSec events were not meant for the new employees specifically but as reminders, and to push the regular employees to review the courses and their content. The new employees were included in these events from the start, regardless of their progress with the online courses. The testing was measurements on their employees as phishing emails or basic spear-phishing, done by third-party providers. The results from this and other tests would determine what topics of InfoSec events and training would focus on.

Company C Stated that their InfoSec training was a part of a larger InfoSec culture program. The InfoSec training was for most new employees general training, which was both aimed for and obligatory for everyone. When the new employee was employed, they got access to the online platform and became registered for the general courses. All of the general courses were online self-learning sessions. The session was made short to fit into the concept of nano-learning, only 2-7 minutes. The general courses covered a range of seven to eight essential topics, with some of the topics divided into several courses. The general training started with what was seen as the most relevant to the work environment and ending with what was relevant to the new employees personally. On the online platform, the progress of the new employees could be followed by the InfoSec department and the closest boss of the new employee, both of which could prompt more progress of the new employee. Additional to the general training, some employees got more courses related to their roles. Some of the courses related to different roles had previously been classroom sessions, but this had changed to online self-learning due to resource limitations. In

order to not loose interactive pars of the classroom training, more events in the form of InfoSec games and challenges were used, but not limited to the new employees. Some of the unique employee roles that received specialized training did so through media outside of the norm. This training was limited by not allowing followup, prompting, and testing to the same degree as the standard ways of training.

For new employees in company D, the InfoSec training started with a classroom or lecture as a part of several sessions about them being new in the company. The InfoSec session lasted 30 minutes and was presented by the CISO. The first session aimed to give an overview of the reasons behind the training and to motivate the new employees. As a part of this motivation and overview, the risk and threats towards the company were introduced in detail. All other topics of the training were introduced but had dedicated online courses. Different departments received specialized training when it was needed, and only for the new employees who would qualify. The InfoSec department had an overview of the InfoSec training in the departments but was not further involved in this training. The InfoSec training in the departments based heavily on the tasks of the new employees. These tasks required information and understanding on deep levels, so the training was focused on providing this.

4.2.2 Planing And Measures In Regards To The Training

The InfoSec training of employees needed like any other part of the InfoSec system to be based on and constituted with the top management or the board. This agreement was specially mentioned by company C and D, who both told of excellent and good relationships respectively. Company A told that they had little to no constitution or support with the top management. This lack of any jurisdiction meant that getting employees to do any form InfoSec training was difficult because it was not a part of their stated work tasks. Company B spoke of the cooperation with upper management as work in progress. They had general authority to make use of other employees time, but some specifics where missing and documents to finalize it was in development. The support from and cooperation with the upper management also reflected in the relationship between the InfoSec department and other departments or support functions. Human Resources (HR) was the only department mentioned by all the companies, as they were responsible or partly responsible when hiring and handling new employees, but the company C and D told of departments in general as well. Company B, C, and D all mentioned a positive relation with HR was crucial during the onboarding and follow-up of the new employees. Company C also mentioned the importance of good cooperation with other departments when arranging or coordinating other InfoSec activities. A follow-up question to the constitution of the InfoSec training was, how the new employees or employees, in general, were beholden to any InfoSec policies. In company A, new employees would

when signing the contract, agree to follow the companies general work policies, which were referenced but not written on the contract. These work policies referred to the InfoSec policies, which again was a separate document. The new employees themselves were responsible for finding and reading this policy. Company B and C told of a similar chain of documents, but that this was provided to the new employees and included in the InfoSec training courses.

On the question of why the companies used the InfoSec training, all the companies give generic answers, that they wanted to improve the overall protection of the company, and that humans are in general the weakest link. With the follow-up question of why they train new employees specifically, company A stated that there was no focus on training new employees in InfoSec. In general, there was a lack of focus on InfoSec, hence also any form of InfoSec training. This problem was first described by company A as the InfoSec department not having the authority to make people take any courses. Secondly, it company A told that resources and funding to any InfoSec training was also lacking. Company B answered that it was a step in the onboarding process. This was further explained in that some none-InfoSec training was already in place. The InfoSec training was combined with this existing training in the onboarding process. The focus was not on training new employees in InfoSec, but the training of new employees in general. Company C and D answered similarly to Company A and B but gave more detailed and in-depth answers. They answered that the main reason was that the pre-existing InfoSec knowledge of the new employee was low, due to most of them not having practiced or learned about InfoSec. Because of this, and the fact that they needed to perform on an expected level in InfoSec before they could be of use, InfoSec training was required. Company B, C, and D did include arguments of learning correctly from the start rather than relearning and utilizing the new employees safely from the start, and for company C and D incorporating the new employee into a good InfoSec culture as early as possible was mentioned as other minor but important reasons.

In regards to how the InfoSec training was made and arranged, the different companies had different verities of the same answers. Company A who had little InfoSec training, told that the training of new employees was more standardized across the company, not only for InfoSec. The training which existed based on a couple of things. In the context of company A, laws and legal obligations would be the first part that affected the training activities and its content. Secondly, some training aimed at improving different aspects of the service the company provides. Company A referred to the second point as the part where InfoSec training would apply. The requirements for each part could also affect the training method, this was mostly related to the first point. Due to resource use, online self-learning was the only reasonable training method. A risk analysis of the company existed and was intended to be, among other things, the basis of InfoSec training, but general

problems with imposing the use of employees time on InfoSec prevented this.

Company B based the content of their training on statistics of most frequent attacks towards their company and public sources that are giving statistics for different attacks or exploits. Older risk analysis existed and had been of use, but testing provided by third-party providers gave more up to date information on the behavior and treats of the employees. Using this as a basis the InfoSec training had been formed but was still in the process of finalizing. As stated earlier, company B had previously relied much on the use of third-party providers of InfoSec in general. This context was beneficial as the company did not start empty-handed, nor did they start with previous, unfinished, or undocumented work. When the new employees started, they would already be registered on the online course platform with all the courses they needed. The online platform used by the company did not currently allow for the follow-up of individual new employees, so the testing of the new employees and employees in general, was necessary.

Company C had a more thorough explanation. Through a documented model shown in the interview, they analyzed the goal of the hole InfoSec topic for the company. In regards to the training of new employees in InfoSec, the goals, motivations, preexisting knowledge, connections between different parties and general point of view was analyzed form all involved parties. This knowledge was then used to determine the guidelines of the content and executions of the training. The risk analysis of the same points of view was hence applied to determine content before testing of different variations. This all concluded in the method and content of the InfoSec training of new employees. This was also used in the method and content of the InfoSec culture program in general. The InfoSec department in company C had received extra resources and legislation to make use of other employees time. The extra received recourses gave the possibility of testing different approaches and methods in a sandbox environment. The InfoSec training of new employees was reviewed on a yearly basis, among other reviews of the InfoSec system. The online platform in which company C hosts their courses does allow follow-up of course progression of individuals. Follow-up of course progression was through the closest boss on behalf of the InfoSec department when needed. Company C did not use any third party InfoSec providers. It was explained that third-party providers were not needed. The company had enough resources to develop and maintain its private InfoSec systems, and hence also control it. Third-party online resources also tended to change outside of the control of the company. The only use of third-party providers in company C were special lectures and presentations as a way of showing that InfoSec was used and essential outside of their company, and to evaluate their private InfoSec system from an external viewpoint.

As the InfoSec training of company D was split into two parts, the decision

making and planning also were handled separately. The method and content of the first part were under the control of the InfoSec department. The method and content of the second were under the control of the individual departments. For the first part, which included general training and topics, the content was decided based on public information about threats, attacks, and their frequency. This was combined with threat estimates towards the company. The InfoSec department had developed the InfoSec training in-house. The second part of company D's training of new employees was a documented process that had been in use for quite some time. This process had been developed in the department and was reviewed regularly based on feedback from previous uses. The content was that which was required by law, contracts, or in order to solve daily tasks. The reason for choosing the classroom and discussion method was not clear, but the lecturer was positive that it provided everything the new employees needed, as well as feedback to the lecturer and the possibility to repeat or further explain topics based on live feedback. Both the leader of the first and second part of the training could not tell of why specifically the chosen training method had been chosen, but both referred to test and feedback that it was successful in its goals.

4.2.3 Education Of Normal Employees And Feedback

For company A, there were no active follow-up of InfoSec training or training for regular employees from the InfoSec department. There was also no testing of employees InfoSec awareness.

Company B's education of regular employees consisted of different topics among the online courses. During the focus period, the employees were encouraged to review the online courses, participate in talks or lectures on different aspects of the topics, or examples such as live hacking, and were sent newsletters. Before a focus period and after the focus period was finished, there were tests. These tests were used to give a more accurate picture of the company's standing on the given topic as well as feedback on the focus period.

As a part of the InfoSec culture program in company C, several InfoSec events are arranged throughout the year. These were mostly focused around the national InfoSec month of October, to ensure no collision with other events arranged within the company, but minor events were arranged all around the year. The minor events were often limited to smaller groups in a different context, as not to affect other company wide events. The event arranged from the InfoSec department included lectures, talks, presentations, stands, emails encouraging specific courses with low test scores, quizzes, news emails, competitions, capture the flag exercises and posters or articles on the internal network. New employees were also apart of these InfoSec events even tho they not necessarily had completed the online courses. Tests were

also being done all around the year. These tests were not linked to different InfoSec events but were run separately and were used to determine the focus of different InfoSec events.

Company D did InfoSec events on a regular basis, these InfoSec events included talks, presentation of company statistics from tests, stands, and live examples. Vague descriptions also mentioned other InfoSec events but without examples. Tests of the InfoSec awareness of the employees were done on a semi-regular basis. These tests were then used to evaluate InfoSec events, and report to the upper management.

4.3 Questionnaire

The questionnaire was done separately on the four companies. The number of recipients and the number of answers received from each company was hence also different. Unfortunately, company A was not able to acquire the contact information of its new employees. So the questionnaire was not distributed within, and hence no received answers from company A's new employees.

From the questionnaire, the majority of the new employees answered that they received their first InfoSec training after 0-2 months. After 3-4 months, more than 86% of the new employees had received some form of InfoSec training. The rest of the answers was either 11-12 months, more than 12 months or "do not know" as seen in 4.1.

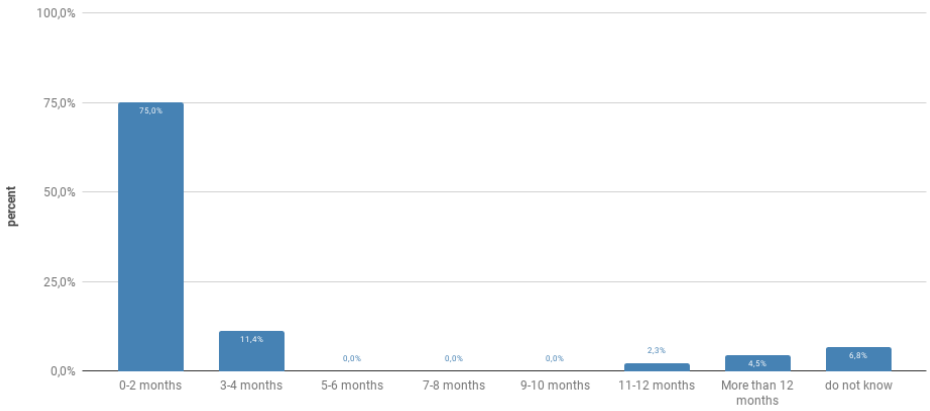

Figure 4.1: How long after hiring did you first get information security training?

From the question "How was the information security training conducted?", we see that the online courses were the most mentioned (4.2). This was followed by

discussion, self-learning, other, lecture, and classroom in that order. Looking at the companies separately showed that: For company B, 29% of the new employees meant that the InfoSec training contained discussion and "other" methods respectively, while only 52% included online courses in their answers, self-learning was at 14%. The answers from company C contained mostly online courses at 77% and self-learning at 31%, still, discussion was mentioned at 23% and lectures at 15%. The answers from company D contained the highest percentage of online courses at 83% with classroom, and lectures all at 17%.

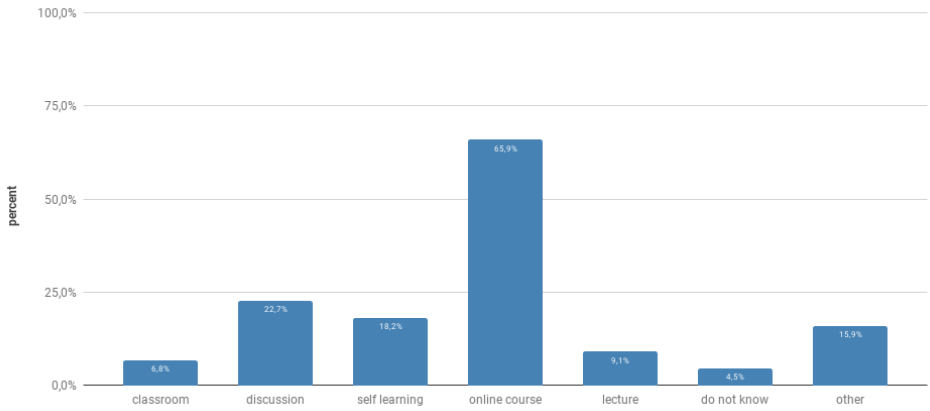

Figure 4.2: How was the information security training conducted?

On the question of "What topics do you remember was included in the training?" roughly half of the new employees, did not write an answer. Of those who did answer, another 20% answered with different versions of the text "I don't know" or topics unrelated to InfoSec. Of those who answered with InfoSec related topics, 56% of the answers contained privacy, 44% contained general security measures on the internet, 28% contained password, 24% contained e-mail and phishing and 24% contained hackers and attackers in general.

The results from the question "To what extent do you find that information security training was related to your duties?" is shown in figure 4.3. These show that most of the new employees found that the InfoSec training related to a large or very large extent to their regular duties. Most of the answers received that was very minor, minor or neutral extent was received from company C. Combined, only 60% of the new employees in company C answered large or very large extent. Both company B and D was similar to the combined answers.

By figure 4.4, most of the new employees answered that they either were neutral

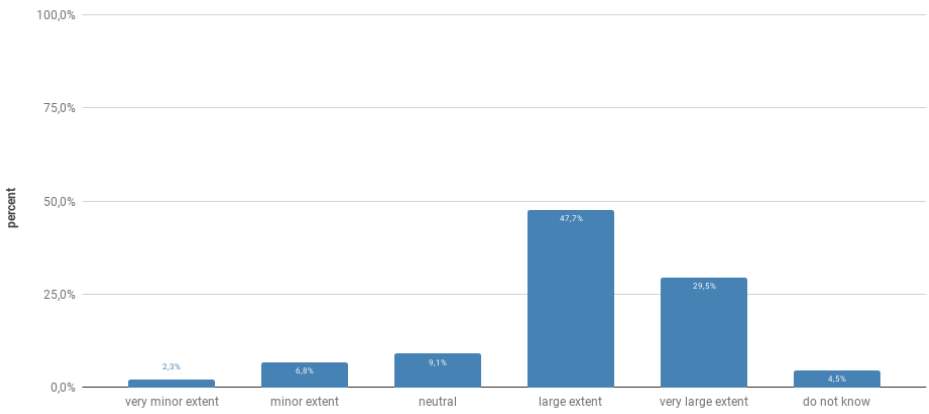

Figure 4.3: To what extent do you find that information security training was related to your duties?

or to a large extent, learned something new from the InfoSec training. More people answered to a minor extent at 19% than to a very large extent at 12%. For the individual companies, the majority of the neutral and minor extent in the combined results was from company C. The majority of the large extent answers were from company B. Company D was equally divided between minor extent, large extent, and very large extent.

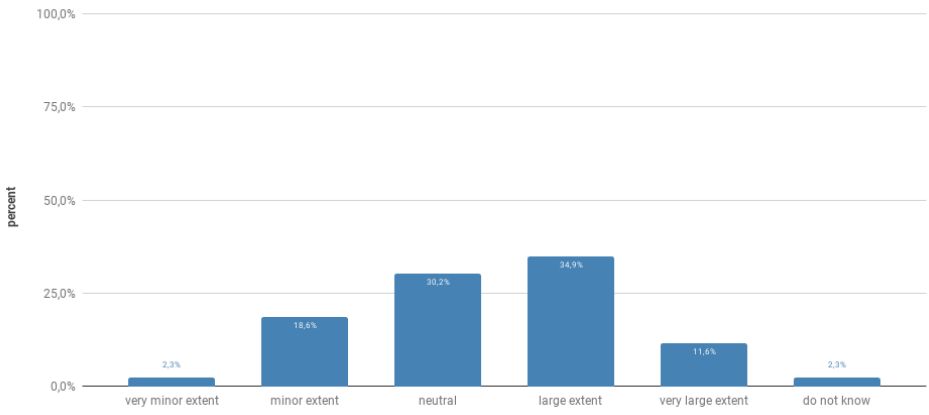

Figure 4.4: To what extent did you find that you learned something new from the information security training?

The combined answers to the question "To what extent did you find that the training was oriented towards the risks towards the company?" was focused around the "large extent" option (4.5). Company B and D had similar answers when looking at them individually, but they were not as spread from the "large extent" option. The answers received from the new employees in Company C had the majority of its percents on the "large extent" option at 46%, but the "neutral" and "minor extent" options received 15% and 31% respectively.

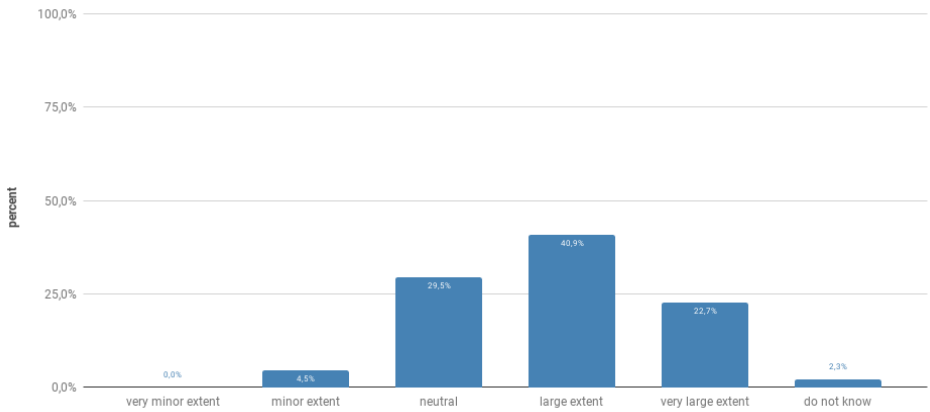

Figure 4.5: To what extent did you find that the training was oriented towards the risks towards the company?

When asked if they perceived the InfoSec training as cautionary, a combined 61% of the answers were positive, with the majority of those answers being to a large extent at 44% (4.6). With some variety, all the companies followed patterns similar to the combined answers.

In figure 4.7, to the question "To what extent did you find that the training was instructive?" the majority of the total answers was to a large extent at 51%, combined with the "every large extent" option 68% of the answer was on the large extent side of the spectrum. The neutral option was 26%. From company B, the answers were 86% large extent or very large extent with 10% neutral. Company C had 58% large or very large extent and 33% neutral, and company D had 50% neutral and 33% large or very large extent.

To the question "To what extent did you find that the training was informative?", the combined answers were 65% large or very large extent and 28% neutral (4.8). Company B and D followed this trend and had no answers in the negative. Company C had 46% to a large extent and 39% neutral, the rest is negative.

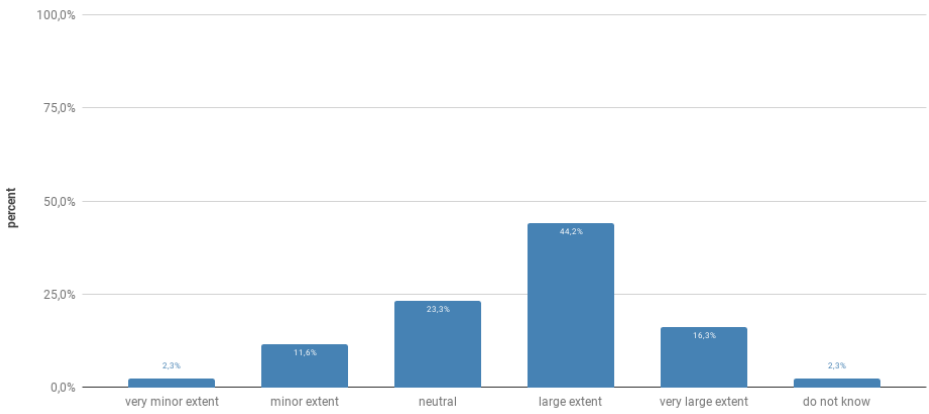

Figure 4.6: To what extent did you experience that the training was cautionary?

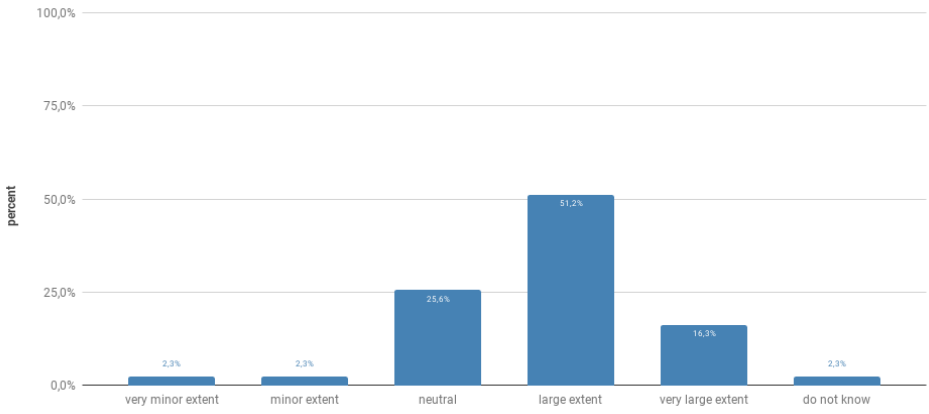

Figure 4.7: To what extent did you find that the training was instructive?

When questioned if the new employees thought they had improved their InfoSec skills after the InfoSec training, the combined results showed that the majority of the answers where positive. The results were also showed a greater verity and difference in the answers than previous questions (4.9). The large and very large extent was only 52% of the total answers, the neutral being 30% and the rest being minor extent or very minor extent. On the company level, company B had a combined 77% in the large and very large extent options. Company C answered neutral at 46% minor and very minor extent at a combined 39% and a large extent alone at 15%. Company D

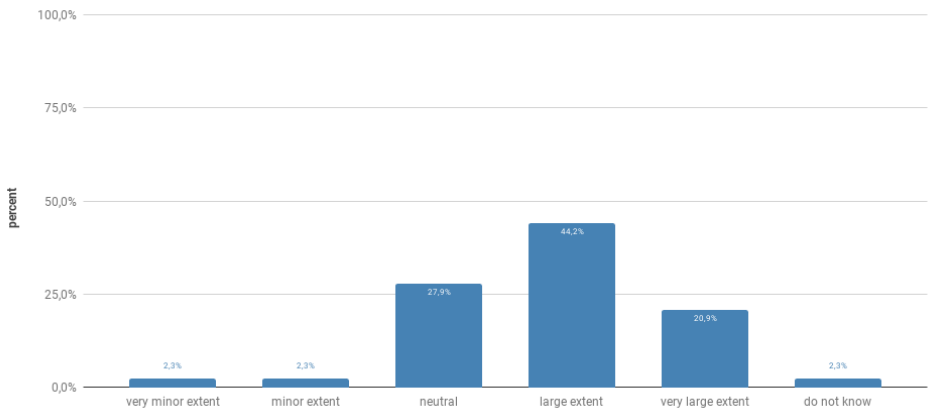

Figure 4.8: To what extent did you find that the training was informative?

had 50% ad neutral answers and 50% at a combined large and very large extent.

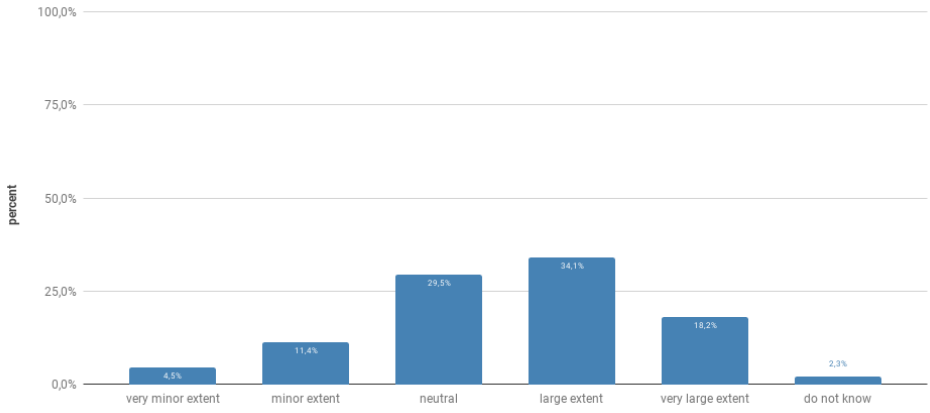

Figure 4.9: To what extent do you think you have improved your skills after training in information security?

Figure 4.10 shows the combined answers to the question, "To what extent do you use what you have learned in information security outside of work?". The graph shows that the majority of the answers being to a large extent at 56%, and a very large extent and neutral both receiving 16% of the answers. Individually in all the companies, the large extent option received more than 50% or the answers. In

company B and D, the very large extent option received the second most answers followed by the neutral option. In company C neutral was the second most answered option with very minor, minor, and very large extent, all sharing the rest equally.

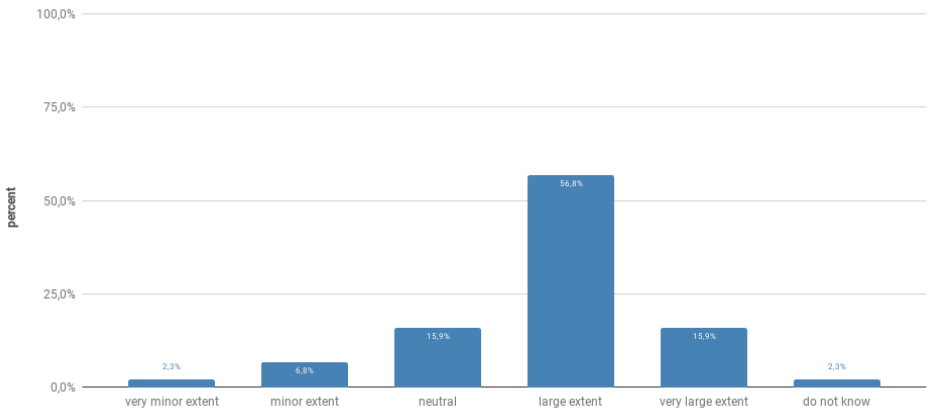

Figure 4.10: To what extent do you use what you have learned in information security outside of work?

For the question "To what extent do you want more information security training?", the option with the most answers was neutral at 33%. Neutral was followed by to a large extent at 31%. The rest of the protons was between 6% and 11% each (4.11). Looking at the answers from company B, the most answered option was neutral at 40%, large and very large extent at 34% combined, and minor and very minor extent at 13% combined. Company C had most answers on the large extent option at 44%, 32% at the neutral option and 16% on the minor extent option, very minor and very large got 4% of the answers each. In company D, the neutral, large, and very large extent options got 33% each.

On the question "what information security activities have been arranged at the workplace outside of training", the majority of the answers were "do not know". From the rest of the answers, phishing campaigns, other, talks, newsletters, and stands as the most common answers respectively.

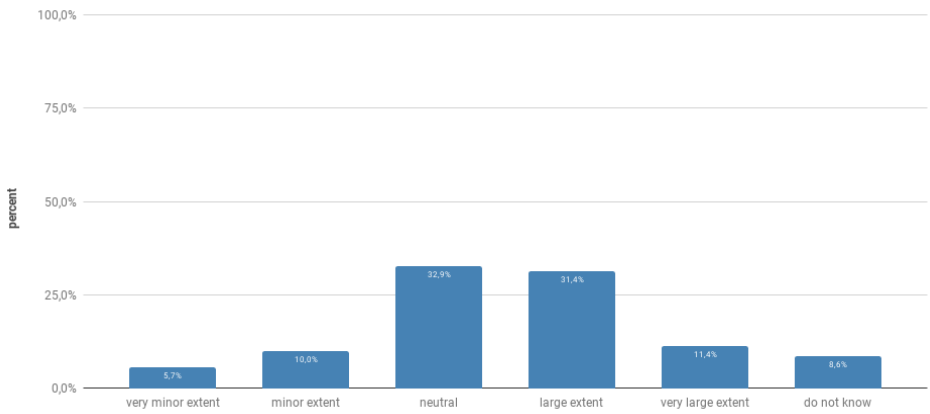

Figure 4.11: To what extent do you want more information security training?

Chapter 5
Discussion

This chapter is a discussion of the material and results presented in the previous chapter. The discussion will start with the research question one and continue throughout research question four. Lastly comes some discussion on the method of this research project and possible future works.

5.1 New Employee's Training In Information Security

The training of new employees in InfoSec was by all the companies done through mostly online courses. This did not appear in the case study of company D, but both the interview and the questionnaire confirms the use of online courses. This indicates that the InfoSec training of company D was more extensive than what was in the classroom training. As the specialized training needed in the different departments was covered in the respective departments, and from the content of the first classroom part provided by the InfoSec deportment, it is likely that the content of the missed online courses was more in-depth information and training on the general topics. The involvement of company D in this research project was done in one of the departments, and was the information was for the most part located in that specific department. The online courses of the company belonged to the department of InfoSec. This is probably the reason why the online courses were not included in the case study of company D.

When asked why they choose online courses or self-study as their primary form of training for the new employees, the general consensus from the companies was that it was the most resource efficient. Several arguments were told as to why this was the most resource efficient, most of which was dependent on the companies the self and their context or situation. The arguments that were common among the companies was: All the companies had some non-InfoSec courses already provided in an online platform by the HR department. This matches with Petri Puhakainen and Mikko Siponen's [PS10] findings, that InfoSec training combined with other

work-related training or tasks gives a more positive behavior change. This seems not to be intentional. The online platforms where also able to provide follow-up of the course progression. In the case of company B, this function was possible to some degree, but not on an individual level. The last commonly mentioned benefit was the minimization of the new employees time usage. As the InfoSec department had limited authority over the time usage of the employees in general, the less time needed to complete any training, the better. With online courses, this was possible without the quality dropping.

5.1.1 Details About The Information Security Training

Knowing about the online courses and the reasoning behind, the next logical question became how were the new employees trained in InfoSec using online courses. The online courses were developed and made within the company's InfoSec department. None of the InfoSec departments had any educational oriented human resources or used any third party providers to build the online courses. This is where the companies differed the most. As the companies did not have any educational help, they used what they had available. Company A used existing courses on other non-InfoSec topics, company B used previous third-party providers as inspiration, while company C researched and sandbox tested in order to make their own template. The resources and available to the InfoSec department clearly played a role in this development. With the use of educational resources to structure and develop the courses, the courses themselves would likely be more effective.

The online courses them self was either a slide show or video based. Going into details, all of the companies A, B, and C had a mixture of text, images, audio, and video in their online courses. The individual companies also mixed some of the media types in different combinations during their courses. In the courses from company A, the factual information was presented mostly with audio, either in a video or while presenting summarised bullet-points or images on the screen. Company B had instances where their courses did provide information in isolated text form, but this was sporadic, and in most cases, the text was combined with audio reading the text, video or presenting images and examples on screen simultaneously. From the results of R.S.Shaw, Charlie C. Chen, Albert L. Harris and Hui-Jou Huang [RH09], when the purpose is to inform and improve the recipient's perception of the material, text only was the best solution. Company C did just this when providing information. They utilized slides with text only so the new employees could read and perceive the information at their own pace. In the instances of company B, when the text presented on screen was read to the new employees through audio, it was perceived as facilitating for people with hearing aid. This was the only such case observed, and it was unclear if this was its intent, the lack of other facilitating features makes this unlikely.

The article of R.S.Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang [RH09], also found that multimedia material help users with comprehension and understanding. Multimedia in their report is defined as a combination of text, image, sound, music, animation, video, and virtual reality used in a linear sequence. Company A, B, and C did utilize all of these in combination with the exception of virtual reality. The combinations where often only some of these, limiting the simultaneous usage, but R.S.Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang does not mention anything about specific combinations. Throughout the multimedia sections or the online courses, no parts were found to deviate from R.S.Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang findings.

The final part from R.S.Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang [RH09], was their finding that hypermedia-based instruction was the most effective way of enhancing the InfoSec awareness in the recipients. Hypermedia was defined to be similar to multimedia, but with text and interactions added media, and provided in a nonlinear way, such that the recipient could navigate between topics or within a specific topic. The closest relation to this in the case study was the online courses in general. The courses who used the form of slide shows utilized this on a lower level, but in general, it utilized only on the online platforms. The scope of R.S.Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang's project does not include any mention of interactive, or relevance

Although most of the educational use of the media matched what research suggests, it was based on the person making the courses perception and ideas of the educational methods. For the employees to get the best possible situation awareness, these tools should be used more efficiently to the gain of both the new employees and the company. With the current usage of these tools, the situational awareness is developing slower than what would be possible.

Other uses of tools and aids include the use of examples, which have shown to be of huge impact in InfoSec training in general. Several articles have found that examples who are relevant for the receiver of the training, will provide a better effect that examples who are not [PS10, KS11, PMX14]. All the companies did this to some degree. The examples of company A and B were more general, all tho they matched the topics, and the topics were relevant for the new employees, the examples had not been customized to match the companies. Company C and D customized the examples to a larger extent. Company C and D did so by providing additional topics when relevant, and to use examples puled previous attacks towards the company in their examples. Company C also provided examples without any attacks. This was done with the intent of enhancing the experience of the new employees regarding the real situation where it might be an attack or not. The intent was not to trick the new employee as they were told of there being no attack in the example. Such a trick

would only have served to make the new employees suspicious and distrustful of the training itself, which may then have carried over to the behavior after the training. It would be harder to find any examples more closely related than that of previous attacks, so these examples seem rather good. Using so closely related examples and providing solutions to them makes it easier for the new employees to use what they have learned, and change behavior. This matches the reports from Cormac Herley and Mete Eminağaoğlu, Erdem Uçar and Şaban Eren [Her09, ME09], to make the usage of InfoSec less complicated and less of a strain on the users. However, it comes with the price of not necessarily having a comprehension of what they use. Missing the building block of comprehension will lessen the effect on which the new employees can project their intentions through their behavior [RH09]. In the end, this comes to the discussion of how high of a InfoSec understanding and awareness the training aims to provide.

The same articles who found that work-related examples had a positive effect also found that InfoSec training relevance to InfoSec pre-knowledge of the recipient also had a positive effect [PS10, KS11, PMX14]. All of the companies had made their starting InfoSec training to require no pre-knowledge. With the exemption of the new employees who have received InfoSec training on a previous workplace, this matches the findings of NorSIS [MR16, MR18]. As InfoSec culture is varies depending on the workplace, that the relevance to pre-knowledge is only one factor affecting the behavior change, and that the InfoSec training introduces the new employee to the InfoSec culture of that workplace that. Those who start with pre-knowledge would not be affected in the negative for the training not being customized to them.

The InfoSec training of new employees for all the companies would be subject to similar problems of other InfoSec training, that of the user's perception. This is explained by Michael Workman, William H.Bommer and Detmar Straub [MWS08] as the PMT (2.2.1) in effect.The PMT is the perception of the weakness, perception of the consequences, and perception of the effectiveness of the countermeasures, in regards to the behavior of the target. For the first of the three points of perception, none of the companies A, B, C, or D addressed the weaknesses directly. The point of the training and education of new employees in general, is to improve the weakness of said employees. This might mean that the weakness is implicit, but the new employees might not pick up on or understand the implication. Similarly, the goal of the InfoSec training is to change the behavior of said employees, which indicates that the behavior is the weakness. Alternatively, the whole course or session may use it as an underlying statement. There is also the chance that the weakness was not mentioned to the new employees. This may be as it was not deemed necessary by the course creator or the lecturer, it may also be that it was not included due to humans not wanting to see their own faults. The fact remains that the case study did not find any evidence that the topic was mentioned specifically or indirectly. Because of

this, it is likely that the topic was not included.

The second point of perception, the perception of the threat, was covered by all the companies. Neither of the companies used fear or emphasized the threats in an excessive way. The companies stated the threats and tried to explain them to the new employees rather than using it to enhance the drive for more protection. Especially in company D, the threats were explained in detail, covering several aspects and viewpoints outside of what would be strictly necessary to ensure the perception of the threat itself. The goal of this approach is not clear from the case study, but it seems that the companies aimed to give an understanding and explain the reasoning of the attackers rather than creating fear. This also helps with creating an understanding of the third point, the perception of the effectiveness of the countermeasures. Knowing the goals behind the attacks and the countermeasures used, the new employees could gain an understanding of why the countermeasures were useful. This also matches what the findings. The effectiveness of the countermeasures was not the main focus of the InfoSec training in any of the companies; the countermeasures them selfs where. The effectiveness was underlying when explaining the measures and why they worked. The logic behind the countermeasures was explained in the underlying explanation as "If you open a mail PDF attachment you might get a virus. So don't open mail PDF attachments". This alone would have put the new employees in a dilemma as this solution would not always hold through, similar to what Cormac Herley argues for [Her09]. It is likely that this is the reason for the focus on how the new employees should make the decision. All the companies provided guidelines or explained how to investigate if the action would, in this example open a PDF attachment, would have negative consequences.

This is comparable to Mikko Siponen, M.Adam Mahmood and Seppo Pahnila [MSP14] who combined the PMT with the TRA 2.2.2 and found that the perception of the severity of the consequences, perception of the vulnerability or weakness, perceived self-efficacy, normative beliefs, and attitude all had a positive effect on the intention to comply with policies. The first two points match with the discussion in the paragraph above. The perceived self-efficacy is part of the purpose of the InfoSec training of new employees. Similar to the perceived effectiveness of the countermeasures, it is not a specific topic but underlying all the individual topics and their countermeasures. The normative beliefs and attitudes fall into the InfoSec culture in general. The training of new employees in InfoSec is one of several ways to affect the norms and beliefs in the new employees and improve the InfoSec culture.

A tool used in order to motivate and increase the perceived importance of the InfoSec training is support from upper management and leaders. Petri Puhakainen and Mikko Siponen [PS10] discusses this, and it may be a way of improving the intention to comply and the norms of the workplace. This was visible only in the

material from company C and D. In company C the CISO was shown on motivational videos before and after a session, in addition to the followup of course progression by the InfoSec department through the closest leader. In company D, the first session was held by the CISO, and the second was held and followed up by other leaders.

Lastly, it is a point to discuss the InfoSec training against the project of Mari Karjalainen and Mikko Siponen's, on how training users in InfoSec is different from training in other subjects. [KS11]. The four significant points their report finds should be included in any InfoSec training system is concrete examples, reflective observations from the recipients part, abstract concepts and generalization, and active experimentation. Of these four points, the concrete examples have been discussed in the paragraph above. The explanation of the second point is that users should take experiences or examples and reflect on the possible implications for the company. Surprisingly this was not used to any significant extent in the InfoSec training in the companies. In the training, it was explained that machines could be compromised, which again would lead to information being stolen, or the servers of the company becoming blocked, resulting in no service and loss of information. This was the general explanation given in the training of company B, C and D. The third point, abstract concepts, and generalization are meant for the recipient to be able to analyze and generalize the experiences or examples to find similarities and differences. This was only done by company C and D, and only in that the examples provided were so close to the reality as possible, shown cases that were not attacks, and tested the new employees on other similar examples afterward. The abstract part was so that the user had to find similarities in the tests. During the training itself, there were no examples or explanations on abstractions of the specific cases. The abstraction seemed to be removed in favor of more specific examples if it was ever included. There were no results found to match any better with this point in Mari Karjalainen and Mikko Siponen's findings. The fourth and last point, active experimentation would allow the users to practice the projection of their knowledge and skills in a safe environment. The minor test or quizzes in the training was the closest to this point. The all the companies used this but, the quizzes and the minor test is a pore substitute for tests out in the context of their actual work tasks. Because it stands so relevant, it was surprising that only the first of the four points was used in any significant degree. This, along with other parts, discussed argues that the development of the InfoSec courses are done without any significant consideration of the educational aspects.

5.1.2 New Employees Compared With The Regular Employees

When comparing the InfoSec training of new employees against regular employees, it was found that regular employees were not trained as directly. The InfoSec department or other equivalent was working to motivate and remind the employees to

be aware. This match Mete Eminağaoğlu, Erdem Uçar, and Şaban Erenc's findings. [ME09]. This system of reminding and motivate also worked quite well with the testing of different topics, allowing to remind on the topics that needed it, and hence being more effective. This is under the topics of InfoSec culture rather that InfoSec training alone. In the companies, the InfoSec training was actually a part of the InfoSec culture program. The InfoSec training that regular employees received was the same online courses that new employees received, but only if they themselves wanted or was prodded due to poor test results. Also if a new course where available the regular employees would be required to take it and be followed up on the same basis as new employees. In these cases, the regular and the new employees would be considered the same.

From the InfoSec training perspective the actual training of regular employees is done the same as for new employees. This is fine educational-wise but does limit the progression of the individual. Any employee seeking to educate themselves further would need to seek outside the InfoSec training provided in the companies. Dependent on the company and its situation the primary goal of the InfoSec training is not to get individual employees to the highest level, but rather to get the employees collectively on a higher level with no weakest link among the employees. The InfoSec departments could facilitate higher levels of learning, but it was the impression of the companies that this would not be useful.

5.2 Content Of The Information Security Training

The factors determining the content or topics of the training was by a combination of common threats and risks, the risk assessment towards the company, and when available the statistic of the attacks being used agents the company. The most common threats referred to were simple attacks, the likes of phishing, targeting many and hoping someone takes the bait. The risk analysis and the statistics of the most common attacks against the companies varied dependent on the companies context. In general, the same type of threats was the most common, with the risk analysis suggesting simple training as the best counterpart. This matches the reports from NorSIS [MR16, sfi17, MR18] that because no previous InfoSec training have accrued, with the exception of a minority of previous jobs. Most people need only simple InfoSec training to gain considerable improvements. Company B, C, and D did not argue using this report as the reason to focus on simple threats in the InfoSec training of new employees. They argued that new employees were observed to have mostly no pre-knowledge in InfoSec, and in order to include everyone and not create a weak point, they needed to start with simple threats.

The specific topics used in the InfoSec training of new employees is mentioned in the chapter 4.1.2. Company A was shown not to have much in the case of InfoSec

training for new employees or employees in general. They did have training in privacy as required by law, but nothing else. The rest of the companies, companies B, C, and D provided general and baseline InfoSec training. The baseline training provided simple topics by InfoSec expert standards. This again matches the NorSIS findings [MR16, MR18]. The topics also matches the topics listed in NIST's report about setting up a InfoSec training system [WH03]. The specialized training provided by company C and D was meant as additional training for those with the extra risk associated with their roles. These topics were not mentioned by the report from NIST and required the baseline or general knowledge of the first part of the training. For all the companies, a common factor is that the InfoSec training was based on law, agreements, or other forms of contracts within or outside of the company. The support or contract between the upper management and the InfoSec department has a huge say in the method and content of the InfoSec training.

5.3 Reasons New Employees Are (Not) Trained In Information Security

All the companies want to protect their assets and resources. In other words, all companies want their resources and assets to be used for their profit, and not to be misused or stolen. The InfoSec training of new employees is only one measure to achieve this. The InfoSec training has shown to be a process requiring resources outside of the jurisdiction of the InfoSec department. For this reason, the relationship between the InfoSec department and other parts of the company have shown to be of great importance. Use of employees time, cross-department managing and collaboration with other departments is only some of the cases where resources outside of the InfoSec department is needed. The most important of these have shown to be the use of other employees time. Without time from the other employees allocated to InfoSec training, there can be no InfoSec training. This was an important part recognized in all the interviews. Those with a proper mandate from the upper management had, in general, a good InfoSec training process. Those with temporary or lacking mandate had poorer InfoSec training process if any at all. It is unknown whether it is the same problem with the companies who declined the invitation to join this research (4), but it is somewhat likely due to some similarities with those companies and company A and partly B. Further, the collaboration and cross-department managing, especially with HR was told to affect the effectiveness of parts of the InfoSec training. Again because resources outside the ordinary jurisdiction are needed by the InfoSec department. This is partly what Whitman and Mattord [EJ16] mean when discussing other placements of the InfoSec department, rather than traditionally as a part of the IT department.

Never the less the collaboration with other parts of the company has shown to

be the most important aspect as to why companies do not train new employees or employees in general in InfoSec. One fact that became apparent was that all the companies trained their new employees in InfoSec topics directly required by law, or in cases where it was directly needed to complete the new employee's tasks. In these cases the main drive force was not the InfoSec department, but often upper management, HR or the baseline workers and their direct bosses. The more specified problem was the indirect or general InfoSec training without a direct relatable. The main drive force for this is the InfoSec department. With a lacking understanding of the cause and effects, the other parts of the companies did not see the benefits. This, combined with limited jurisdiction in the company, was the cause of delayed or lacking InfoSec training of new employees. This can be seen as a InfoSec culture problem in general, and this is correct. The InfoSec training was, a part of the InfoSec awareness, and this again is a part of the InfoSec culture. In most of the companies, the InfoSec training of new employees was a part of the InfoSec culture budget. Though looked at as a InfoSec culture problem, it is more of a InfoSec culture management problem. The responsibility of fixing this problem would fall to the CISO. The companies who had overcome this problem had used written contracts. The main contract was between the InfoSec department and the upper management specifying a broader jurisdiction to the InfoSec department on specific tasks. The InfoSec department was required to cooperate with the other parts of the companies, and they, in turn, had to help facilitate the InfoSec department when needed. This solution would give the InfoSec department a stronger argument when dealing with other parts of the company, and hence solve the direct problem.

From the standpoint of the InfoSec departments there where several sub-reasons as to why the new employees should have InfoSec training. The risk analysis and testing showed the security risk of the new employees posed before receiving any InfoSec training, again matching NorSIS [MR16, sfi17, MR18]. Having the InfoSec training early and together with the other training they received also helped the new employees use it correctly and involved them in the InfoSec culture from the start. This is supported by research, but was only referred to as logical thinking in the interviews [PS10, PMX14, NSSF16, MSP14, ME09]. This is not a large problem as most of their thinking and ideas match what research tells, and currently there are other problems more significant. There might be problems in the future following this path, but discussing it would only be speculation and guesses.

5.4 Utilisation Of Training New Employees

The utilization of new employees in InfoSec training has shown to be heavily dependent on what the company they work in is providing. In general, there are two groups those who train their new employees in InfoSec and those who do not. From the companies that responded to the invitation to this research project, four out of seven

companies did not train their new employees or employees in general in InfoSec. This is similar to the findings of NorSIS [MR16], who found that 53% in the private sector had received InfoSec training of any sort in the last two years. The sample size of this research project is too small to compare directly in a question of how many percent, but our findings are still that less than 50% of the companies train their new employees or regular employees alike in InfoSec.

The group of companies that do not train their InfoSec was typical non-IT companies. Of the companies participating in this research project, only company A falls in this group. From the paragraph above, its seen that is likely closer to 50%, rather than one in four. The companies in this group did train their new employees on topics related to their work and tasks, and training related to or required by laws. The motivation for this training was not from the InfoSec department or personnel. The InfoSec department and personnel did not seem as the bottleneck preventing the training of new employees in InfoSec. The results indicated that communication and cooperation with other departments, and restrictions of the InfoSec department by jurisdiction or resources is the main problems. Without any InfoSec training at all, the potential of the new employees is not utilized in this regard.

In the group of companies who do train their new employees in InfoSec, most of the new employees are trained from the start. Only a combined 6,8% of the new employees answered that they received InfoSec training later than four months after starting. Of those who received InfoSec training before the end of the fourth month, 87% answered that they received the training within the first two months. The reason for educating so early was explained by the companies with the benefits of early training versus only negative effects of delayed or later training. Looking at the training itself, it also matches these arguments of benefits from early InfoSec training.

From the results, the group who trained the new employees in InfoSec and the group who utilized the new employees from the start were the same. No middle ground example was found where InfoSec training would occur later, or the training did not match the arguments for efficient InfoSec training.

5.5 Limitations

The first part of the results that may contain uncertainties is the invitation to the research project. Three companies declined to join the research project because they had no InfoSec training of employees. Giving this reason for declining may indicate that other companies also have no InfoSec training of employees, and refrain from answering the invitation because of it. The companies who declined were, as described earlier, typical non-IT companies, so it is more likely that this is related

to those types of companies rather than companies in general. Further, the number of companies participating in this project is not large enough to represent the total amount of all companies. However, with the time limitations for this project, the number of companies that could be included became limited. The findings of this project are still relevant, and because it matches the findings of other projects, the likelihood of these findings being an edge case is much lower.

From the case study, all the material form company D was in relation to the classroom sessions. Thus it was surprising when the interview also mentioned online training. The questionnaire also suggests that company D uses an online questionnaire to a large extent, similar to that of company B and C. Less than 20% of the new employees in company D remembered that the classroom or lectures were used in the InfoSec training. The result of this is that all the companies in this research project used online courses for the majority of their InfoSec training. This again implies that Company D used the classroom sessions more to the effect of creating motivation, showing leader support and involvement, and improving the norms and intention to comply. Overall this matches with the findings of company B and C but leaves a large room for interpretation and uncertainty in regards to the effects the results from company D have on the total findings.

The questionnaire was supposed to be sent out to all new employees in all the companies A, B, C and D. Normal problems with questionnaires is that the questionnaire is sent out to many recipients, but only a few actually answers. The problems experienced in this research project was that of distribution. Because of the topic and content of the questionnaire invitation mail, lots of recipients were skeptic when testing the questionnaire. The invitation would be rather standard with a link to the actual questionnaire, and a PDF attachment with the required information and the approval from the Norwegian Center for Research-information. Hence the questionnaire was sent out from the companies themselves. First off all the companies had problems filtering out a list of only the new employees. Because of this, the total amount of questionnaire sent in company B represents the whole company, all employees included (5.1). The results represented the regular employees are filtered out, but this still affects the calculation of the confidence interval. The total amount of questionnaires sent from company C included new employees in other countries. As the questionnaire was written in Norwegian, the calculation of confidence interval, and possibly misunderstandings may affect the results. Company A initially stated that they had problem obtaining a list of new employees, but later stated that due to workload would not be able to send out the questionnaire.

The confidence interval on average for all the companies was calculated to be ± 22, with company B having ± 18, company C having ± 18 and company D having ± 30, with a 50% answer variation. The 50% answer variation does however not fit.

For the individual companies, the percentage answer variation was leaning in one direction, in table 5.1 the specific confidence interval was calculated. This calculation is however affected by the problems described above, and the answers from company D has so low total questionnaires sent that it affects the confidence interval. Because of this, an average confidence interval for the questionnaire was not calculated. More unified answers were observed, and this affects the answer variation to one side, indicating that the average confidence interval is lower than the previous calculated ±22.

Company	Sample size	Total sent	Percentage	Conf interval	Conf level
A	0	0	na	na	na
B	25	3022	71	17.72	95
C	21	140	61	19.3	95
D	6	13	65	29.15	95

Table 5.1: Calculated confidence interval for the individual companies in the questionnaire.

5.6 Further work

The findings of this research project are interesting and may be used as the basis for future research. The problems around communication and cooperation between different departments were the main thing preventing InfoSec training of new employees in the companies that did not do so. Hence more research into this problem would be needed. Concrete tasks would be a template for how to gather information and hence support for the InfoSec department's projects. This is overall, a large project and would not fit in a single Master's thesis. This would be more suited to a Philosophiae Doctor (PHD) project or split into several chaining Master's thesis under a single professor. Similarly, a project looking into the bureaucratic capabilities of the CISO or InfoSec department compared with the resources and freedom of the InfoSec department, would help to narrow down the problem and solutions used to solve it.

The second suggested future work is a template for the use of online courses in training InfoSec. Online courses are observed to be widely used. But the educational methods used in them are varying and dependent on the observations and ideas of the person making the course. A sett with guidelines or guiding templates, based on educational and InfoSec literature and works, would standardize the online courses and remove the variations that confuse or have little behavioral change on the users.

Chapter 6
Conclusion

InfoSec training is only one method of changing or affecting the InfoSec culture and the InfoSec awareness, still it is arguably one of the most essential tools. InfoSec training is widely acknowledged as a critical point for changing the behavior of users. Knowledge is the foundation and the building block from which decision making is made in order to achieve the desired result. Companies utilize this in training their new employees in making decisions to further the cause of the company. There are several other reasons why the InfoSec training of new employees is a critical point. In Norway, there is no organized InfoSec training prior to what an employer provides. Learning InfoSec early will help with minimizing the time the new employees is an untreated weakness, prevent having to relearn tasks, and introduce them to the InfoSec culture. Through this research project, the training process and reasons behind the training of new employees in InfoSec have been examined.

RQ1 The training of new employees in InfoSec was not done by all the companies. The answer to RQ1 "How are new employees trained in InfoSec, and are there any differences compared to other employees?" hence becomes two parts. The first part is that in roughly half of the companies had no InfoSec training of new or regular employees, and hence no difference. The second part is that in the other half of the companies, the InfoSec training of new employees is mainly done through online courses. The reason for this was found to be the minimizing of resource use outside of the InfoSec department, such as employees time usage and cooperation with other departments. The InfoSec department also had limited human resources of its own to do this task. Comparing this to the training of regular employees showed that the regular employees as not trained as directly, but rather continuously reminded and tested. All of this matched the findings of relevant literature when compared. Going further with the group of companies that did train their new employees in InfoSec, showed that the courses themselves were individually made by the companies. The content and reason for the InfoSec training is described in RQ2 and RQ3, respectively. The methods, tools, and combinations of these used in the online courses were put

together by the InfoSec personnel and are subject to their ideas and thoughts. This makes for variations in the effectiveness of the online courses from different companies.

RQ2 The topics of the InfoSec training of new employees varied somewhat based on the company. The main topics were attacks and solutions to common weaknesses, often with easy solutions. This included passwords, phishing-mail, mail in general, and threats to the workplace. Some companies deemed it to be necessary with more topics in their general InfoSec training and included, general do's and don'ts, social engineering through different media, VPN and off workplace security. Specialized training was also included by companies where it was relevant, but this was only provided to those who were in need of it. The process of choosing the topics was individual for each company, but in all the cases, it was done by comparing online sources for most likely attacks, risk analysis and registered attacks for the individual companies.

RQ3 Due to roughly half of the companies not training their new employees in InfoSec, the answer to RQ3 is in two parts. Companies who did not train their new employees in InfoSec did so mainly because of the restriction of resources. This was mostly a lack of jurisdiction to make use of other employees time and resources outside of the InfoSec department, but also problems with cooperating with other departments were mentioned. The InfoSec departments were aware of the benefits of early InfoSec training, but it was not a prioritized task. The group of companies who did train their new employees in InfoSec, did so in order to minimize the risks of attacks. The reason they trained the new employees from the start was the benefit of minimizing the risks an untrained new employee poses, and the new employees not having to relearn. From a practical standpoint, the InfoSec training being done simultaneously as other training new employees received was also a significant reason.

RQ4 Also, this answer is divided into two parts. Those who did not train new employees in InfoSec did not utilize the new employees in InfoSec training. The training of new employees was wanted by the InfoSec departments, support for this was missing in the companies in general. The companies who did train their new employees in InfoSec utilized the new employees in InfoSec training to a large extent. Content, planning, organization, follow-up, testing, and the training itself was all done to the extent of the InfoSec department's capability. The InfoSec training itself was found to be varying between the companies, and to be less effective than optimal. This is due to the online courses being made by the InfoSec departments without any educational support.

References

[AJ02] Martins A and Elofe J. Information security culture. *Security in the Information Society*, 86:203–214, 2002.

[BHSW88] Jon Hartwick Blair H. Sheppard and Paul R. Warshaw. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, 15(3):325–343, December 1988.

[CNJ14] DiCenso Alba Blythe Jennifer Carter Nancy, Bryant-Lukosius Denise and Neville Alan J. The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5):545–547, September 2014.

[dVM15] Adéle da Veiga and Nico Martins. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49:162–176, 2015.

[EJ16] Whitman Michael E. and Mattord Herbert J. *Managment of Information Security.* Course Technology, Boston, MA, US, 2016.

[END95] MICA R. ENDSLEY. Toward a theory of situation awareness in dynamic systems. *HUMAN FACTORS*, 37(1):32–64, March 1995.

[FP97] Schott F. and Driscoll M. P. *Instructional Design: International Perspective, Vol. 1, Theory, Research, and Models.* Lawrence Erlbaum Associates, Mahwah, NJ, US, 1997.

[Gau98] Nick Gaunt. Installing an appropriate information security policy. *International Journal of Medical Informatics*, 49(1):131–134, 1998.

[Gub87] Egon G. Guba. What have we learned about naturalistic evaluation? *The American journal of evaluation*, 8(1):23–43, 1987.

[Her09] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. *MSR-TR-2009-46*, 46, April 2009.

[Hob60] Mowrer O. Hobart. *Learning theory and behavior.* John Wiley & Sons Inc, Hoboken, NJ, US, 1960.

[JFTJC89] Ellen Day John F. Tunner Jr and Melvin R. Crask. Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research*, 19(4):267–276, December 1989.

[Kah96] David Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. CSRIBNER, New York, 1996.

[Kit04] Barbara Kitchenham. Procedures for performing systematic reviews. *Keele University Technical Report TR/SE-0401, Department of Computer Science Keele University*, July 2004.

[KS11] Mari Karjalainen and Mikko Siponen. Toward a new meta-theory for designing information systems (is) security training approaches. *Jurnal of the Association for Information Systems*, 12(8):518–555, August 2011.

[Lar18] Strand Kristine Larsen. Influencing factors and effectiveness of a security awareness campaign. *Institutt for informasjonssikkerhet og kommunikasjonsteknologi [1166]*, pages 1–89, 2018.

[M.82] Ryan Richard M. Control and information in the intrapersonal sphere: An extension of cognitive evaluation theory. *Journal of personality and social psychology*, 43(3):450–461, 1982.

[ME09] Şaban Eren Mete Eminağaoğlu, Erdem Uçar. The positive outcomes of information security awareness training in companies – a case study. *Information Security Technical Report*, 14(4):223–229, November 2009.

[MR16] Bjarte Malmedal and Hanne Eggen Røislien. The norwegian cyber security culture. *Norsk senter for informasjonssikring*, 2016.

[MR18] Bjarte Malmedal and Hanne Eggen Røislien. Nordmenn og digital sikkerhetskultur 2018. *Norsk senter for informasjonssikring*, 2018.

[MSP14] M.Adam Mahmood Mikko Siponen and Seppo Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224, March 2014.

[MWS08] William H.Bommer Michael Workman and Detmar Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6):2799–2816, September 2008.

[NSSF16] Rossouw Von Solms Nader Sohrabi Safa and Steven Furnell. Information security policy compliance model in organizations. *Computers & Security*, 56(1):70–82, February 2016.

[OC81] Charles A. O'Reilly and David F. Caldwell. The commitment and job tenure of new employees: Some evidence of postdecisional justification. *Administrative Science Quarterly*, 26(4):597–616, December 1981.

[oS] Harvard Department of Sociology. Strategies for qualitative interviews. https://sociology.fas.harvard.edu/files/sociology/files/interview_strategies.pdf. Accessed: 2019-02-04.

[PJ91] John P.Meyer and Natalie J.Allen. A three-component conceptualization of organizational commitment. *Human Resource Management Review*, 1(1):61–89, 1991.

[PMX14] Yi Ding Peter Meso and Shuting Xu. Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, 9(1):47–67, July 2014.

[PS10] Petri Puhakainen and Mikko Siponen. Improving employees' compliance through information systems security training: An action research study. *Computers & Education*, 34(4):757–778, December 2010.

[RH09] Albert L. Harris R.S.Shaw, Charlie C. Chen and Hui-Jou Huang. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1):92–100, January 2009.

[RM11] Colin Robson and Kieran McCartan. *Real World Research*. John Wiley & Sons Ltd, Southern Gate, Chichester, 2011.

[RMRK83] Valerie Mims Richard M Ryan and Richard Koestner. Relation of reward contingency and interpersonal context to intrinsic motivation: A review and test using cognitive evaluation theory. *Journal of personality and social psychology*, 45(4):736–750, October 1983.

[SFD02] M. Gennatou S.M. Furnell and P.S. Dowland. A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5):352–357, 2002.

[sfi17] Norsk senter for informasjonssikring. Nordmenn og digital sikkerhetskultur. *Norsk senter for informasjonssikring*, 2017.

[Spu95] Phil Spurling. Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2):20–26, 1995.

[TvS98] M.E. Thomson and R. von Solms. Information security awareness: educating your users effectively. *Information Management & Computer Security*, 6(4):167–173, 1998.

[VJ10] A.Da Veiga and J.H.P.Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010.

[W75] Rogers Ronald W. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1):93–115, September 1975.

[WH03] Mark Wilson and Joan Hash. Building an information technology security awareness and training program. *NIST Special Publication 800-50*, October 2003.

[WML11] Haworth Dwight Wolf Michael and Pietron Leah. Measuring an information security awareness program. *The Review of Business Information Systems; Littleton*, 15(3):9–21, 2011.

[Yin09] Robert K. Yin. *Case Study Research, Design and Methods*. SAGE Publications, Thousand Oaks, California, 2009.

Appendix A
Interview Guide

Intervjuer: Jonas Gedde-Dahl
Intervjue av bedrift:
Dato: 2019
Sted:

Interview Guide:

Practises for teaching information security to new employees

Master prosjekt ved NTNU

1. **KAN DET JEG SPØR OM BRUKES I DISKUSJON?**

2. Kan du beskrive opplæringen i informasjonsikkerhet slik den er nå?
    a) Hvordan gjennomføres opplæringen?
    b) Hva er innholdet i opplæringen?
    c) Hvorfor har dere opplæringen?
3. Bruker dere instruktører?
    a) Hvordan er kunnskapsnivået til instruktørene?
    b) Hvordan er instruktørene kvalifisert?
    c) Får dere hjelp av eksterne til å gjennomfør opplæringen?
4. Har dere en praktisk del i opplæringen?

   a) Hvordan vil du beskrive den praktiske delen?
   b) Hvordan samsvarer de praktiske oppgavene med de ansattes faktiske oppgaver?
   c) Hvorfor har dere den praktiske delen?

5. Har dere en individuell del i opplæringen?
   a) Hva går den individuelle delen ut på?
   b) Hvorfor har dere den individuelle delen?

6. Har dere en gruppe del i opplæringen?
   a) Hva går gruppe delen ut på?
   b) Hvorfor har dere en gruppe del?

7. Hvor gammelt er det nå værende opplegget?
   a) Hvordan ble oppleget laget?
   b) Er det basert på tidligere arbeid?
      —Lærings teori, andre kurs, annen opplæring, etc.
   c) Fikk dere hjelp fra noen eksterne når dere lagde oppleget?

8. Hvordan kvalitetssikrer dere opplæringen?
   a) Hvor ofte reviderer dere opplæringen?
   b) Hvor ofte reviderer dere innholde i opplæringen?
   c)

9. Hvor lang tid etter ansettelse gjennomfører der opplæring i informasjonsikkerhet?

10. Hvorfor lærer dere de ansatte opp i informasjonsikkerhet?

11. Hva skal de ansatte få ut av opplæringen?

12. Hvordan prøver opplæringen å påvirke de ansattes handlinger?
    —Den gir kunskap, men prøver den å skape motivasjon til å bruke den?

13. FOLLOWUP - case study

14. Er det noen endringer du kunne tenke deg å gjøre med opplæringen, prosessen eller innholdet?

Questionaire questions in Norwegian

Practises for teaching information security to new employees

Master prosjekt ved NTNU

1. Hva er navnet på din nåværende arbeidsgiver?
2. Hva er ditt kjønn?
    a) Mann
    b) Kvinne
    c) Annet
3. Din alder
    a) 0-14 år
    b) 15-24 år
    c) 25-34 år
    d) 35-44 år
    e) 45-54 år
    f) 55-64 år
    g) 65+ år
4. Hvor lenge har du jobbet for din nåværende arbeidsgiver?
    a) 0-2 månder
    b) 3-4 månder
    c) 5-6 månder
    d) 7-8 månder
    e) 9-10 månder
    f) 11-12 månder
    g) Mere enn 12 månder
    h) Vet ikke
5. Har du fått opplæring i informasjonsikkerhet tilpasset alle ansatte?
    a) Ja
    b) Nei

   c) Vet ikke

6. Har du fått opplæring i informasjonsikkerhet spesielt tilpasset nyansatte?

   a) Ja
   b) Nei
   c) Vet ikke

7. Hvor lang tid etter ansettelsen fikk du første gang opplæring i informasjonsikkerhet?

   a) 0-2 månder
   b) 3-4 månder
   c) 5-6 månder
   d) 7-8 månder
   e) 9-10 månder
   f) 11-12 månder
   g) Mere enn 12 månder
   h) Vet ikke

8. Hvordan ble informasjonsikkerhetsopplæringen gjennomført?

   a) Klasserom
   b) Diskusjon
   c) Selvlæring
   d) Online-kurs
   e) Foredrag
   f) Vet ikke
   g) Annet

9. Hvilke temaer husker du ble gjennomgått i opplæringen?

10. I hvilken grad opplevde du at informasjonsikkerhetsopplæringen var knyttet til arbeidsoppgavene dine?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad

f) Vet ikke

11. I hvilken grad opplevde du at du lærte noe nytt av informasjonsikkerhetsopplæringen?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

12. I hvor stor grad opplevde du at opplæringen var orientert rundt risikobildet til bedriften?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

13. I hvor stor grad opplevde du at opplæringen var advarende? Eksempelvis fokuserte på hva man ikke skulle gjøre eller negative konsekvenser.

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

14. I hvor stor grad opplevde du at opplæringen var instruerende? Eksempelvis fokuserte på hva man skulle gjøre eller hvordan unngå konsekvenser.

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad

f) Vet ikke

15. I hvor stor grad opplevde du at opplæringen var informativ? Eksempelvis fokuserte på sammenhengen mellom handlingene og konsekvensene.

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

16. I hvor stor grad synes du at du har forbedret dine ferdigheter etter opplæringen i informasjonssikkerhet?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

17. I hvilken grad bruker du det du har lært i informasjonssikkerhet utenfor arbeidslivet?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad
    f) Vet ikke

18. I hvilken grad ønsker du mer opplæring i informasjonsikkerhet?

    a) Svært stor grad
    b) Stor grad
    c) Verken stor eller liten grad
    d) Liten grad
    e) Svært liten grad

f) Vet ikke

19. Hvilke av følgende informasjonsikkerhets aktiviteter har blitt arrangert på din nåværende arbeidsplass utenom spesifikk opplæring?

a) Foredrag

b) Stand

c) Nyhetsbrev

d) Phishing-kampanje

e) Vet ikke

f) Annet

20. Er det noe du ønsker å legge til i forhold til opplæring av nyansatte i informasjonsteknologi?