Sub-cultures effect on information security culture in an organization.

ERLEND CHRISTIANSEN SKAAR

SUPERVISOR

Eli Hustad

University of Agder, [2023]
Faculty of Social Sciences
Department of Information Systems

PREFACE

This study marks the end of my education at the University of Agder, something that started with a bachelor’s degree in IT and information systems and ended with a master’s degree in information systems.

This study deals with the different subcultures effect on information security culture. The levels of culture in an organization can be an overwhelming subject, as there exist a lot of variables that could affect the culture. I am thankful for the opportunity I’ve had to get the chance to explore this topic in a real organization.

Thank you to the organization who helped me develop this thesis and made this study possible. I also want to thank the contact person from the organization, as this individual provided me with the resources I needed and helped develop the thesis.

I would also like to give a big thank you to my supervisor Eli Hustad for her support and guidance throughout this semester.

Finally, I want to thank my family and close friends for their support and motivation, as well as my fellow students who made this master’s degree tremendously fun.

Kristiansand, 29.05.2023

Erlend Skaar

Erlend Christiansen Skaar

ABSTRACT

This study investigates the influence of subcultures on information security culture within organizations. The research focuses on the cultural and policy dimensions of information systems security and aims to explore how subcultures within an organization affect information security culture. The study employes a qualitative case study approach, conducting interviews with employees from different departments of a Norwegian IT consultant company.

The findings reveal variations in information security ownership, knowledge and awareness, and work goals and challenges among departments. The study emphasizes the need for tailored information security measures that consider the unique characteristics of each department. Collaboration and knowledge sharing between departments are identified as crucial for improving information security understanding and alignment with work goals. Flexibility and adaptability in information security policies and routines are recommended to strike a balance between security and operational efficiency. The study contributes to the understanding of information security culture and provides practical insights for organizations to enhance their practices and policies. Further research is suggested to explore subcultures related to information security, examine alignment between work goals and information security across departments, and investigate the long-term impact of security measures on organizational outcomes. Despite limitations such as sample size and participant selection, this study provides empirical insights into the relationship between subcultures, information security culture, and organizational dynamics.

Table of contents

List of figures

List of tables

1 INTRODUCTION

This study focuses on investigating the cultural and policy dimensions of information systems security within organizations through a qualitative case study. The existing literature emphasizes the human factor as a significant vulnerability in information security, with the majority of security breaches originating from human actions. Numerous contributing factors can be identified in this context (Govender, Loock, & Kritzinger, 2018).To mitigate the associated risks and prevent employees from becoming liabilities, organizations have implemented information security policies, as well as training and education programs in information security (Ismail, 2022).

Information systems security encompasses a collection of activities aimed at safeguarding systems and the data they store. Kim & Solomon (2013) define information systems security as the protection of information and its critical attributes, including the systems, hardware, and processes involved in storing, using and transmitting such information. This protection is achieved through the implementation of policies, training, and awareness programs (Whitman & Mattord, 2013).

The significance of this topic becomes evident when considering the vital role information plays within organizations, thus becoming the motivation for this study. Information serves as the most valuable asset for organizations, but it also represents a significant weakness due to the potential harm that can result from targeted attacks (Lopes, 2015).

Previous research has highlighted the significance of subcultures within organizations in relation to information security culture. Da Veiga and Martins (2017) found that deviations from the dominant information security culture can give rise to information security subcultures, characterized by unique norms that may influence individuals' perception of security. An information security subculture can be defined as a group of employees collectively adhering to information security values, perceptions, and policy principles that deviate from those commonly shared by the majority of the organization's employees (Da Veiga & Martins, 2017).

1.1 Aim and Research Question

The aim of this thesis is to explore how subcultures within an organization affect information security culture, with the motivation being the recognition of the human factor as a vulnerability and the need to safeguard valuable information. The different levels of compliance can affect the security of the company. With this in mind, I want to investigate how cultures in different departments within an organization affect information security culture. My research question for this study is:

> *How do subcultures affect information security culture in an organization?*

This will be done through examining different artifacts of information security culture in different departments and its relevance to the impact of subcultures. The research question is researched by interviewing employees from the same organization. The organization interviewed is a Norwegian IT consultant company. The research seeks to contribute to the understanding of information security culture and provide insight for organizations to enhance their practices and policies.

1.2 Disposition

This study is divided into 6 chapters, and the first chapter is 1. Introduction, which this part belongs to. Chapter 2, Theory, presents the relevant theory used in this study. Chapter 2 is to provide the central concepts for this study, as it includes all the relevant literature and its main findings. It introduces the conceptual model used in this study.

Chapter 3, Method, describes the research approach for this study, and what research methods have been utilized. Research design includes sample selection, data collection and data analysis, which will also be explained in this chapter. The research context will be explained, but the case company and the interview participants will be held anonymous throughout the study.

Chapter 4, Findings, presents the findings from the study. The individual chapters are based on the different measurements from the conceptual model.

Chapter 5, Discussion, goes through the results from findings in relation to prior research. It discusses what implications the study has for research and practice, limitations of the study, and future research.

Chapter 6, Conclusion, summarizes the most important findings and results to a conclusion.

2 THEORY

In this chapter I will present previous research literature on information security topics relevant for the research question. Scopus was used as the main database for acquiring literature and articles, as it provided good results and an easy way to extract the sources. Google Scholar was used to gain more general knowledge, or to look up a specific topic. After completing the analysis of the literature study, the findings were categorized into the following topics: IS-policy compliance, organizational culture and IS-culture, and subculture.

2.1 IS-Policy Compliance

The goal of a security policy is to ensure confidentiality, integrity, and availability (CIA) (Subramanian V., 2012). This means that the policy should consider who is authorized for the information, the preservation of the information's original features, and that the information is always available for legitimate use (Lopes, 2015). ISPC (IS-policy compliance) can be for some organizations a challenge when it comes to security. Xu & Go (2019) and Siponen et al. (2014) shows to one of the biggest challenges in IS-security is employees' ability to follow the imposed security-tasks that are determined in the ISP of the organization. ISPC has been investigated from a variety of different levels, such as individual level, cultural level, and organizational level, resulting in a list of variables that may affect employee's behavior towards ISPC (Sohrabi Safa, 2016).

One of the variables affecting ISPC is leadership/management. Information security managers do not have any rights to order employees to comply with ISP but should actively help and lead employees towards proper behavior, by setting a good example through motivation, influence, and consideration (Choi, 2016). The proactive involvement of management in information security demonstrated through their commitment, provision of employee education, and support in developing skills and confidence, plays a pivotal role in influencing the organizational culture and fostering compliance with information security practices (Cram, 2020). Management's choices and attitude can also affect employees in a negative way. Punishment and blame towards employees for not complying to ISP can create a desire for the employees to punish their leaders by intentionally violate or ignore ISP, thus creating a "us vs them" culture in the organization (Cram, 2020; Wall, 2012). The relationship between management and employees is a part of creating the organizational culture, which relates to the attitude towards ISP.

There are a lot of examples when it comes to challenges with ISPC. Finding the ideal ISP for your organization can be challenging, as it needs to include a plethora of routines, requirements, and variable processes (Subramanian V., 2012). A major challenge is balancing the security requirements that conflicts with work goals, resulting in a lack of awareness that creates bad practices of finding ways to work around security compliance (Sadok, 2020). There is a correlation between perceived benefits in work goals, such as efficiency, safety, integrity, or work quality, that conflict with ISPC (Woltjer, 2017).

2.2 Organizational Culture and Information Security Culture

Culture is influenced by many variables. Shared values, with cultural strength describing which values are shared by organization employees is the core of organizational culture (Büschgens, Bausch, & Balkin, 2013). Organizational culture is important for organizations as it is a collection of the overall values and norms of the organization, but it also includes a very important subculture in information security culture (ISC). Conolly & Lang (2012) distinguish between organizational culture and ISC, where ISC is defined as "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any points in time" (Connolly & Lang, 2012). Ismail (2022) describes ISC as a set of visible and invisible manifestations shared by employees within an organization. Lopes & Oliveira (2015) states that the focus should be on creating a strong ISC, rather than the technological aspects, by using the RITE principles with a high degree of efficiency. The RITE principles are principles for creating an information security culture (Lopes, 2015):

- Responsibility: As organizations move away from traditional hierarchical organizational structure, the significance of responsibility become more prominent.
- Integrity: Being able to deal with sensitive information without the risk of leaking it or giving in to pressures.
- Trust: Being responsible for actions and high self-control without constant supervision.
- Ethicality: Ethics must be present in all situations to ensure an appropriate response.

While the RITE principles can lead to creating a healthy ISC, there are other factors which takes base in the individuals in the organization that influence ISC too. These factors are: security awareness, security ownership, and security compliance. These factors reflects different levels of culture, and can be used as measurements of security culture in an organization (Ismail, 2022).

2.2.1 Security Awareness

Information security awareness encompasses two key aspects. The first aspect emphasizes the level of understanding and awareness among users in organizations regarding the importance of information security issues and threats. The second aspect revolves around the adherence of users to the privacy and security policies set by the organization when utilizing the internet (R. Rohan, 2023). In organizations, the cultivation of an information security culture is facilitated through fundamental awareness and training initiatives (Govender, Loock, & Kritzinger, 2018). Knowledge and skills include information security awareness, specifically referring to the understanding of risks and threats, as well as awareness of available measures to mitigate and address these risks and threats (Lin & Luo, 2021).

2.2.2 Security Ownership

Understanding security roles and responsibilities is crucial for all staff members in an organization. This understanding enhances their security performance, which in turn contributes to the overall security performance of the organization. When employees comprehend their responsibilities, interacts with information systems, and recognize the significance of information security, they become aware of the security risks associated with their actions (Alnatheer, Chan, & Nelson, 2012). Security ownership refers to the engagement and interest of employees in prioritizing information security. As security ownership evolves, users develop a heightened sense of accountability for the overall security of their company’s information systems (Ismail, 2022).

2.2.3 Security Compliance

Security compliance has been introduced earlier in this chapter, but it is worth exploring the connection between security compliance and information security culture. Security awareness has a significant impact on employees’ intentions to adhere to security policies. The level of security awareness is linked to employees’ perception of potential consequences, which influences their level of compliance (Ismail, 2022). In an organization characterized by a healthy information security culture, security compliance becomes an expected attribute of that culture (Da Veiga & Martins, 2017).

2.3 Subculture

In a dominant IS culture, there are deviations which shows to IS subcultures with norms that could influence the perception of security (Da Veiga & Martins, 2017). Da Veiga & Martins (2017) shows that in an organization, a subculture emerges in a branch or department that is different from the dominant IS culture at their head office, generating different threats to the protection of the organization's information. This means that an organization could have different subcultures based on multiple variables, where each subculture varies from the dominant IS culture. Subcultures are usually formed around existing divisions, departments, functional or professional groups (Kolkowska, 2011). For this study, the definition of subculture used is: a group of employees in an organization that has a subculture differing from the dominant culture (Da Veiga & Martins, 2017).

Value conflicts exists between different security cultures within the same organization (Kolkowska, 2011). In this study, the value conflict looked at will be the work goals of the employees in the different departments. Organizational subcultures dedicated to information security is essential for effectively managing the human factors associated with information security breaches (Govender, Loock, & Kritzinger, 2018). In a study conducted by Kolkowska (2011), empirical evidence demonstrates that different security subcultures exists in the same organization. Subcultures can be identified across various job levels, functions, and roles within an organization, leading to variations in attitudes, beliefs, and values among the employees (Govender, Loock, & Kritzinger, 2018). An IS subculture refers to a distinct group of employees who collectively hold on the same IS values, perceptions and policy principles that may differ from those commonly shared by the majority of the organization's employees (Da Veiga & Martins, 2017).

2.4 Conceptual model

For this study, a conceptual model has been used as a framework for developing the interviewguide. The conceptual model is adapted from Ismail (2022, p.325). This model conceptualizes the IS-security culture and its three artifacts, which are security ownership, security compliance, and security awaresness (Ismail, 2022). The model is based on Theory of Planned Behavior, which is a framework used in psychology to explain human behavior (Ismail, 2022). In the study by Ismail, the framework is explaining how employees' attitudes, subjective norms, and perceived behavioral control make influences on their security behavior as, regards information security. The model proposes that security awareness and organizational culture make influence on employees' behavior (Ismail, 2022). This model will provide a framework to inform this research study by reavling how employees knowledge, compliance, and security ownership relate to security culture in the different departments of the organization.

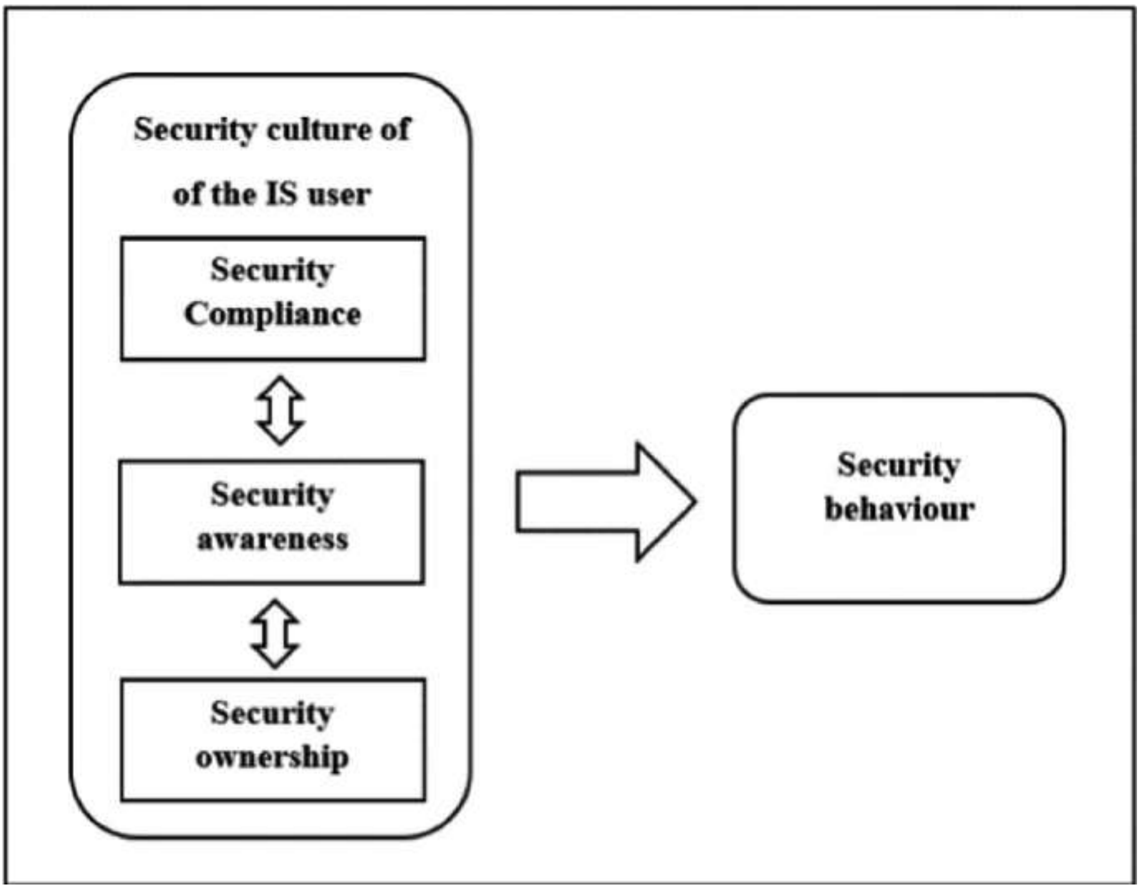


Figure 1 Conceptual model of IS security culture, its artifacts, and its behavior adapted from Ismail (2022, p.325).

3 METHOD

This chapter’s purpose is to introduce the research context, research approach, design, and data collection. The chapter aims to give the reader an understanding of how the research approach has been used to answer the research question.

3.1 Research Context

The case company for this research is an IT-consulting company based in Norway. The company specializes in delivering case- and archive systems to the public sector while offering consulting services in various IT domains including Robotic Process Automation (RPA), project management, technical solutions, and privacy services. As a subsidiary of a larger holding company, it operates multiple offices across Norway and has an employee count of approximately 270 individuals. It originated from a previous IT company before establishing itself as an independent entity. This study will primarily focus on employees situated within different departments of the organization, namely the sales, development, and delivery departments.

3.2 Research Approach

The goal of this case study is to see how different departments in the same organization develop sub-cultures that affect the ISPC. A case study is a research method that involves a detailed examination of e specific phenomenon or subject of analysis. The purpose of a case study is to thoroughly investigate a subject of analysis in order to reveal a new understanding about the research problem and contribute new knowledge to what is already known from previous studies (McCombes, 2023). Interviews are a qualitative research method that aims to collect data about what the interview object thinks. Interviews may also try to find out things that cannot be observed directly (Hannabus, 1996). Choosing interviews as a qualitative approach will help answer the research question, as data from interviews in this case will be focused on experiences, the interviewees’ perspective, and view of procedures (Hannabus, 1996).

The philosophical approach in this study is based on interpretivism. The interpretivist approach fits this study the best, as it has a focus on knowledge based on human experiences, which fits the study since it will be based on data collected on the employees’ perspectives and experiences (Pranas Žukauskas, 2018).

3.3 Research Design

Research design is used to provide a framework for data collection and analysis of data. The research design reflects the prioritization of different factors in your research (Bryman, 2012, p. 44).

The research design employed in this study is a cross-sectional design, commonly utilized for surveys, interviews, observations, and content analysis (Bryman, 2012, p. 59). The design involves the collection of data from cases at a specific point in time, enabling the examination of quantitative or qualitative data to identify patterns and trends (Bryman, 2012, p. 59). This fits well considering the study focuses on different departments within the same organization. It is expected to find variations in the variables of the study, which is common for cross-sectional design (Bryman, 2012, p. 59). In this research design chapter, I will present how the sample was selected, the data collection, and how the data were analyzed.

3.3.1 Sample Selection

The selection of interview participants was conducted by the designated contact person within the organization. The objective was to include employees from various departments, preferably from the same physical office location. This selection process and its implications will be further addressed in the forthcoming chapter on limitations. The criterion for the sample size was to have four employees representing each respective department.

The interview participants consisted of three distinct departments within the organization. The sales department primarily focused on customer relations, providing advice and generating revenue by offering high quality products. The development's main emphasis is on efficient and quality driven product development, ensuring understandable software structures, and addressing potential issues through practices such as pen-testing (penetration testing) and code review. The delivery department comprises diverse teams, including professional consultants, technical consultants, project managers, and an integration team. The delivery department's responsibilities include internal management, customer relations, and providing product related consultancy services.

The interview participants were contacted via email. The contact person from the organization provided me with their email addresses and also informed the participants in advance about the interview's topic. Additionally, an information letter was shared, outlining details about the interview process, the implications of participation, and privacy measures in compliance with NDS guidelines.

Table 1 Interviewee’s Role and Interview ID

Sales	ID	Delivery	ID	Development	ID
Key Account Manager	Sales1 (S1)	Team Leader for Project Leaders	Delivery 1 (DEL 1)	Chief Developer	Development 1 (DEV 1)
Bid Manager	S2	Product Area Manager	DEL 2	Advisor for Development Teams	DEV 2
Customer Manager	S3	Team Leader for Technicians	DEL 3	Developer	DEV 3
Customer Manager	S4	Team Leader for Integration Team	DEL 4	Junior Developer	DEV 4

The employees in the study exhibited variations in their lengths of employement within the company, ranging from indivudals who ha been with the organization since its inception as part of another company, to those who had only one year of experience. Due to the diverse gepgraphical locations of the employees, all interviews were conducted using Microsoft Teams, which facilitated convenient scheduling. To ensure the comfort and free expression of the interviewees, the interview were conducted in Norwegian, their native language. Subsequently, the interviews were transcribed and translated into English to the best of my abiliy, ensuring the preservation of contec and capturing the key points of the responses.

3.3.2 Data Collection

The data collection was done through a qualititative method, interviews. The interviews was based on the conceptual model of IS security culture and behavior from Ismail (2022) article about designing information security culture artifacts. The questions were centered around topics that related to the research question, and covered different areas within information security. By designing the interview questions with the conceptual model in mind, the questions will be centered around security-related behavior (Ismail, 2022).

Table 2 Interview design based on conceptual model

Topic	Goal of the questions
Introduction	To get an understanding of what the interview object works with, work goals, and area of expertise.
Information Security Ownership	How interrested the interview objects are in information security. Their understanding of information security, and prior education/training/certification in information security. How important they feel IS is.
Information Security Knowledge and Awareness	Knowledge about different types of risks and threats related to IS. How familiar they are with the company's security measures.
Challenges (Policy Compliance)	Challenges and their own experiences with IS-policies. How IS.policies affect their work. Areas where the employee could see potential improvments.

The primary focus of the data collection in this study relate to to the employees' experiences and perspectives regarding information security. To gather this information, semi-structured interviews were contuced, providing an oppertunity for a more flexible and conversational approach. An interview guide was utilized as a supportive tool to ensure that the interviews stayed on track and to redirect the conversation if necessary. The conceptual model served as the foundation for the interviews, aiding in the analysis of the interview data. This conceptual model includes various dimensions of information security culture, including information security ownership, knowledge and awareness, and challenges, which together contribute to an exploration of the information security culture within the departments (Ismail, 2022).

3.3.3 Data Analysis

The data analysis was centered around analyzing the content of the interviews. By looking at how often a specific theme is addressed, and the frequency of keywords that are mentioned, it allows me to categorize the different answers into fixed categories (Kvale, 2011). Concepts from literature (conceptual model, Ismail, 2022), making the data analysis a deductive approach (Zhang & Wildemuth, 2005). For the data analysis process, I have followed the steps from the process of qualitive content analysis in Zhang & Wildemuth (2005):

Step 1: Prepare the data:

The process starts with preparing the data. In this case, preparing the data means transcribing the interviews. All questions and answers relevant to the research question have been included in the transcription. Unnecessary sounds like stuttering and longer pauses that don't contribute to the data have been left out of the transcription. The principle I followed for the transcription of the interviews was that if it did not provide any value, I could not justify the additional time required to implement it.

Step 2: Define the unit of analysis:

This is the process of finding themes to be used as units for analysis. In the data collection chapter, Table 2 shows the measurements that will be used for the analysis. Those topics are the different themes used as coding units. The themes are; security ownership, security awareness, and potential challenges.

Step 3: Develop categories and a coding scheme:

The categories and coding scheme can be taken from three sources: the data, previous related studies, and theories. Coding schemes can be developed both inductively and deductively. As mentioned earlier, the conceptual model from Ismail (2022) has been used as the base for the categories in the interviews and data analysis. The coding schemes follow a deductive approach.

Step 4: Test your coding scheme on a sample of text:

This is the part of the process where you test the clarity and consistency of the coding scheme to avoid low consistency, doubts and problems concerning the definitions of categories.

Step 5: Code all the text:

During this process, the coding must be checked repeatedly to prevent losing the meaning of the code. Coding will proceed while new data continue to be collected, it is possible that new themes and concepts will emerge.

Step 6: Assess your coding consistency:

Human coders are subject to fatigue and are likely to make more mistakes as the coding proceeds. New codes may have been added since the original consistency.

Step 7: Draw conclusion from the coded data:

This part of the process is about exploring the properties and dimension of categories, identifying relationships between categories, and uncovering patterns. This is where I will look at the relationship between the categories from the conceptual model and potential challenges that affect the ISPC in the different departments.

Step 8: Report your methods and findings:

Step 8 revolves around presenting the findings, which will be in the chapter Results. This is where the results of the data analysis will be presented. As this is a qualitative study, the interpretation of the data will represent both personal and theoretical understanding of the data.

The tool used for data analysis is NVivo. NVivo is a software tool used for analyzing data from interviews, surveys, field notes, web pages and journal articles. It allows coding of interviews, which creates an easy way to analyze and visualize data (NVivo, 2023). As the university provided license key for this software, it became the choice of software tool, as it is something I have used in past studies, some familiarity with, and easy access to.

3.4 Quality Criteria

There exist a lot of different frameworks and checklists one can follow for quality criteria (Bryman, 2012). This study follows the four criteria of trustworthiness set by Guba and Lincoln (1985) in Bryman's book Social Research Methods (2012). These four criteria are (Bryman, 2012, p. 390):

Credibility:

This stress on multiple accounts of social reality is important because it affects how trustworthy information is. When there are different possible explanations for something in society, it is the credibility and believability of the explanation that determines if other will accept it. To establish the credibility of findings, researchers need to follow good research practices and get confirmation from the people they studied to ensure they understood the social world correctly (Bryman, 2012, p. 390). This has been done by sending the results to the informants, as well as having the contact person from the organization to look over the study and make sure there are no statements that would possibly hurt the organization, and no internal information has been leaked.

Transferability:

Qualitive studies often focus on individuals or groups of individuals to obtain knowledge about their experiences or perspective. To ensure that the results are, or are not, transferable to different settings, the importance of including the research setting and variables of the study becomes significant, as it makes it possible for future research to determine if the results are valid in another context (Bryman, 2012). This study has researched different departments within the same organization. The organization and interview participants have been held anonymous throughout the thesis, while the research setting has been explained by providing relevant information without compromising the anonymity of the organization.

Dependability:

In order to assess the credibility of research based on the criterion of trustworthiness, researchers should adopt an auditing approach. This involves maintaining comprehensive records of all stages of the research process (Bryman, 2012, p. 392). In other words, making it possible for the reader to follow the research process and the choices made. This has been done throughout the study, going through the process of literature selection and the research process.

Confirmability:

Confirmability focuses on ensuring that, even though acknowledging the impossibility of attaining absolute objectivity in social research, the researcher can demonstrate their genuine commitment to unbiased investigation (Bryman, 2012, p. 392). This has been done through using quotes given by the interview objects in the results, and accounting for the limitations affecting the study.

4 FINDINGS

In this chapter, the findings from the qualitative study will be presented and my analysis of the interviews. It will explore the different categories set in the Method-chapter by studying the different departments IS ownership, IS knowledge and awareness, and their potential challenges. As this study focuses on different departments, each department will have their own subsection for each section in this chapter.

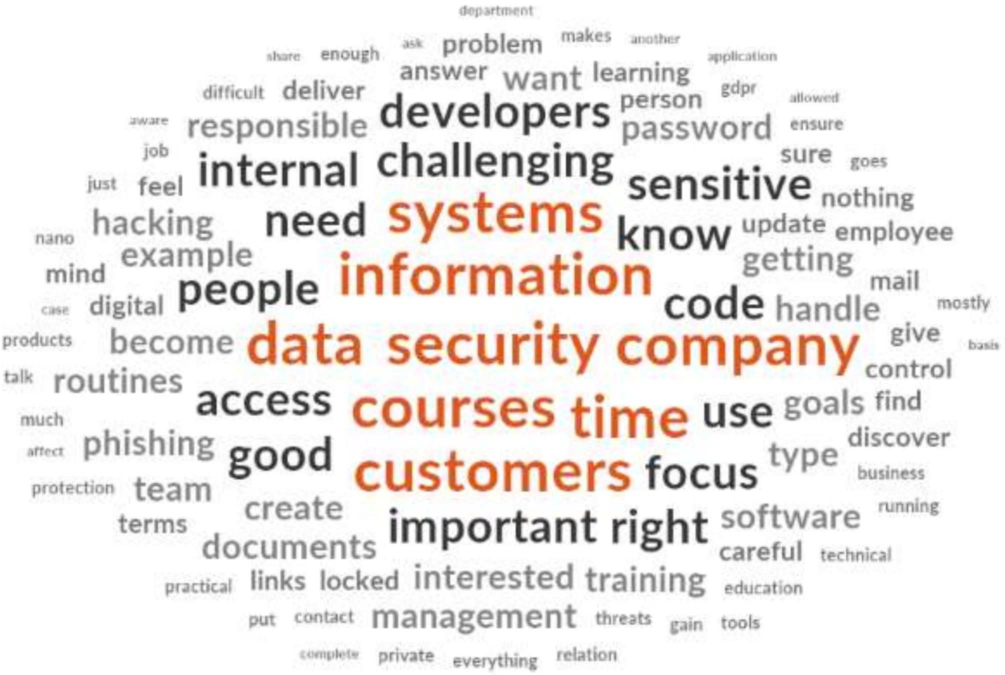


Figure 2 Wordcloud from interviews

The presented wordcloud is derived from the anaylsis of the interview data, specifically the codings assigned to different segments. It captures the 100 most frequently mentioned words accross all 12 interviews, exlucding commonly used words to emphasize the meaningful content and contextual relevance of the interviews. The purpose of creating the wordcloud is to visually represent the dominant themes and provide an overview of the topics discussed during the interviews. The words siplayed in organge represent the most frequently mentioend themes, indicating the employees' emphasis on customer-related matters and safety. Aditionally, the recurring mention of

”time” aligns with the following exploration of information security policies, which will be examined in further detial.

4.1 Information Security Ownership

Information security ownership looks at how interested the interview objects are in information security, their understanding of information security, and prior knowledge and education/training/certification in information security.

4.1.1 Delivery Department

The level of interest displayed by the delivery department regarding information security exhibits a range of perspectives. The interview findings indicate a shared comprehension of the significance of information security, although the degree of interest in the subject matter varies, ranging from person interest to a purely professional inclination driven by job requirements. Nonetheless, a significant majority of employees within the department demonstrate a combination of personal and professional interest in the domain of information security.

> ***“I would say I’m above average interested in [IS], and I hope the rest of the company also are that interested when thinking about what kind of business we work in, and the systems we deliver.”*** (DEL4)
>
> ***“Neither or, it’s not something I’m very interested in, but it’s also very important and can’t be ignored”*** (DEL 3)

This spread of interest might be because that the delivery department is the most versatile when it comes to different backgrounds and educations. The employees that participated in the interviews are in managerial roles in different professional fields. Half of the interview objects have an education in social studies but show high reflection around the importance of the topic through their view on what information security entails.

> ***“I think it’s a strategy and a set of measures to ensure, at all times, that information is securely stored in line with security and company policies.”*** (DEL2)

All the interview objects do have some type of education through courses, certification, or training related to information security through previous jobs or from the current job they have. Another thing they have in common is their focus on information not going astray, as this is important for the company and for their customers. It shows healthy IS ownership, as most of them reflect over the responsibilities they have regarding customer data.

> ***"The software we deliver must handle and take care of sensitive information about people, the company, etc. To have the right tools to make sure information doesn't go astray is the first thing that comes to mind."*** (DEL1)

4.1.2 Sales Department

The sales department exhibits a relatively low level of interst in information security, which can be attributed to their limited involvement in the technical aspects of the business and their primary focus on customer interaction. When asked about their intial thoughts upon hearing the term ”information security”, the respons from the sales department reveal a comparatively lower level of engagement and enthusiasm towards the subject matter, in contrast to the more pronounced interest demonstrated by the other departments.

> ***”I think of passwords, and passwords in a way to avoid someone getting acess, securing our data."*** (S1)

> ***”I think; be a little aware."*** (S4)

These short answers may be an indicator for a medium to low understanding of information security, as there is a lack of detailed explanations. The interviews still show signs of reflection towards the importance of information security, as they see the proffesional importance of it. One of the employees (S2) stands out, showing high IS ownership towards their own actions, compared to the other employees, which may come from the training this employee revieced in security and GDPR.

> ***”It is a part of job, that we do it in a proper way, and of course the daily, that we don't mingle with, again it comes down to what it means [IS], but if security is the big word, it is that I am carefuil with what I am doing daily in terms of links, I never click on any links, phising or virus.."*** (S2)

The employees knowledge about information security stems from internal cources, nano learning courses in the company and previos jobs, but there are no former education or external courses. This is to be expected since the sales department mostly handle the the economical aspect of the business.

> ***”I have IBM courses, nano learning, our own courses with certifiations, been through multiple security courses through the jobs I have had."*** (S1)

4.1.3 Development Department

The development department is the department that shows the most interest in information security. A reoccurring theme from the interviews is that not all the employees in a department have a personal interest towards the subject, and instead have a professional interest because of the importance of security, as it ties into both customers and the organization. In the development department we can find the same theme, where every employee is professionally interested in the subject matter, and some are personally interested. Those who are personally interested describe themselves as excessively interested in security, something that shows through their answers. All of the employees show a high understanding of the importance of security.

> ***"You very quickly become interested in it since you don't want to be the one who leaks something or is the problem. You don't want something you worked on to be published in the newspaper, because of something you have done, a lot of private information has been leaked."*** (DEV4)

> ***"Honestly, on a scale from one to ten, where one is very little and ten is very interesting, the technical part I would say is a 5, but the production part [case management] is a 10."*** (DEV1)

Their knowledge about information security stems from different internal courses and work experience, as none of the employees have any prior education in information security. The different courses range from NSM-courses (Nasjonal Sikkerthetsmyndighet/ National Security Authority) to GDPR courses. They also had smaller internal courses which revolve around small parts of information security.

> ***"I've had one course autumn last year by NSM…We have some ongoing smaller courses, where we go through small parts of information security, but I never remember the name of those courses."*** (DEV1)

All of the employees show a high security ownership. The development department is the most technical one out of the three departments in this study, which shows through their reflection around the responsibility of their work. Their focus is shared between two main areas, the security of the products they deliver, and on their own security. There is a big focus on the security of the products they deliver, as they develop the code for the products and that it can affect the customers as they interact with these products.

> ***"It kind of boils down to how you get the developers to make the system comprehensible. You want to make it simple. Make it difficult to make mistakes. Don't think about it normally, but deal with it."*** (DEV2)

> ***"That we need to be the first instance of security, be careful of what we click on. We spend a lot of time on trying to discover faults in code."*** (DEV4)

Another facet of their information security ownership is evident in their emphasis on penetration testing (pen-testing). The organization places great importance on pen-testing as it provides insights into areas of potential enhancement for employees. They must ensure that their code does not inadvertently expose clues to hackers regarding the software's structure and vulnerabilities. This practice fosters a heightened sense of reflection among employees regarding the security measures they have implemented, as they rigorously test various scenarios to ascertain the product's robustness and resilience.

> ***"That we do not create code that causes case managers to send information to the wrong person. We had a case on this recently where data was sent to the wrong person, and that was because the scenarios we had thought about were not thoroughly thought about"*** (DEV1)
>
> ***"Challenges with pen test, which showed results where we need to make improvements"*** (DEV2)

4.2 Information Security Knowledge and Awareness

Information security knowledge and awareness looks at the employees' awareness of different types of risks and threats related to information security, and how familiar they are with the company's security measures.

4.2.1 Delivery Department

The delivery department demonstrates a notable level of awareness concerning diverse threats and risks associated with information security. Predominantly, the identified threat frequently mentioned by the department is hacking, given its broad inclusion of various infiltration techniques beyond mere brute force entry. Social engineering hacking techniques, such as phishing and email scams, are also prominently highlighted during the interview discussions.

> ***"Hacking generally, malicious software that gets downloaded. Finding back doors or security holes in digital solutions. Data leakage. Phishing is another threat, or getting asked to give up username and password…"*** (DEL2)
>
> ***"Well, it could be hacking, hacking of passwords, key logging, machine locking."*** (DEL3)

When asked about their familiarity with the organization's security measures in case something goes wrong, the employees show a high understanding of both internal security protocols and security measures taken regarding customer data and safety. For the company's security measures, all the employees seem to be very comfortable with the subject matter, as they feel like they are on a level where they know how to react and who to notify if something were to happen.

> ***"I am very aware of what I would do in various situations given what it is. I have a little idea if I discover something that I'm not sure what to do, then I know who to contact, someone who has a security role in the office."*** (DEL1)
>
> ***"On a level where I can act and notify the right instances"*** (DEL4)

One employee was more centered around customer safety measures than the others. Instead of explaining their own security measures, the employee leaned more towards explaining security measures they have in case something happens to a customer, which gave insight into the customer perspective, and how the customer security also affects the organization's security measures.

> ***"We do describe in our tender response, we deliver primary through cloud, and there is a disaster recovery, several backups running that runs on a daily basis, that is maybe what you're looking for. We also have strict regulations for our consultants' access to our customer data."*** (DEL2)

4.2.2 Sales Department

The sales department demonstrates a notable level of awareness regarding internal threats to information security. Through interviews, the prominent internal threat identified by the employees is the presence of unfaithful servants, where individuals exploit company data or information for personal gain. This may involve activities such as selling data to competitors or illicitly leaking customer information through unauthorized channels. When asked about various threats and risks in information security, the employees display a commendable knowledge and reflective consideration of the diverse threats that the company may encounter.

> ***"It's phishing, when you click on something or are tricked into one or the other, then it's a type of virus that spreads further and paralyzes the systems internally, also with sharing of data of course…"*** (S2)
>
> ***"It could be hackers, unfaithful servers, it is mostly those two that often come up. Either hackers attack from outside or malicious attack from outside, or unfaithful servers internally."*** (S3)

As for the security measures within the organization, the results are spread among the employees. The results range from no familiarity with the security measures to knowing who to contact. The sales department employees are aware of the existence of the security measures, but not in great detail. This could be because of the department's low technical nature, as their ability to act on information security cases may be low, thus making it more beneficial for them to contact those who are able to act upon it. Still, the department shows knowledge and awareness of threats and risks in information security, which could be a result of the nano learning courses the organization has implemented. One employee shows some familiarity with measures taken for customer safety.

> ***"If things go wrong, we have recovery solutions that will get customers up and running quickly. As for our own systems, I assume we have the same thing there."*** (S4)

4.2.3 Development Department

The development department shows a commendable level of awareness regarding various risks, including hacking and phishing. The employees, predominantly due to the technical nature of their roles, provide detailed explanations encompassing the diverse manifestations and variations of these threats. This deeper understanding of the potential impacts of threats on the company can be attributed to the department's more specialized expertise. The most frequently cited threats and risks mentioned by the employees include hacking, phishing, and data leakage.

> ***"It's hacking where one gains access to the systems, authorization, stealing sensitive data. It's probably those thing one fears the most. The fact you can enter a system and pretend to be someone else and execute command as administrator."*** (DEV1)

The interviews provide a comprehensive insight into the security measures implemented within the organization. The employees exhibit a notable level of awareness as they provide detailed explanations regarding the measures in place to uphold security. Notably, one employee highlights the organization's ISO certification as evidence of comprehensive coverage of crucial security aspects. Among the four employees participating in the interviews, only one individual show limited familiarity with the organization's security measures.

> ***"I think that having a brisk relationship with the fact that these are things that happen all the time might be a good idea. All these systems build up and pull each other forward. As we are ISO certified, I think we cover a lot of important stuff."*** (DEV2)

An unexpected finding from the interviews is the emergence of a disagreeing viewpoint among an employee regarding a specific security measure. The organization has implemented physical security measures, including the requirement for access cards to gain entry into the office premises, along with security policies mandating the locking of PCs when leaving the office. However, from the employee's perspective, these measures are perceived as unnecessary obligations, given the constant presence of colleagues and the assurance of locked doors. Consequently, employees may occasionally deviate from complying with this policy, deeming it redundant. This noteworthy finding will be presented in the next chapter addressing potential challenges, as it adds valuable insight to the overall discussion.

> ***"We will also lock PCs when we leave them in the office, which does not always get handled because we have locked doors and colleagues are always around, which makes it a silly obligation if you ask me"*** (DEV1)

As the development department consists of mostly programmers, coding assumes a primary role within their activities. The process of coding for the product includes various facets, including functionality, design, and security considerations. During the interviews, an employee highlighted the significance of maintaining awareness of coding security and emphasized the importance of staying updated with newly discovered tools. This heightened awareness may stem from the organization's updates and internal training courses, fostering a culture of attentiveness to current trends and threats in information security.

> ***"Because people discover new things all the time, and new tools get discovered all the time, so what are the mistakes people make the most when it comes to coding security. Get an update on best practice when it comes to coding security."*** (DEV4)

4.3 Challenges

Challenges look at how the employees perceive how the IS-policies affect their work by delving into their work goals and potential challenges. This could be challenges and their own experiences with IS-policies, or areas of improvement in the organization regarding information security.

4.3.1 Delivery Department

Common themes discovered in the interviews regarding the department's work goals are the employees' desire to deliver on goals and objectives set by the company. Those goals often revolve around creating value for the company and stakeholders, and ensuring customer satisfaction by implementing projects successfully. Although the employees are team leaders in different fields, their work goals are centered around contributing to the company's overall strategy and direction.

> ***"They are pretty defined; it is the value of our products. How much income does our work generate to the company, compared to the expenses. Beyond having responsibility over budget, it is also about strategy, objective and key results ."*** (DEL2)

> ***"I'd like to think I have three things I want to focus on, to create value for myself, for my colleagues, and for the company, I try to contribute to that"*** (DEL3)

As the departments within the organization possess distinct areas of specialization, they encounter diverse sets of challenges. These challenges, although not hindering their work goals directly, occasionally result in delays that hinder the pace of work and create bottlenecks. Given that the employees' work goals revolve around maximizing efficiency and generating value for the company, any routine or processes that hinder the smooth progression of these goals can present considerable challenges for the employees. The predominant challenge highlighted in the interviews revolves around customer follow-ups. The employees elaborate on the complexities associated with accessing customer data, as it is not always straightforward due to certain restrictions. Additionally, another challenge encountered in relation to customers is the secure sharing of passwords. The difficulty lies in finding a reliable method to exchange passwords for customer accounts, considering that conventional channels such as email may not always offer adequate security measures.

> ***"so it can be challenging in terms of what you are allowed to do, if you are allowed to log in their account, if you are allowed to look at their data, it can be challenging because its not that black and white…"*** (DEL1)

> ***"Daily challenges tied to passwords, and password sharing to customers are maybe the challenges we face the most."*** (DEL3)

Another employee brings attention to the challenges associated with organizational processes and requirements. These requirements often rely on the efforts of a single individual who may not always have the capacity to fulfill them, resulting in a "stop and wait" scenario or bottleneck. Despite these challenges causing delays in work goal progress, employees do not perceive any specific hindrance to their overall work goals. They acknowledge the presence of these routines and policies as essential for ensuring security, although they express a desire for certain processes to be changed while maintaining awareness that prioritizing efficiency might compromise security measures.

> ***"In a way that some requirements, you must do to move on, can only be executed by one employee in the company who does not have the capacity to do, so it becomes very stop-and-wait before we can move on. Basically, bottlenecks and waiting periods."*** (DEL4)

> ***"It may in some cases be that if things could be done in a more flexible way, it could go faster, but then it not necessarily be safe, and then we are back to customer follow-up."*** (DEL1)

4.3.2 Sales Department

The sales department employees all share work goals, as the overlapping themes found in the interviews lean towards generating income and achieving sales targets. To achieve these goals, the employees must interact with customers and partners, thus creating a good relationship between the customers and the company. This is also done by providing quality products or offers with timely delivery to ensure customer satisfaction and encouraging repeat purchases.

> ***"My work goals are to ensure that we have enough missions for the company through sales of products we offer. It revolves around being in contact with customers and partners to ensure business. Work that creates income."*** (S1)

In terms of potential challenges, the sales department encounters relatively few obstacles in achieving their work goals due to the information security policies and routines in place. However, one prominent challenge identified during the interviews relates to the categorization of documents. This challenge arises from the need to classify documents as either private or public, with varying levels of security classifications such as secret or top secret, for instance. The presence of multiple labeling options often leads to confusion and ambiguity regarding the appropriate categorization of documents.

> ***"I would say it is a little challenging with the categorization of documents with regards to public and private documents to be stored. Some codes are a bit difficult to use, should I use this code or that code, or use the wrong code if something is meant to be limited, using the wrong code feels horrible."*** (S3)

Except for the challenge with document categorization, employees in the sales department do not find any challenges with routines and policies in the organization. In the interviews, the employees express no complaint about reaching their work goals regarding the routines and policies. As mentioned earlier, the sales department is not technological in its nature, which could explain the department's lack of challenges when it comes to information security.

> ***"No, they don't (routines). It is a completely normal and suitable level for what we work with, and my customer group, private and public."*** (S1)

4.3.3 Development Department

The work goals for the employees in the development department are generally themed towards focusing on development, efficiency, and quality. To meet customer expectations and satisfaction, the employees adjust their goals based on changing circumstances and solving problems. Another common goal for the employees is to continuously improve and master their work tasks, as creating understandable and secure software is a big part of their work.

> ***"The most important thing I think about is development, efficiency, and quality. When you have worked with a product for so long, you get a gut feeling about what do and not to do."*** (DEV2)

The most prominent challenge found in the development department is the challenge mentioned in the previous chapter. One employee expresses frustration with the practice of locking screens when leaving the PC or the office. The interview reveals the employee's contemplation on the adverse effect that a policy can have when it is perceived as unnecessary or burdensome. This situation raises concerns about the potential disregard for such security measures and underscores the significance of balancing security protocols with employee motivation while prioritizing customer security. The employee further expresses that security practice interferes with achieving the work goal and highlights the importance of motivation for developers as it drives developers to automatically think about security.

> ***"One can become negative and ignore these guidelines or commands, if it comes another regulation and you are already irritated over the existing regulation that you find unnecessary, one might start to ignore those orders. I think it's a bit unnecessary."*** (DEV1)

Apart from the aforementioned challenge, the employees within the department exhibit overall satisfaction with the security measures implemented by the organization. The employees express a positive sentiment regarding the organization's recent emphasis on security. Notably, one employee emphasizes the involvement of internship students in conducting tests, which has not only resulted in the identification of vulnerabilities but has also prompted a greater emphasis on hiring individuals responsible for such testing activities.

> ***"we've had some students on the office that are able to find some things though some test, so some of the reports we've ordered doesn't include everything, but I know there has been more focus to hire people with that type of responsibility, so can't complain about it when I see something gets handled."*** (DEV4)

5 DISCUSSION

This chapter discusses the results from the interviews in relation to prior research. The results will be categorized by the same topics used in the previous chapter, the three different measurements from Ismail (2022), which are information security ownership, information security knowledge and awareness, and potential challenges. It will also discuss implications for practice and research, limitations of the study, and future research.

5.1 Information Security Ownership

The findings from the study reveal both similarities and differences among the departments regarding their ownership of information security. All departments acknowledge the significance of information security, which appears to stem from diverse sources such as internal training programs and individual experiences. However, differences exist in the level of interest demonstrated by each department. These differences may be attributed to the varying background, education, and degrees of technical involvement within the departments.

The sales department shows relatively lower interest in information security, which aligns with its limited engagement in technical aspects of the organization. The primary focus on the sales department lies in customer interaction. In terms of information security ownership, employees within this department demonstrate moderate reflection on their roles and responsibilities.

In contrast, the development department, known for its technical expertise, displays a higher level of interest in information security. The employees in this department show a combination of personal and professional interest, showcasing a deep understanding of the importance of security. Their sense of security ownership is evident in their emphasis on pen-testing as a means to enhance security and their focus on securing the products they develop. This heightened interest can be attributed to their daily interactions with information systems and their involvement in security-related tasks.

The delivery department falls in the middle, with a range of interests in information security stemming from a mix of personal and professional motives. This department comprises employees from diverse backgrounds and educations, resulting in a versatile workforce. The employees in the delivery department demonstrate a good sense of information security ownership as they reflect on their responsibilities regarding customer data.

One notable difference between the departments lies in their emphasis on different aspects of information security. While the delivery and sales departments prioritize customer interaction, the development department places a greater emphasis on product security. These differences reflect the varying priorities and responsibilities within each department.

The findings highlight the varying levels of interest and engagement in information security across the departments. This is consistent with the literature, which suggests that security ownership can differ among employees based on their backgrounds, education, and technical involvement. The development department, characterized by its technical expertise, demonstrates a higher level of interest in information security, supports the literature's claim that employees with technical roles tend to exhibit a deeper understanding and engagement with security (Alnatheer, Chan, & Nelson, 2012).

The sales department, on the other hand, shows relatively lower interest in information security, which is in line with the literature's observation that departments less involved in technical aspects of the organization may have lower levels of engagement with security. The focus of the sales department on customer interaction may contribute to their perception of information security as less relevant to their primary responsibilities (Ismail, 2022).

Overall, the findings from the interviews align with the literature's emphasis on the significance of understanding security roles and responsibilities and the varying levels of interest and engagement among employees. The differences observed in the emphasis on different aspects of information security across the departments also resonate with the existing literature. The findings provide empirical support and further insight into the relationship between departmental characteristics, individual interests, and information security ownership.

5.2 Information Security Knowledge and Awareness

In terms of information security knowledge and awareness, the departments exhibit both similarities and differences. The similarities are evident in their overall awareness of threats and risks in information security, as well as their varying levels of familiarity with the security measures implemented within the organization. However, the findings also reveal notable differences in the extent of awareness and understanding of specific threats and risks, as evidenced by the depth and detail of their explanations. These differences may be influenced by the department's respective areas of expertise, which aligns with the patterns observed in information security ownership. Moreover, divergent perspectives on the importance and necessity of certain security measures further emphasize the distinctions between the departments.

The delivery department demonstrates a high level of awareness regarding diverse threats and risks in information security. Specifically, the employees show a strong understanding of hacking and social engineering techniques. They also exhibit comprehensive knowledge of internal security protocols and measures related to customer data and safety. This confidence in responding to security incidents and promptly notifying the appropriate personnel may stem from their managerial roles within the department.

In contrast, the sales department displays notable awareness of internal threats to information security, particularly the concept of unfaithful servants. While the employees demonstrate knowledge and recognition of various threats, their responses lack detailed descriptions and reflection. Most of their knowledge and awareness are derived from internal nano learning courses. Additionally, the employees in this department exhibit varying levels of familiarity with internal security measures, ranging from a lack of knowledge to knowing whom to contact for assistance.

The development department exhibits commendable awareness of various risks in information security, including hacking, phishing, and data leakage. This heightened awareness can be attributed to the specialized expertise and technical nature of their roles. The employees demonstrate comprehensive knowledge of the security measures implemented within the organization. Notably, their emphasis on coding security and staying updated with tools and trends reflects their understanding of the importance of addressing security issues and threats. It is worth noting that one employee within this department expresses disapproval and highlights potential challenges related to specific security measures, providing an interesting perspective for further exploration.

Overall, the findings from the interviews provide insights that resonate with the existing literature on information security awareness and challenges in organization. They highlight the importance of fostering a culture of awareness and training, understanding the specific needs and perspectives of different departments, and addressing potential conflicts between security requirements and work goals (Govender, Loock, & Kritzinger, 2018).

The differences observed among the departments in terms of awareness and understanding of specific threats and risks also resonate with the literature. Different departments may have varying areas of expertise and responsibilities, leading to differences in their knowledge and awareness of information security. Additionally, the divergent perspectives on the importance and necessity of certain security measures, as seen in the development department employee’s disagreeing viewpoint, reflect the complex nature of information security and the need for ongoing discussions and evaluation. The literature emphasizes challenges in information security awareness and practices, including finding the ideal information security policy for the organization, addressing conflicts between security requirements and work goals, and mitigating the potential for bad practices or circumventing security compliance (Woltjer, 2017). These challenges are relevant to the discussions around perspectives on security measures, and the need for ongoing training and awareness initiatives (Subramanian V., 2012).

5.3 Challenges

In terms of work goals, there are notable similarities and differences among the three departments. All departments share a common objective of meeting customer needs and ensuring customer satisfaction. The delivery department focuses on successful project implementation and stakeholder value. The sales department prioritizes income generation, meeting sales targets, and cultivating positive customer relationships. The development department aims to develop high quality software and continuously improve work tasks. These shared goals underscore the significance of customer focus and the importance of delivering products or services that meet customer expectations.

Furthermore, all departments encounter challenges related to information security policies and routines. The delivery department faces difficulties in accessing customer data and securely sharing passwords, while also grappling with organizational processes and requirements that may cause delays. In contrast, the sales department struggles with the categorization of documents, which can be confusing due to the existence of multiple labeling options. The development department highlights the challenge of adhering to the policy of locking screens when leaving the office, with one employee expressing frustration and perceiving it as an unnecessary burden.

There are notable differences among the departments as well. The challenges faced by the delivery department are primarily associated with customer interactions and accessing customer data securely. The sales department, being less technically oriented, encounters relatively fewer challenges concerning information security routines and policies. On the other hand, the development department, with its technical expertise, places particular emphasis on coding security and staying updates on tools and trends. The department’s challenge lies in striking the right balance between security protocols and employee motivation, particularly regarding the practice of screen locking.

The challenges encountered by each department shed light on the specific requirements and constraints inherent in their respective roles. Understanding these similarities and differences enables the organization to tailor its information security measures to address the unique needs and challenges of each department. This approach fosters a culture of security while empowering employees to effectively pursue their work goals.

Information security policies and routines emerge as a common challenge in both the interviews and the literature. The literature underscores the challenges organizations face in ensuring employees’ compliance with security tasks in the information security policy (Subramanian V., 2012). The interviews confirm this, with each department encountering specific challenges related to information security policies and routines. The delivery department struggles with accessing customer data and securely sharing passwords, the sales department faces issues with document categorization, and the development department expresses frustration with the practice of screen locking (Kolkowska, 2011).

The interviews reveal that some routines and processes may hinder the smooth progression of work goals, leading employees to find ways to work around security compliance. This aligns with the literature's exploration of the misalignment between work goals and ISP. The challenges faced by the departments reflect these conflicts, such as delays caused by organizational processes or frustrations with security practices that hinder work efficiency (Sadok, 2020).

The literature also highlights the existence of information security subcultures within organizations, where different departments or groups may have varying attitudes and values regarding information security (Kolkowska, 2011). While the interviews do not explicitly discuss subcultures, they indirectly touch upon the differences between departments, such as the technical expertise of the development department compared to the sales department, which is less technically oriented. These differences may influence the perception of security and the challenges faced by each department.

5.4 Implications for Practice

The findings from this study have important implications for practice in the field of information security. The differences observed among departments regarding their interest and engagement with information security highlight the need for tailored measures in organizations. It is crucial for organizations to design information security policies, routines and training programs that take into account the unique characteristics and requirements of each department. This tailored approach will enhance compliance and ownership of information security within the organization.

Promoting collaboration and knowledge sharing between departments is crucial in improving information security understanding and alignment of work goals with security requirements. Facilitating communication and cooperation between different departments can help bridge gaps in knowledge and expertise, allowing for a better integration of security measures within the workflow. By sharing experiences and best practices, departments can learn from each other and develop a more comprehensive approach to information security.

Organizations should demonstrate flexibility and adaptability in their information security policies and routines. Recognizing the unique challenges and requirements of each department is essential in ensuring effective security practices without compromising operational efficiency. Regular evaluation and feedback loops can aid in identifying areas where adjustments are needed to strike a balance between security and organizational goals.

By implementing these implications in practice, organizations can enhance their information security, strengthen compliance, and create a culture of security. This will contribute to the protection of sensitive information and mitigate potential security risks within the organization.

5.5 Implications for Research

The exploration of subcultures within the organizations related to information security expands on existing literature that has examined the role of organizational culture in shaping attitudes and behaviors. By investigating how different departments develop distinct attitudes, values, and practices regarding information security, this research provides a deeper understanding of the underlying factors that influence compliance and ownership. It contributes to the existing knowledge by highlighting the importance of considering the dynamics of departments and adapting security approaches to address the unique needs of each department.

The investigation of the alignment between work goals and information security across different departments and roles builds on existing studies that have explored the challenges and conflicts organizations face in balancing security requirements and work efficiency. By studying the specific areas of misalignment and identifying potential challenges, this research offers practical insights into developing strategies that support both information security and productivity. It contributes to existing literature by providing an understanding of the complexities involved in aligning security measures with the goals and responsibilities of different departments.

5.6 Limitations

The selection of interview participants for this study was conducted by the organization's contact person, thereby excluding my involvement in the participant selection process. While the selection criteria were met, ensuring the inclusion of four employees from each department, it would have been preferable to have all participants located in the same office. However, considering the organization's resource limits, it is understandable that involving 12 employees from a single office may not be an efficient use of company resources. This also brings up the limitation of sample size, as four employees from each department is not enough to make a generalized statement about their department. It is important to acknowledge that having participants from the same office would have minimized potential variables that could impact the study's outcomes, including office culture, available resources, and the number of employees working in a given office.

Furthermore, it is worth noting that the interviewed employees have varying lengths of time within the organization. Some participants had been working for one or two years, while others had been employed for a considerable duration. Additionally, some participants had been with the organization since its inception as part of another organization. The influence of the previous organizational culture on their perspectives and experiences cannot be disregarded, as training practices and regimes may have differed between the previous and current organization.

Another point that was not addressed in this study is how the delivery department's employees are all in a managerial position. As they all are responsible for different teams within the delivery department, the findings from the interviews may not reflect the department, but rather reflect the individual teams that are a part of the department. Because of the nature of the department being made up of many different teams, it becomes harder to generalize a statement that reflects the whole department.

5.7 Future Research

There are several key implications for future research that can contribute to the advancement of information security culture within organizations. One important area for further exploration is the existence of subcultures within organizations related to information security. Investigating how different departments develop distinct attitudes, values, and practices regarding information security can provide valuable insights into the underlying factors that influence compliance and ownership. Understanding these subcultures can help organizations tailor their approaches to address the unique needs and challenges of each department.

This study interviewed four employees, each from different departments within the same organization. Future research should use a larger sample size to get a more accurate impression of each department. This can be done through quantitative methods, which should produce a more accurate result. Future research should also consider what types of subcultures it studies, as in this study, the development department proved to be a varied department with different fields of expertise, making the results more varied. If I were to do it again, I would be more specific about the departments chosen, include a bigger sample size, and add more structure to the interviews.

Studying the alignment between work goals and information security across different departments and roles is also essential. This research can shed light on potential conflicts and challenges that arise when balancing security requirements and work efficiency. By identifying areas of misalignment, organizations can develop strategies to strike a balance that supports both information security and productivity.

As this study was affected by a time constraint, looking into long-term impact of information security measures on employee satisfaction, productivity, and organizational outcomes is another area for future research to explore. This research can provide valuable insights into the effectiveness of security measures and their impact on overall organizational performance.

6 CONCLUSION

In conclusion, this study aimed to investigate the influence of subcultures within an organization on information security culture. The findings reveal both similarities and differences among departments in terms of information security ownership, knowledge and awareness, and work goals and challenges. The study confirms the significance of understanding security roles and responsibilities, as well as the varying levels of interest and engagement among employees. The departments' characteristics, such as technical expertise and customer focus, play a role in shaping their perspectives on information security. Challenges related to information security policies and routines were identified, highlighting the need to strike balance between security protocols and work efficiency. While subcultures were not explicitly discussed, the differences between departments indirectly suggest the presence of information security subcultures. The study acknowledges limitations such as the sample size and participant selection process, emphasizing the need for further research to generalize the findings. Overall, the study contributes to the existing literature by providing empirical insights into the relationship between subcultures, information security culture, and organizational dynamics.

REFERENCES

Ali R.F., D. P. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 33-83. doi:doi:10.3390/app11083383

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Proceedings of the 16th Pacific Asia Conference on Information Systems*, 1-15. Retrieved from https://eprints.qut.edu.au/80598/1/Understanding%2BAnd%2BMeasuring%2BInformation%2BSecurity%2BCulture.pdf

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford University Press.

Büschgens, T., Bausch, A., & Balkin, D. B. (2013). Organizational Culture and Innovation: A Meta-Analytic Review. *Journal of Product Innovation Management*, 763-781. doi:https://doi.org/10.1111/jpim.12021

Choi, M. S. (2016). Leadership of Information Security Managers on the Effectiveness of Information Systems Security Through Mediate of Organizational Culture. *Advanced Multimedia and Ubiquitous Engineering, Singapore*, 649-654. doi:https://doi.org/10.1007/978-981-10-1536-6_84

Connolly, L., & Lang, M. (2012). Data Protection and Employee Behavior: The Role of Information Systems Security Culture. *IADIS International WWW/Internet Conference*. Retrieved from https://www.researchgate.net/publication/323550919_DATA_PROTECTION_AND_EMPLOYEE_BEHAVIOUR_THE_ROLE_OF_INFORMATION_SYSTEMS_SECURITY_CULTURE

Cram, W. A. (2020). Maximizing Employee Compliance with Cybersecurity Policies. *MIS Quarterly Executive*. doi:19.17705/2msqe.00032

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 72-94. doi:https://doi.org/10.1016/j.cose.2017.05.002

Govender, S., Loock, M., & Kritzinger, E. (2018). Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. *Cyberspace Safety and Security*, 281-290. doi:https://doi.org/10.1007/978-3-030-01689-0_22

Hannabus, S. (1996). Research interviews. *New Library World*, 22-30. doi:https://doi.org/10.1108/03074809610122881

Ismail, O. (2022). Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs. *International Conference on Design Science Research in Information Systems and Technology*, 319-332.

Kim, D., & Solomon, M. (2013). *Fundamentals of Information Systems Security.* Retrieved from Google: https://books.google.no/books?hl=no&lr=&id=me0QAAAAQBAJ&oi=fnd&pg=P

R2&dq=information+systems+security&ots=r1UlNfFPzE&sig=cvTLNuehqVflBrCQPhFG18KU-PQ&redir_esc=y#v=onepage&q=information%20systems%20security&f=false

Kolkowska, E. (2011). SECURITY SUBCULTURES IN AN ORGANIZATION - EXPLORING VALUE CONFLICTS. *ECIS 2011 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2011/237/

Kvale, S. (2011). *Doing Interviews.* Sage Publications, LTD. doi:https://doi.org/10.4135/9781849208963

Lin, C., & Luo, X. (. (2021). Toward a Unified View of Dynmaic Information Security Behaviors: Insights from Organizational Culture and Sensemaking. *SIGMIS Database*, 65-90. doi:https://doi.org/10.1145/3447934.3447940

Lopes, I. O. (2015). Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. *New Contributions in Information Systems and Technologies, Cham*, 459-468. doi:https://doi.org/10.1007/978-3-319-16486-1_45

McCombes, S. (2023, January 30). *Methodology: What Is a Case Study*. Retrieved from Scribbr: https://www.scribbr.com/methodology/case-study/

NVivo. (2023). *Content: About Nvivo*. Retrieved from NVivo: https://help-nv.qsrinternational.com/20/win/Content/about-nvivo/about-nvivo.htm

Pranas Žukauskas, J. V. (2018). *Philosophy and Paradigm of Scientific Research.* InTech. doi:10.5772/intechopen.70628

R. Rohan, D. P. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon 2023*. doi:https://doi.org/10.1016/j.heliyon.2023.e14234

Romeo, C. (2023). *6 ways to develop a security culture from top to bottom*. Retrieved from TeachBeacon: https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom

Roopa, S. R. (2012). Quesitonnaire Designing for a Suvery. *The Journal of Indian Orthodonict Society*, 37-41. doi:10.5005/jp-journals-10021-1104

Sadok, M. A. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security*, 467-483. doi:https://doi.org/10.1108/ICS-01-2019-0010

Siponen M., A. M. (2014). Employees' adherence to information security policies: An exploratory field study. *Information Management*, 217-224. doi:https://doi.org/10.1016/j.im.2013.08.006

Sohrabi Safa, N. V. (2016). Information security policy compliance model in organizations. *Computers & Security*, 70-82. doi:https://doi.org/10.1016/j.cose.2015.10.006

Subramanian V., S. R. (2012). PCIEF: A policy conflict identification and evaluation framework. *International Journal of Information and Computer Security*, 48-67. doi:10.1504/IJICS.2012.051090

Wall, J. I. (2012). The Dark Side of Leadership in Information Systems Security: A Model of the Efect of Manager Transgressions on Employee Security Behaviors. *Proceedings of the 18th Americas Conference on Information Systems*. Retrieved from https://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/12/

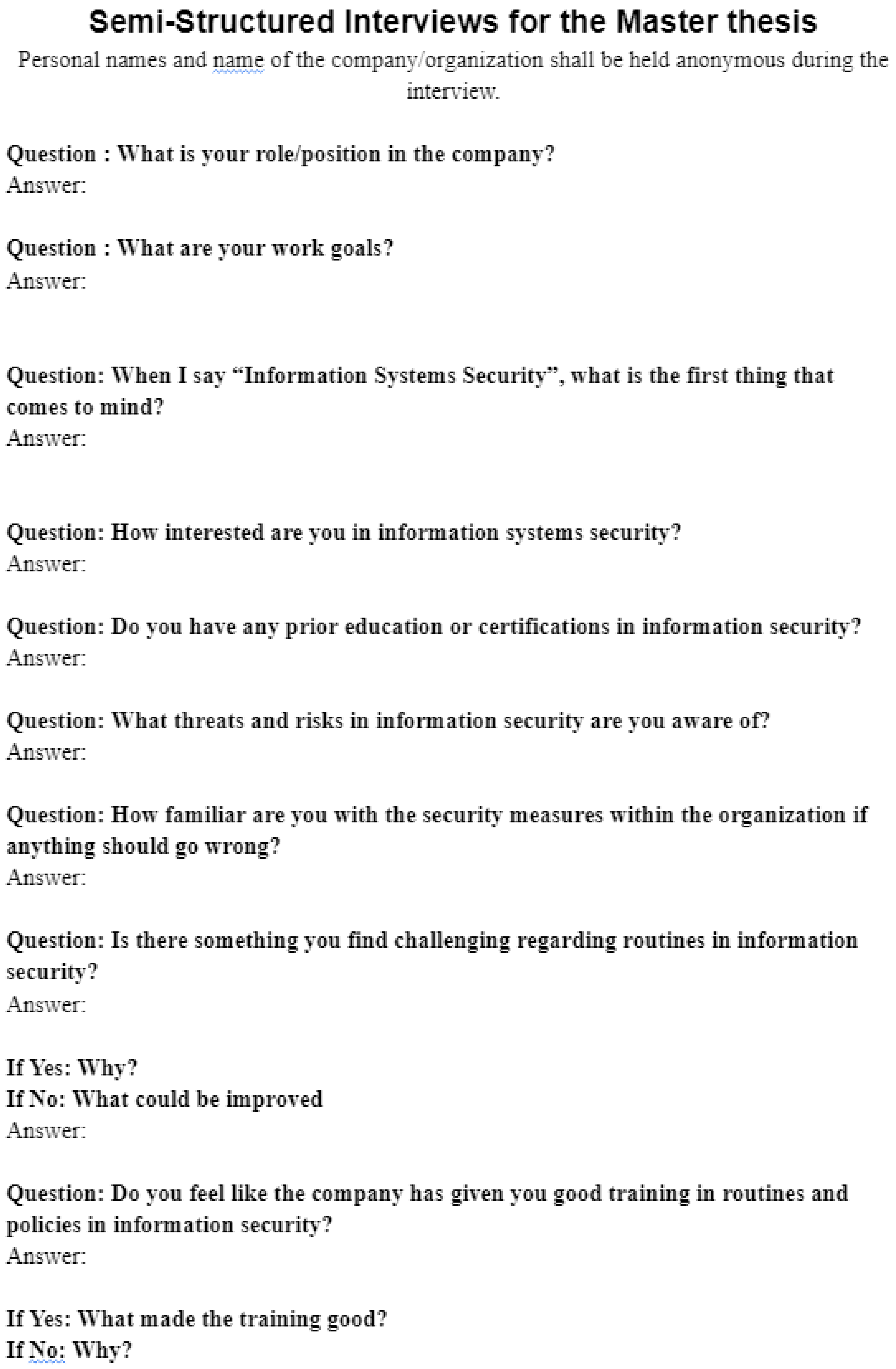
Whitman, M., & Mattord, H. (2013). *Management of Information Security (Fourth Edition).* Cengage Learning.

Woltjer, R. (2017). Workaround and trade-offs in information security - an exploratory study. *Information and Computer Security*, 402-420. doi: https://doi.org/10.1108/ICS-02-2016-0017

Xu Z., G. K. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Knowledge Management Research and Practice*, 824-842. doi:https://doi.org/10.1108/JEIM-10-2018-0229

Zhang, Y., & Wildemuth, B. M. (2005). Qualitative Analysis of Content. *Human Brain Mapping*, 2197-2206. Retrieved from https://www.ischool.utexas.edu/~yanz/Content_analysis.pdf

Appendix



Semi-Structured Interviews for the Master thesis

Personal names and name of the company/organization shall be held anonymous during the interview.

Question : What is your role/position in the company?
Answer:

Question : What are your work goals?
Answer:

Question: When I say "Information Systems Security", what is the first thing that comes to mind?
Answer:

Question: How interested are you in information systems security?
Answer:

Question: Do you have any prior education or certifications in information security?
Answer:

Question: What threats and risks in information security are you aware of?
Answer:

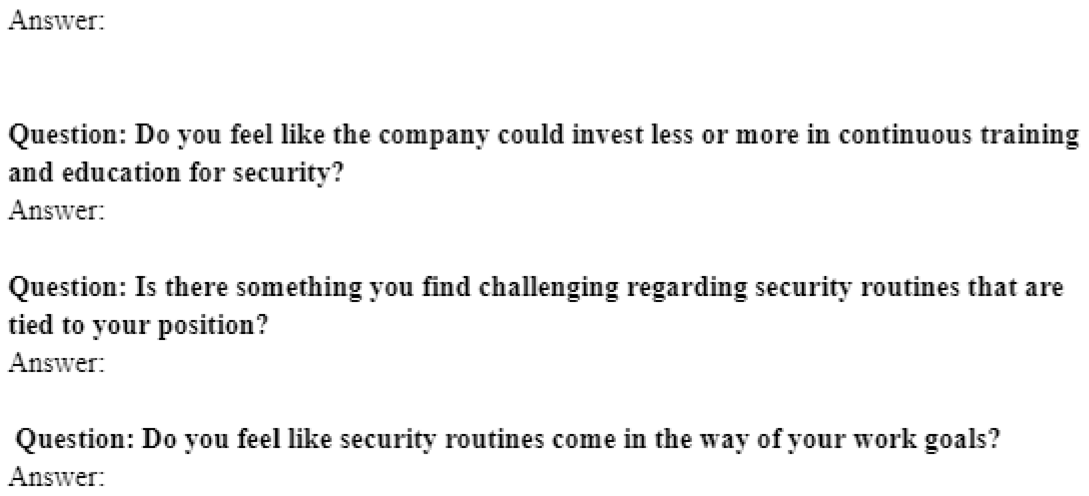
Question: How familiar are you with the security measures within the organization if anything should go wrong?
Answer:

Question: Is there something you find challenging regarding routines in information security?
Answer:

If Yes: Why?
If No: What could be improved
Answer:

Question: Do you feel like the company has given you good training in routines and policies in information security?
Answer:

If Yes: What made the training good?
If No: Why?



Answer:

Question: Do you feel like the company could invest less or more in continuous training and education for security?
Answer:

Question: Is there something you find challenging regarding security routines that are tied to your position?
Answer:

Question: Do you feel like security routines come in the way of your work goals?
Answer: