UiA University of Agder

Master

How do security managers motivate employees' security behavior - Leadership perspective

SANDRA CATHRINE BJØNNES

SUPERVISOR
Marko Ilmari Niemimaa

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

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

I would like to thank my supervisor, Associate Professor Marko Ilmari Niemimaa, from the Department of Information Systems, for his guidance, feedback, and support throughout this process. His expertise, patience, and encouragement were helpful in shaping this thesis and achieving its goals. Our meetings during this time have been of great help, and I appreciate all the feedback and advice he has given.

I would also like to thank the anonymous individuals who participated in the interviews for this study. Without their willingness to share their knowledge and perspectives, this research would not have been possible. Their insights and contributions are very appreciated.

Lastly, I would like to express my gratitude to my family and friends, who have been a constant source of motivation and encouragement throughout this process. Their belief in me and my abilities has been essential in helping me overcome the challenges and obstacles that came my way.

Thank you all for your contributions, support, and encouragement.

Kristiansand
June 2nd 2023

Sandra Bjønnes

Sandra Cathrine Bjønnes

Abstract

In today's digital world, there are several possible threats to organizations. Because of these possible threats, it is important to be as aware as possible and prepared for attacks to occur. Large and small organizations should have a good team of employees and a good leader to carry the organization through possible threats and attacks. Cybersecurity is not just about technology but a mix of different aspects involving people and policy. For an organization to succeed in the field of cybersecurity, the organization needs to have committed and skilled managers at the top. This study examines how security managers seek to motivate and influence employees' security behavior and which leadership styles they adopt to do so. There is a need for research that specifically addresses the approaches that security managers can adopt to motivate their employees toward security behavior.

To find this out, the research approach I used was a qualitative interview study with semi-structured interviews and a systematic literature review approach. I interviewed eight security managers in various organizations from Norway and abroad. The interviews were transcribed and then coded into different categories. I also used a systematic literature review approach to look at previous studies on this topic and create a literature background for my study.

The findings show a variation in the leadership styles adopted by the different security managers and the approaches used to motivate employees. I created a table with an overview of the leadership styles I found in my study, including the different approaches related to the leadership styles. There are differences in the approaches that are used to motivate in relation to the adopted leadership styles, but also similarities across the styles.

This study contributes to promoting approaches that can help various organizations and security managers to motivate and influence their employees' security behavior. It can also help raise awareness of how necessary it is to motivate your employees, especially in cybersecurity.

Contents

Acknowledgements **ii**

Abstract **iii**

List of Figures **vii**

List of Tables **ix**

1 Introduction **1**

1.1 Research gap 2

1.2 Research question 2

1.3 Research approach 2

1.4 Thesis structure 3

2 Literature background **4**

2.1 Security managers as leaders - CISO 4

2.1.1 Leadership skills 5

2.2 Leadership styles 6

2.2.1 Paternalistic leadership 7

2.2.2 Transactional leadership and Transformational leadership 8

2.2.3 Passive/avoidant leadership 10

2.2.4 Servant leadership 11

3 Research approach **12**

3.1 Literature review approach 12

3.1.1 Process of systematic literature review 13

3.1.2 Literature criteria 14

3.1.3 Searching for literature 14

3.1.4 Screening process 15

3.2 Qualitative approach 18

3.2.1 Research method 18

3.2.2 Data collection 18

3.2.3 Data analysis 21

3.2.4 Ethical consideration 23

4 Findings **24**

4.1 Leadership styles 24

4.2 Motivation 27

4.2.1 The need for motivation 27

4.2.2 Approaches to motivation 29

4.2.3 Approaches that don't work 33

4.2.4 Future approaches 35

5 Discussion **38**

5.1 The various leadership styles 38

5.2 Approach to motivation 41

5.3 The different leadership styles in relation to the approaches to motivation . . 42

5.4 Implications for practice 45

5.5 Limitations and future research 45

6 Conclusion **47**

References **48**

A Interview guide **50**

B Consent form **53**

List of Figures

3.1 PRISMA Flow Diagram 16

3.2 Qualitative semi-structured interview guide framework (Kallio et al., 2016) . 19

3.3 Qualitative data analysis (Miles & Huberman, 1994) 22

List of Tables

3.1 Keywords used in the search string 15

3.2 Reviewed articles 18

3.3 Subject selection 21

5.1 Overview of the leadership styles and approaches to motivation 44

Chapter 1

Introduction

In today's digital world, there are several possible threats to organizations. According to ENISA's (European Union Agency for Cybersecurity) Threat Landscape report from 2022, the top three threats identified were ransomware, malware, and social engineering threats (Naydenov et al., 2022). This indicates some of the challenges organizations deal with daily. Because of these possible threats, it is important to be as aware as possible and prepared for attacks to occur. Organizations, large and small, should have a good team of employees and a good leader to carry the organization through possible threats and attacks that may occur.

In March 2019, Norsk Hydro, a Norwegian industrial group with operations in energy and aluminum, was hit by an extensive cyber attack, specifically a ransomware attack. The attack affected the entire global organization in more than 40 countries (Hydro, 2021). In this case, the ransomware virus that hit Hydro is called LockerGoga. The hackers behind the attack demanded the ransom to be paid in cryptocurrency, specifically Bitcoin, but Hydro didn't pay anything. Although Hydro didn't pay the ransom demand, they have estimated the total cost of the cyber attack at around NOK 800 million (Hydro, 2020). The attack may have started with something as simple as an e-mail, where an employee trusted that the content of the e-mail was secure and came from an authentic sender (Brekke & Gundersen, 2019). This example shows the importance of awareness of cybersecurity and the need for good training within organizations.

Cybersecurity is not just about technology but a mix of different aspects involving people and policy. Dr. Mansur Hasib (2014) defines cybersecurity as: "Cybersecurity is the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy and technology, while perennially improving over time" (Hasib, 2014, p. 3). For an organization to succeed in the field of cybersecurity, the organization needs to have committed and skilled managers at the top. Many senior executives view cybersecurity as a technology problem and do not embrace their role in the leadership and management of cybersecurity. The top management

needs to view cybersecurity as their responsibility within the organization, and successful cybersecurity leadership starts at the highest executive levels of an organization (Hasib, 2014, pp. 5–6). According to Børresen (2023), studies show that employees who are not motivated in the workplace experience 60% more accidents than motivated employees. This study examines how security managers seek to motivate and influence employees' security behavior and which leadership styles they adopt to do so.

1.1 Research gap

Despite the extensive literature on employee motivation and its impact on organizational outcomes, there is a lack of research that focuses explicitly on the role of security managers in motivating their employees toward security behavior. While previous studies have explored the factors that influence employee motivation from the employees' perspective, little attention has been paid to how security managers can motivate their employees regarding security. As security breaches and cyber threats continue to pose a significant risk to organizations, it is crucial to understand the unique challenges security managers face in motivating their employees towards a culture of security.

1.2 Research question

There is a need for research that specifically addresses the approaches that security managers can adopt to motivate their employees toward security behavior. Hence this study's research question is: "How do security managers seek to motivate and influence employees' security behavior?"

1.3 Research approach

The research approach taken in this master thesis involves a systematic literature review of existing literature relevant to the research topic of leadership, motivation, and cybersecurity. The process consists in searching for literature in electronic databases, backward searching, and forward searching using the main search terms of leadership, motivation, and cybersecurity, including other synonyms. The selection criteria for literature include relevance to the research question and topic, and the screening process involves reviewing the articles' titles, abstracts, and full text. After reviewing 205 results, I was left with 11 relevant articles for my study. The study is conducted through a qualitative interview study with semi-structured interviews to gain a deeper understanding of how security managers in different organizations motivate and influence employees' security behavior, as well as looking

at different leadership styles and approaches used to motivate and influence. The interview guide consists of various questions divided into four different categories.

1.4 Thesis structure

Chapter 1 - Introduction provides an overview of the research problem, the research gap, and the research question, including the aims and motivation of the research.

Chapter 2 - Literature background gives an overview of the background and related work regarding this study.

Chapter 3 - Research approach discusses the literature review process and the research approach and methods used. Ethical considerations are also a part of chapter three.

Chapter 4 - Findings presents the most important findings from the study.

Chapter 5 - Discussion is where I discuss the findings from previous studies and the findings from my study. This chapter also contains implications for practice, limitations, and future research.

Chapter 6 - Conclusion summarizes the most important research findings and provides a conclusion of the study and the research question.

Chapter 2

Literature background

This chapter presents the literature background for this study, including research from previous studies. The findings from the literature review are sorted into different categories, including Security managers as leaders, specifically the Chief Information Security Officer (CISO), Leadership skills, and Leadership styles. This chapter introduces the role of the Chief Information Security Officer (CISO) and the responsibilities that come with this role, communication as an important leadership skill, and various leadership styles like Paternalistic leadership, Transactional leadership, Transformational leadership, Passive/avoidant leadership, and Servant leadership. This study doesn't cover security behavior because the focus is on security managers and how they motivate.

2.1 Security managers as leaders - CISO

Previously, the role of the Chief Information Security Officer (CISO) was mainly focused on defining technical security standards and policies. But today, organizations are becoming more aware that cyber risk is directly related to their innovation and growth strategies (Monzelo & Nunes, 2019). According to Monzelo & Nunes, the CISO is becoming more recognized as a core element in the definition of the organization's information risk management strategy, with different responsibilities like: (1) developing, managing, and operationalizing the security strategy, (2) monitoring and evaluate the information security practices frequently, (3) implement information security audits and risk assessments, (4) supervise, lead and train their department and team, (5) making the organization compliant with regulations regarding information security, (6) develop and implement business continuity plans, (7) protect the intellectual property of the organization, (8) information security risks and strategy training and awareness of the employees, (9) handle information security budgets, and (10) report to the board of directors and being an active member in the top management team (Monzelo & Nunes, 2019).

In the study conducted by Monzelo & Nunes, they state that the CISO must have a technical background. However, they do not need to be a pure technician since they should have a critical view of information security issues, be aware of existing techniques, and be able to communicate sufficiently with the technical teams responsible for the topics. Additionally, the CISO should also have a business, governance, and strategic vision on issues regarding security (Monzelo & Nunes, 2019). They also state that it is the CISO's responsibility to influence and improve the culture in the organization in order to support information security. In their study, they conclude that: "The CISO role and their mission in organizations may be directly related to the awareness that exists on the matter, and that information security is not only an organizational matter but also a social and cultural theme" (Monzelo & Nunes, 2019).

In a study conducted by Sveen et al. (2023), they mention the importance of a CISO that can communicate well. In the article, it is also mentioned that technical expertise is not the only key competence of a CISO. According to this article, in addition to technical expertise, the CISO should also have the following properties: excel in communication skills, possess adequate business knowledge, and have interpersonal skills (Sveen et al., 2023). It is important for the CISO to communicate well and be able to translate his/her technical expertise into a more fitting language to make other employees and top management understand the cybersecurity risk or solutions better (Sveen et al., 2023).

A study conducted by Karanja (2017, as cited in Sveen et al., 2023) researched the position of the CISO by looking at the role of CISOs before and after an IT security breach. The results showed that 6 out of 13 organizations didn't have a CISO in their organization before the security breach, but 5 out of those 6 organizations hired a CISO after the security breach. Karanja also stated that IT security is being seen as a more technical and specialist function and that CISOs struggle to gain credibility from the management (Karanja, 2017, as cited in Sveen et al., 2023).

In the study conducted by Sveen et al. (2023), they conclude that the perceived role and responsibilities of the CISO include the following: 1) Excel the goals and strategies of the business; 2) Communicate with the top management and learn about the most important assets of the organization; 3) Define appropriate/necessary measures, i.e., technical and strategic controls; and 4) Being a good communicator and security adviser, and also being able to propose appropriate measures to the top management in an understandable way.

2.1.1 Leadership skills

An important leadership skill is communication. The ability to communicate well with other employees and managers is essential for the message to go through. According to a study conducted by Maynard et al. (2018), CISOs are required to have good communication, collaboration, and influential skills, so that they are able to work with other business leaders

and secure support from senior management and/or board when it's required, and also to influence employee behavior. They also state that communication gaps exist between ISM and senior management, other functional parts of the organization, and employees in general.

In a study conducted by Sveen et al. (2023), one of the findings involving communication is that the CISO's responsibility often relates to and evolves around communication. They state that the most important job of the CISO is to communicate what might be a little more technically demanding for the other leaders to understand, using correct, proper, and understandable business terminology and language. Their study also shows that skills are needed for communicating cybersecurity to everyone in an understandable way, regardless of their background.

> "When the top management involves themselves in cybersecurity and has direct communication with a CISO that knows how to communicate in a good way, this might help in enabling the CISO's abilities to work on a more strategic level, and by doing so also improve the organization's cybersecurity overall." (Sveen et al., 2023)

According to a study conducted by Monzelo & Nunes (2019), the CISO should be a leader that is able to manage people and have good communication skills, both up and down on the organizational chain, and the CISO should also have a reporting capability to pass the message to the board appropriately.

> "To be able to transmit the message properly, the CISO must be able to communicate how the security risks which the organization is exposed may manifest in risks to the operation of the organization and must be able to understand and transmit not only in terms of financial risks, but also social and environmental risks." (Monzelo & Nunes, 2019)

2.2 Leadership styles

Much of the previous literature about leadership in cybersecurity deals with different leadership styles and how different leadership styles can impact employees and organizations. Westwood (1992, as cited in Jiawen et al., 2019) states that leaders of different leadership styles have different ways of implementing plans and motivating people. An example described by Truss et al. (1997, as cited in Jiawen et al., 2019) is that in compiling and executing information security policies, some leaders may prefer strict control while others may prefer a benign approach. Another statement by Ouchi and Maguire (1975, as cited in Jiawen et al., 2019) is that some leaders may prefer using articulated prescriptions to regulate their employees' behavior while others may prefer relying on social power and self-regulation.

Following, I present various leadership styles from previous literature, including Paternalistic leadership, Transactional leadership, Transformational leadership, Passive/avoidant leadership, and Servant leadership.

2.2.1 Paternalistic leadership

Both Jiawen et al. (2019) and Feng et al. (2019) write about how paternalistic leaders motivate employees' information security policy (ISP) compliance.

In an article written by Jiawen et al. (2019), Paternalistic Leadership (PL) is described as a father-like leadership style (Farh et al., 2000, as cited in Jiawen et al., 2019). Farth & Cheng (2000, as cited in Feng et al., 2019) describe Paternalistic Leadership as a style that combines strong discipline and authority, parental benevolence and moral integrity, and they define Paternalistic Leadership as having three different dimensions: authoritarianism, benevolence, and morality.

Authoritarian leaders are described as very controlling and rigorous, and authoritarian leaders often use punishment and monitoring as effective control mechanisms to ensure employees' obedience (Chan 2014; Pellegrini & Scandura 2008, as cited in Jiawen et al., 2019). To ensure employees' Compliance, authoritarian leaders tend to adopt hard control strategies, such as directly inherently implementing reward and punishment (Kelman & Hong, 2016, as cited in Jiawen et al., 2019). Another statement is that authoritarian leaders are mostly concerned about doing things in the right way and ignore the perceptions of their subordinates (Wu & Tsai, 2012, as cited in Jiawen et al., 2019).

According to Cheng et al. (2004, as cited in Jiawen et al., 2019), benevolent leaders show great concern for their subordinates' well-being and are willing to make an effort to best secure their interests. Thus, benevolent leaders tend to initiate and support a series of information security practices and nurture the corresponding climate to protect the IT assets of the organization. As stated by Zhang et al. (2015, as cited in Jiawen et al., 2019), benevolent leaders are sensitive to employees' needs and avoid putting their employees in embarrassment or dilemma. Because of this, benevolent leaders would initiate a series of measures, such as training and education programs and courses to emphasize the organizational value and express their expectations to the employees (Jiawen et al., 2019).

As stated by Wu & Tsai (2012, as cited in Jiawen et al., 2019), moral leaders feel responsible for organizational and employees' interests. Moral leaders feel that it is their obligation to protect the information assets in their organization from different threats. Therefore, moral leaders take information security issues seriously and encourage such value among their employees (Jiawen et al., 2019).

"Moral leaders promote their values via two-way communication and decision-

> making. On the one hand, moral leaders directly explain to employees about the benefit and importance of information security to their organization. On the other hand, moral leaders may initiate a series of information security policies, procedures, and practices to protect their organization. These policies and procedures inform employees which behavior will be rewarded or supported." (Erben & Guneser, 2008, as cited in Jiawen et al., 2019)

The study conducted by Jiawen et al. (2019) shows that the three Paternalistic Leadership dimensions, Authoritarian Leadership, Benevolent Leadership, and Moral Leadership, have a significant positive influence on employees' ISP Compliance intention. Further, they state, "This suggests that leaders who score high in these leadership styles will have stronger effect on employees' ISP Compliance. This finding explains why some leaders are more effective than others in motivating employees' ISP Compliance" (Jiawen et al., 2019). An example is that leaders can nurture the climate in their organization by offering supporting programs, such as the security, training, and awareness program, and an open communication working environment, to assist employees in making sense of how their organization values information security (Jiawen et al., 2019).

> "Employees who regard their moral leaders as role models will learn from their leaders to concern about the collective interests and develop the sense of duty to their organization, which will motivate them to make sense of the promoted values and priorities of their organization and protect their organizational information assets." (Jiawen et al., 2019)

Feng et al. state, "Leaders should pay attention to their current leadership style and adjust their behavioral patterns to effectively influence employees' ISP compliance" (Feng et al., 2019). Their research also shows that Paternalistic Leadership effectively encourages desirable IT security behavior.

2.2.2 Transactional leadership and Transformational leadership

According to Pawar and Eastman (1997, as cited in Amankwa et al., 2018), in light of how leaders motivate followers, you can group leadership into two different classifications; transformational leadership and transactional leadership. "Transactional leaders are people being responsive to the necessities of others, who follow them in return for the satisfaction of these necessities" (Jung and Avolio, 1999; Waldman et al., 2001, as cited in Amankwa et al., 2018). According to Amankwa et al. (2018), by differentiation to transactional leaders, transformational leaders are the individuals who, by the drive of their own capacities, are fit to have significant and unprecedented impacts on followers.

> "In the information security context, information security managers may be transformational or transactional leaders seeking to secure sensitive and critical information assets to protect the business, customers, employees and investors from eminent security threats. To achieve information security, business stakeholders, especially employees, are expected to comply with information security policies on daily basis. However, as followers (employees) always look up to their leaders (security managers) for directions, their beliefs, attitudes and behaviour intentions toward ISP compliance may be highly dependent on what leaders portray." (Amankwa et al., 2018)

Referring to previous leadership research, Guhr et al. (Avolio & Bass, 2004; Bass, 1985, as cited in Guhr et al., 2019) defines transformational leadership as a style of leadership that transforms associates to rise above their self-interest by altering their ideals, morale, values, and interests, motivating them to perform better than initially expected. "Transformational leaders are proactive: they seek to optimize individual, group and organizational development and innovation, not just achieve performance 'at expectations" (Avolio & Bass, 2004, as cited in Guhr et al., 2019). In contrast to transformational leaders, Guhr et al. (Avolio & Bass, 2004, as cited in Guhr et al., 2019) define transactional leaders as leaders who display behaviors associated with constructive and corrective transactions, for example, clarifying what the employee should do in order to be rewarded as well as monitoring performance and taking action when problems occur. "Transactional leadership defines expectations and promotes performance to achieve these levels" (Avolio & Bass, 2004, as cited in Guhr et al., 2019).

According to Sadeghi & Lope Pihie (2012, as cited in Guhr et al., 2019), transactional leadership aims to motivate followers by helping them to fulfill their own self-interests. Guhr et al. (Avolio, Bass, & Jung, 1999; Bono & Judge, 2004; Stewart, 2006, as cited in Guhr et al., 2019) states that transactional leadership is mainly composed of 2 dimensions of behavior: contingent reward and active management-by-exception. "Contingent reward encompasses the degree to which followers are rewarded (e.g., wages or prestige) in exchange for meeting defined performance standards" (Bass et al., 1987; Bono & Judge, 2004, as cited in Guhr et al., 2019). "The active management-by-exception leader monitors follower behaviour for mistakes and rule violations and corrects errors and problems before they become severe" (Sadeghi & Lope Pihie, 2012, as cited in Guhr et al., 2019).

As stated by Burns (1978, as cited in Guhr et al., 2019), in contrast to transactional leadership, transformational leadership encourages people to collaborate rather than work individually. Jung & Sosik (2002, as cited in Guhr et al., 2019) describes transformational leaders as charismatic, encouraging people to adapt their values and standards by motivating them to put their own interests behind those of the organization. Four specific components have been identified of transformational leadership; idealized influence, inspirational motivation (IM), intellectual stimulation (IS), and individualized consideration (IC) (Bass et al., 2003;

Geijsel, Sleegers, Leithwood, & Jantzi, 2003; Jung & Sosik, 2002, as cited in Guhr et al., 2019). "Through idealized influence, leaders lead by good example and motivate followers to identify with them" (Bass et al., 2003; Bono & Judge, 2004, as cited in Guhr et al., 2019). "Inspirational leaders promote enthusiasm, optimism, and energy in their followers" (Liu, Siu, & Shi, 2010; Rafferty & Griffin, 2004; Stewart, 2006, as cited in Guhr et al., 2019). "An intellectually stimulating leader inspires followers to develop their own innovative strategies for challenging established methods and improving standards" (Avolio et al., 1999; Bass et al., 1987; Bono & Judge, 2004, as cited in Guhr et al., 2019). "With IC, leaders establish a supportive climate and provide coaching and mentoring to help followers raise their personal abilities and potential" (Geijsel et al., 2003; Stewart, 2006, as cited in Guhr et al., 2019).

In the study conducted by Guhr et al. (2019), the results demonstrate that the transformational leadership style is best suited to achieve the desired behavioral intention of employees compared with transactional and passive/avoidant behaviors. Their findings show that transformational leaders are capable of positively influencing employees' behavioral intentions toward information security. They also state that transformational leaders can motivate employees to perform beyond expectations (Avolio & Bass, 2004, as cited in Guhr et al., 2019), thereby influencing employees' in-role and extra-role security behavioral intentions.

Another article that also brings up Transformational leadership is an article written by Cleveland & Cleveland (2018). The article mentions that Transformational leadership focuses on tasks that help understand what influences and motivates employees, how to coach employees to improve performance, how to help employee progress, and assesses value rather than numbers (Galloway, 2016, as cited in Cleveland and Cleveland, 2018). As cited by Cleveland & Cleveland (2018), "This seems to be an approach of 'transforming' the employee to 'value' organizational goals" (Cleveland & Cleveland, 2018).

2.2.3 Passive/avoidant leadership

Avolio & Bass (2004, as cited in Guhr et al., 2019) defines passive/avoidant leaders as more passive and "reactive", and they "tend to react only after problems have become a serious to take corrective action and may avoid making any decisions at all" (Avolio & Bass, 2004, as cited in Guhr et al., 2019). According to Guhr et al. (2019), passive/avoidant leadership consists of two leadership styles: management-by-exception (passive) and laissez-faire. As stated by Bass et al. (1987, as cited in Guhr et al., 2019), leaders tend to avoid corrective actions with the passive management-by-exception leadership style, and they wait until deviations and errors occur before taking actions (Stewart, 2006, as cited in Guhr et al., 2019). This way, they avoid ex-ante clarification of agreements and expectations to their followers (Sadeghi & Lope Pihie, 2012, as cited in Guhr et al., 2019). "With the laissez-faire style, leaders completely avoid influencing followers because they do not clarify goals, objectives, or expectations to followers or take any corrective actions" (Bass, Avolio, Jung, & Bergson, 2003, as cited in Guhr et al., 2019). This leadership style is often called

non-leadership (Guhr et al., 2019).

2.2.4 Servant leadership

Cleveland & Cleveland (2018) mention that one of the most distinct qualities of an inspirational leader is his or her passion for helping others and that this type of quality is associated with servant leadership. According to Cleveland & Cleveland (2018), leading is a form of guiding and supporting, being genuine, understanding, developing relationships, and building a community. Albright (2016, as cited in Cleveland and Cleveland, 2018) describes servant leadership as leaders investing in their employees, and they break down servant leadership into four key values: inspiration, equality, community incorporation, and guidance.

> "By investing in employees, servant leaders encourage and support their employees to hone in on their successes, instead of the leader's success. In organizations, servant leaders would be effective in helping their employees adapt to change by learning how the employees process things, and together, work on ways to integrate better within the organization. The practice of servant leadership is often characterized by positive results, such as decreased employee turnover (a major inhibitor for company success), improved job satisfaction, and employee loyalty. Inspirational leaders who practice such qualities will ensure that their organizations create a safe place where employees remain committed to the mission of the organization and motivated to follow its vision." (Cleveland & Cleveland, 2018)

In conclusion, the role of the security manager, or more specifically, the Chief Information Security Officer (CISO), has evolved to become a critical component of an organization's information risk management strategy. The CISO's responsibilities now include developing and operationalizing the security strategy, monitoring and evaluating information security practices, ensuring compliance with regulations, and protecting intellectual property, among others. To succeed, CISOs need to possess technical expertise, communication skills, business knowledge, and interpersonal skills. Effective communication, especially with senior management and the board, is crucial for CISOs to secure support, influence employee behavior, and improve an organization's overall cybersecurity. Furthermore, previous studies show that various leadership styles can be used to impact employees and organizations and that the different leadership styles can have a significant positive influence on employees' ISP Compliance intention, among other things.

Chapter 3

Research approach

The research approach is critical to any study, providing a framework for investigating a research problem. This chapter outlines the research approach adopted for this master thesis, including the research design, data collection methods, sampling technique, and data analysis procedures, in addition to the literature review approach. The literature review is an essential part of this research approach because it provides a collection of previous studies on the selected topic, which gives an overview of what has been studied previously and what could then be studied further. Another essential part of this research approach is a qualitative interview study with semi-structured interviews. The purpose of this study was to find out how security managers in different organizations seek to motivate and influence employees' security behavior. In addition to this, looking at different leadership styles and seeing which approaches the various security managers adopt to motivate and influence. To find this out, the study addresses the following research question:

- How do security managers seek to motivate and influence employees' security behavior?

3.1 Literature review approach

The literature review approach comprehensively analyzes existing literature relevant to the research topic. I have evaluated and synthesized the relevant literature to identify gaps in knowledge and areas requiring further research. This approach allows me to gain a thorough understanding of the topic and the current state of research on the topic.

A systematic literature review is used to carry out this literature review. By carrying out such a systematic literature review, it provides a good overview of previous research, and for this study, the main topics are leadership, motivation, and cybersecurity.

3.1.1 Process of systematic literature review

A systematic literature review is critical to any master's thesis as it provides a comprehensive overview of the existing literature in a specific field. It involves a proper and structured approach to identify, analyze, and synthesize relevant research studies that address a particular research question or topic. This process enables researchers to evaluate the quality of existing research, identify gaps in knowledge, and develop a more subtle understanding of the research area. According to Xiao and Watson (2019), there are eight steps in the systematic literature review process, and these eight steps are:

1. **Formulate the problem** - In this step, I had to identify an appropriate research question that was not too broad. The research question has been changed several times during this process.

2. **Develop and validate the review protocol** - This step is part of planning the review and includes the purpose of the study, research questions, inclusion criteria, search strategies, quality assessment criteria and screening procedures, strategies for data extraction, synthesis, and reporting. It is essential to validate the review protocol carefully before execution (Xiao & Watson, 2019).

3. **Search the literature** - I used search engines and databases Scopus and AIS Electronic Library during the search process, and I used the three main search terms leadership, motivation, and cybersecurity when searching for literature. I also used synonyms to cover more literature. In this step, I only reviewed the title.

4. **Screen for inclusion** - After compiling a list of references, I screened each article by reviewing the abstract.

5. **Assess quality** - In this step, I read the full texts of the articles I had found in order to figure out which articles were relevant enough for my study. I also created a PRISMA Flow Diagram to visualize the article selection process.

6. **Extract data** - I used NVivo to code when extracting the data. In this process, I also placed the extracted data into different categories, making it clearer.

7. **Analyze and synthesize data** - In this step, I combined and evaluated the extracted data. I looked at similarities and differences and decided which findings were relevant and should be included in my study.

8. **Report findings** - In this last step, I reported the findings from my review. When writing the findings, I created different categories, just like I did in the coding, to make it easier for both the reader and myself to see what kind of literature was relevant to my study.

3.1.2 Literature criteria

A literature review is a critical analysis and evaluation of existing literature in a field of study. The purpose of a literature review is to identify gaps in the existing literature and provide a framework for my research. The criteria for selecting literature in this literature review are as follows:

- The articles must be written in English
- The literature I select should be current and up-to-date, so the articles should not be older than 5 years (2018 - 2023)
- The selected literature should be relevant to my research question. I should only select literature that is related to my research topic and contributes to my research objective
- The literature I select should be reliable and trustworthy. I should only select literature that is published in reputable academic journals or books by reputable authors in my field of study
- The articles must contain the keywords related to the topic and research question

By following these criteria, I can ensure that the literature I select for my literature review is relevant, current, reliable, diverse, and comprehensive. This will provide a solid foundation for my research and help me to identify the gaps in the existing literature that my research can fill.

3.1.3 Searching for literature

When conducting the review, you start off by searching for literature. First, you have to decide where to search for literature. According to Xiao and Watson (2019), there are three major sources to find literature: electronic databases, backward searching, and forward searching. I used search engines and databases Scopus and AIS Electronic Library during the search process. Furthermore, I used the main three search terms leadership, motivation, and cybersecurity when searching for literature. Still, I also used synonyms in the search string that you can find in table 3.1. I also used Boolean operators like "AND" and "OR" to specify the search string. My main focus was to find literature about leadership, but also about motivation and cybersecurity. When searching for all three keywords, the results were not that relevant to my study. Therefore, I decided to search for leadership and motivation or leadership and cybersecurity, and the search string ended up looking something like this: (leadership OR CISO) AND (motivation OR encouragement) OR (leadership OR CISO) AND (cybersecurity OR "cyber security" OR "information security"). The search was also sorted by relevance.

Keyword	**Synonym**
Leadership	- CISO
Motivation	- Encouragement
Cybersecurity	- Cyber security - Information security

Table 3.1: Keywords used in the search string

3.1.4 Screening process

After searching for literature in both Scopus and AIS Electronic Library with the selected criteria, the search came back with 191 results in Scopus and 22 results in AIS Electronic Library, therefore 213 results in total. Then the duplicates from the search were removed, leaving a total of 205 articles. Here begins the screening process to exclude articles irrelevant to the topic and research question. As shown in figure **??**, there is a method to reduce the number of articles or "narrow down the body of work". This method includes first reviewing the article's title to see if it is relevant to the topic and research question. Secondly, the abstract of the article should be reviewed. And finally, the full text should be reviewed to determine which articles are relevant to the study and which are not.

After reviewing 205 results, I was left with 20 articles after screening both the title and abstract. The next step in the screening process was to go through and read all of the 20 articles and see which ones were relevant to this study. During this process, I used NVivo to read through and code parts of the articles that were relevant. After this process, I was left with 10 relevant articles for my study. I created a PRISMA Flow Diagram to visualize this process, as shown in figure 3.1. After this process, I later found another relevant article for my study, leaving me with 11 articles in total.

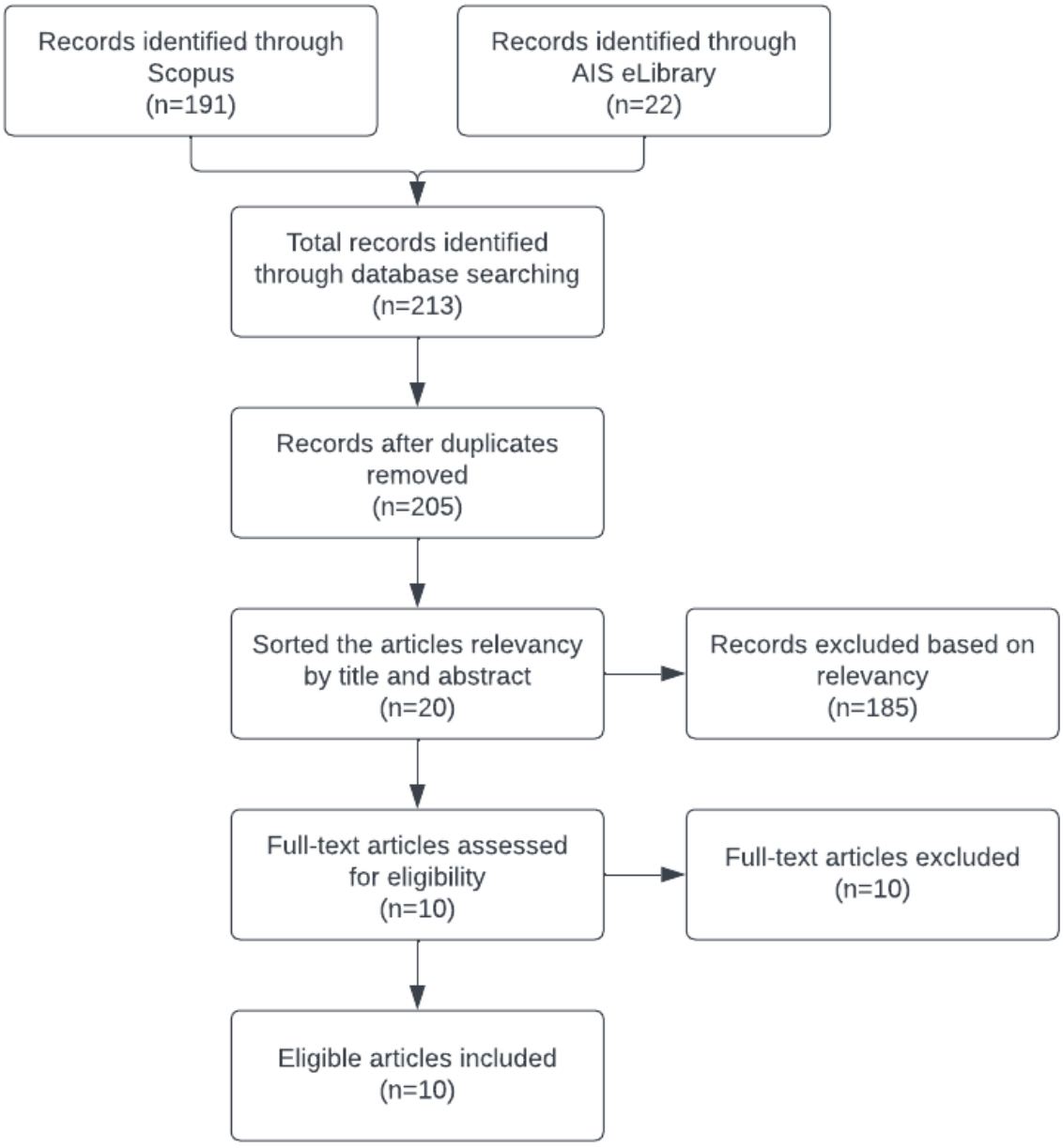

Figure 3.1: PRISMA Flow Diagram

Selected articles

The 11 selected articles from the screening process are in table 3.2 below with the title, author(s), and year.

Title	Author(s)	Year
Soft Skills of The Chief Information Security Officer	Jeroen M.J. van Yperen Hagedoorn, Richard Smit & Patric Versteeg and Pascal Ravesteyn	2021
Defining the Strategic Role of the Chief Information Security Officer	Sean Maynard, Mazino Onibere & Atif Ahmad	2018
Competencies of Cybersecurity Leaders: A Review and Research Agenda	Ashley Baines Anderson, Atif Ahmad & Shanton Chang	2022
The Role of the Chief Information Security Officer (CISO) in Organizations	Pedro Monzelo & Sérgio Nunes	2019
How Paternalistic Leaders Motivate Employees' Information Security Policy Compliance? Building Climate or Applying Sanctions	Zhu Jiawen, Gengzhong Feng & Huigang Liang	2019
Toward Cybersecurity Leadership Framework	Simon Cleveland & Marisa Cleveland	2018
How Paternalistic Leadership Influences IT Security Policy Compliance: The Mediating Role of the Social Bond	Gengzhong Feng et al.	2019
The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory	Nadine Guhr, Benedikt Lebek & Michael H. Breitner	2019

Establishing information security policy compliance culture in organizations	Eric Amankwa, Marianne Loock & Elmarie Kritzinger	2018
The role of employees' information security awareness on the intention to resist social engineering	Tanja Grassegger & Dietmar Nedbal	2021
The CISO Role: a Mediator between Cybersecurity and Top Management	Sveen et al.	2023

Table 3.2: Reviewed articles

3.2 Qualitative approach

This section consists of the research method used in this study, what data was collected and how it was collected, the data analysis, and ethical considerations.

3.2.1 Research method

This study could be conducted in both a qualitative and a quantitative way, but to get an answer to what I want on a deeper level, a qualitative method is best suited. According to Myers (2022), "The motivation for doing qualitative research, as opposed to quantitative research, comes from the observation that, if there is one thing which distinguishes humans from the natural world, it is our ability to talk". When you choose a qualitative research method, you can research the area on a deeper level. In this way, you can actually have a conversation and discussion with the person you are talking to, and you can get a better and broader understanding of the topic you are researching. As a research method, I chose a qualitative interview study with semi-structured interviews.

3.2.2 Data collection

> "Interviews, as a way to construct knowledge, are typically between the researcher(s) and key informants, subjects whose positions in a research setting give them specialist knowledge about other people, processes, events, or phenomena that are relevant to the research and more extensive, detailed, or privileged than that ordinary people might have." (Recker, 2021, p. 117)

Interviews can be structured with pre-planned questions or unstructured without any pre-conceived protocol or sequence. Interviews can also be semi-structured, "where respondents are asked about the topics of the study following a flexible interview structure (a protocol) that allows new questions to be brought up during the interview in response to what the interviewee says" (Recker, 2021, p. 118). I created an interview guide, which can be found in Appendix A, consisting of various questions divided into four different categories, but the interviews followed a conversational form that allowed for follow-up questions and bidirectional discussions about the topic or other topics that emerged during the interview (Recker, 2021, p. 118). When I went through this process, I took inspiration from and followed the qualitative semi-structured interview guide framework developed by Kallio et al. (2016), which you can see in figure 3.2 below.

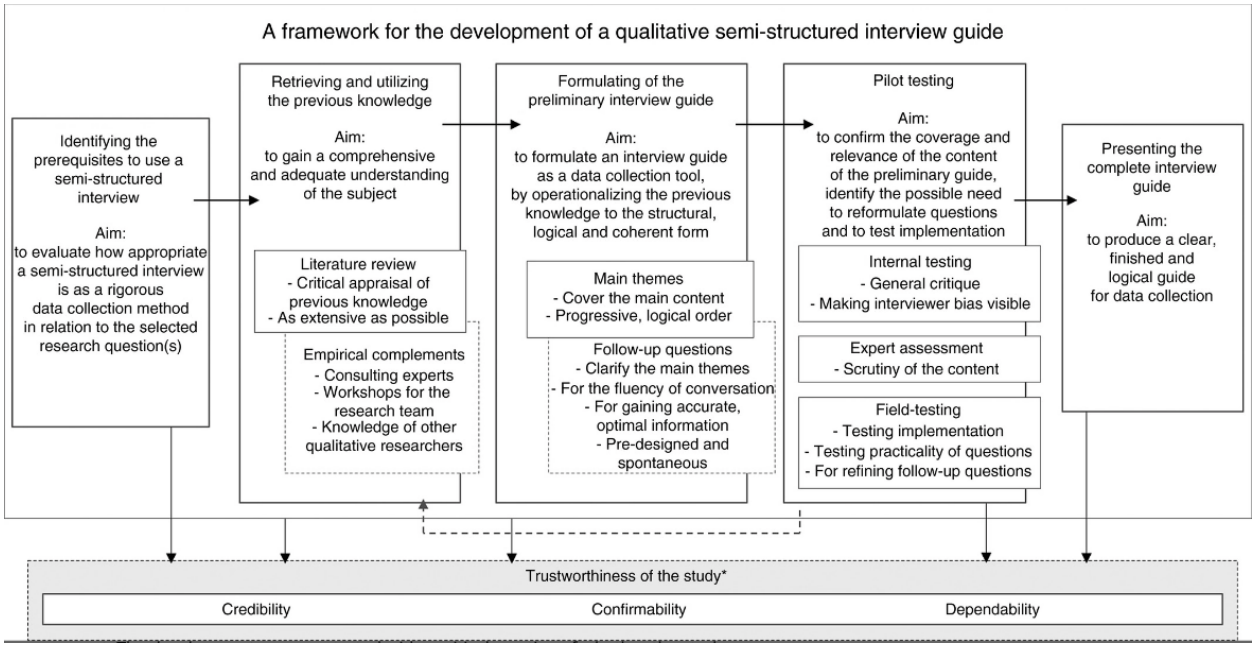

Figure 3.2: Qualitative semi-structured interview guide framework (Kallio et al., 2016)

The first step in this framework is Identifying the prerequisites for using a semi-structured interview. In this step, I had to weigh the pros and cons of choosing a semi-structured rather than, e.g., a structured interview. I thought that a semi-structured interview would give room for follow-up questions or discussions about the topic, which could give me more complementary content. The second step in this framework is Retrieving and utilizing the previous knowledge, which includes the literature review. What I did in this step is described in the literature review approach section. The third step in this framework is Formulating of the preliminary interview guide. Here I divided the interview guide into four different categories with questions regarding the topic of the category. The fourth step in this framework is Pilot testing. In the autumn of 2022, I conducted an interview with a security manager but chose not to use the data from this interview in this study. This interview can thus be seen as pilot testing, as it gave me a starting point and something to work on with regard to the interview guide. The last step in this framework is Presenting the complete interview

guide. I produced and presented a clear, finished, and logical guide for data collection, which can be found in Appendix A.

Most of the interviews were conducted digitally via Teams, with the exception of one interview, which was conducted in person with a recorder. The interviews varied slightly and lasted between 30 and 70 minutes, with an average of around 45 minutes. After the interviews had been completed, they had to be transcribed. For the interviews I conducted via Teams, I used the automatic transcription found in the app when recording and later went through the transcription to correct any errors. For the interview in person, I used Nettskjema, a web-based survey tool developed by the University of Oslo that allows you to create, save and manage surveys and data collection (Nettskjema, 2023). With Nettskjema, I could download a Dictaphone app and later upload this to the website with security measures to ensure data accuracy and privacy. When transcribing this interview, I used Microsoft Word's transcribe feature that converts speech to a text transcript. This way, I could easily upload an audio file and get Word to transcribe it for me. In addition to this, I went through the entire text afterward and corrected where there were any errors, as I did with the other interviews as well.

Subject selection

When choosing candidates for interviews, I wanted to find people who had a lot of experience with cybersecurity but also with leadership. In this way, there was a greater probability of getting good answers to the questions in the interview guide and thus being able to answer the research question in the end. I also wanted to gain insight into leadership roles from both large and small organizations, with both female and male candidates.

I chose to use LinkedIn to find and contact potential candidates; in this way, I had the opportunity to see how experienced they were before possibly contacting them. I tried to look for candidates with a lot of cybersecurity and leadership experience. When I started to contact people, I knew there was a possibility that not everyone would answer or have the opportunity to attend an interview. I, therefore, contacted more people than I had intended to interview to ensure a good number of candidates.

I ended up with a total of eight candidates that I interviewed, which can be found in table 3.3. Most of the selected candidates are located in Norway, but two of them are located elsewhere in Europe. This gave me an opportunity to see how security managers operate in different places in the world, and not just in Norway. The candidates consist of both men and women with varying ages and experience. Table 3.3 shows their current role in the organization, a pseudonym to anonymize the candidate, and the number of total years in a leadership role. The candidates come from both the public and private sectors and from industries within finance, communications and information technology, and media, to mention some.

Pseudonym	**Current role**	**Total years in leadership role**
CISO_1	Chief Information Security Officer (CISO)	12 years
Section_manager	Section Manager IT Security	7 years
CISO_2	Chief Information Security Officer (CISO)	4 years
Risk_director	Risk Management Director	4 years
CISO_3	Chief Information Security Officer (CISO)	24 years
CISO_4	Chief Information Security Officer (CISO)	20 years
Security_director	Security Director	13 years
Service_security	Head of Service Security	10 years

Table 3.3: Subject selection

3.2.3 Data analysis

After collecting the data, it has to be analyzed. This process involves getting an overview of the data that has been collected and then reducing it by selecting the most important findings. There are several techniques for analyzing the data, but probably the most commonly employed, useful set of techniques for analyzing and reducing qualitative data to meaningful information is coding (Recker, 2021).

> "Coding organizes raw data into conceptual categories, where each code is effectively a category or "bin" into which a piece of data is placed. Coding involves assigning tags or labels as units of meaning to pieces or chunks of data–, whether words, phrases, paragraphs, or entire documents. Coding is often used to organize data around concepts, key ideas, or themes that we identify in the data or to map theoretical expectations to a set of data with the view to corroborating or falsifying the theory." (Recker, 2021)

I used NVivo to code the transcribed documents, which is an analysis tool/computer program used in qualitative research (UiO, 2023). The questions from the interview guide, Appendix A, were already divided into four categories, including general questions about the candidate and the organization in part 1, security culture in part 2, motivation and leadership in part 3, and security policies in part 4. Furthermore, I created subcategories within these main categories. In this way, I got a better overview of the findings and was also able to collect the findings from each interview under the same categories. This made it easier to be able

to compare answers from the various candidates and look at similarities and differences. Before I could present the findings, I had to translate the interviews that were conducted in Norwegian, which applied to 6 out of 8 interviews, where I translated the parts that were to be included in the findings. The remaining two interviews were conducted in English.

Figure 3.3 below shows a model for qualitative data analysis consisting of three stages, which are data reduction, data display, and conclusion drawing/verifying.

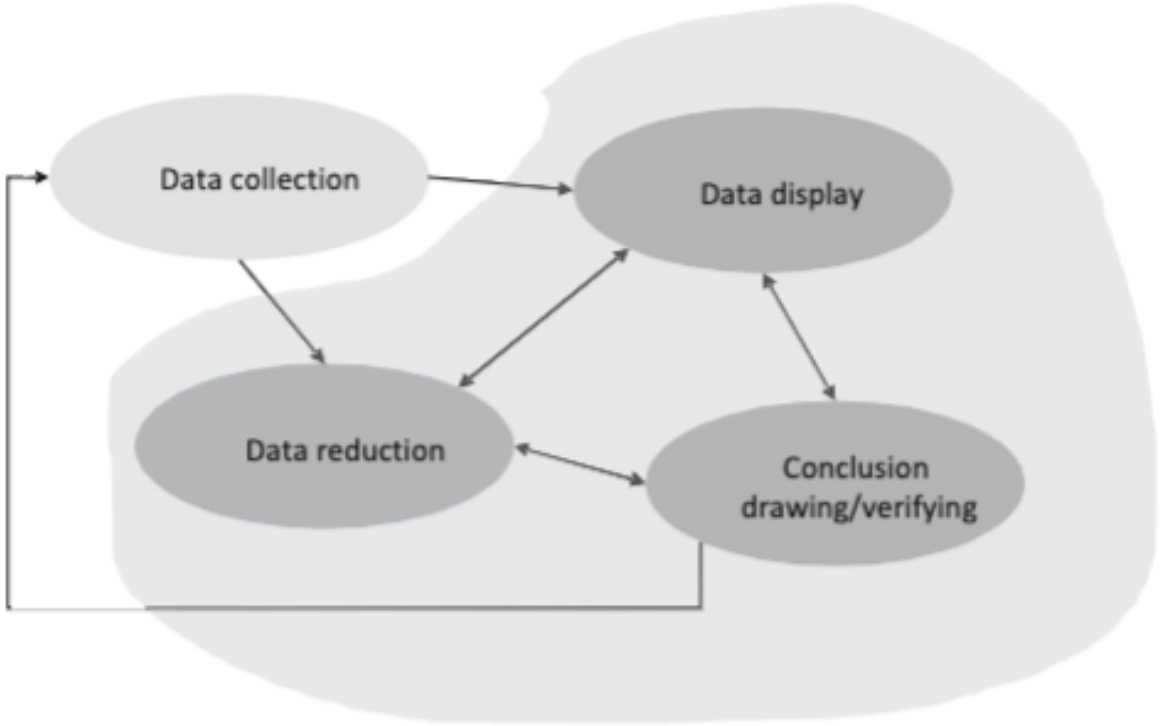

Figure 3.3: Qualitative data analysis (Miles & Huberman, 1994)

- **Data reduction** - As mentioned, I used NVivo to analyze and code the transcribed interviews by dividing the data into different categories and subcategories. In this process, there was also a lot of data that was not relevant and thus "discarded".
- **Data display** - The main findings were displayed in both text in the findings chapter and in a table in the discussion chapter. These findings are most interesting and relevant in relation to the topic and the research question.
- **Conclusion drawing/verifying** - When drawing a conclusion, I looked at all the interviews and looked for both similarities and differences in order to form a comprehensive picture of the data I have collected and written about.

In this chapter, I have discussed two commonly used research approaches: literature review and qualitative. While each approach has both strengths and limitations, they can be combined to provide a more comprehensive understanding of the research topic.

3.2.4 Ethical consideration

When conducting a research project, thinking about principles, laws, and regulations is essential. The Norwegian National Research Ethics Committees is the foremost national resource on research ethics through guidance, statements, and decisions in all subject areas (The Norwegian National Research Ethics Committees, 2023). They have made a list of previously considered unnecessary data of general guidelines containing 14 points, which are: 1) Quest for truth, 2) Academic freedom, 3) Quality, 4) Voluntary informed consent, 5) Confidentiality, 6) Impartiality, 7) Integrity, 8) Good reference practice, 9) Collegiality, 10) Institutional responsibility, 11) Availability of results, 12) Social responsibility, 13) Global responsibility, and 14) Laws and regulations (The Norwegian National Research Ethics Committees, 2019).

Point 4, voluntary informed consent, was an important thing to consider in the research process. When collecting data from people, in this case through interviews, it is essential to get consent to collect information about the person and the organization, e.g., before starting the interview process. Each candidate who agreed to be interviewed had to sign a consent form prepared in collaboration with Sikt, which can be found in Appendix B. Sikt is the knowledge sector's service provider and develops, acquires, and delivers products and services for education and research. They offer the knowledge sector infrastructure, data, and joint services that provide good user experiences and meet the overarching goals of digitalization, data sharing, and open research (Sikt, 2023). This consent form states, among other things, that it is voluntary to participate and what rights the candidate has, e.g., the right to have information about the candidate deleted or changed. Point 5, confidentiality, is another thing to consider. The candidates must be anonymous, and revealing who is behind the various statements shouldn't be possible. Another relevant point to this process is point 11, the availability of results. When the thesis is completed, the candidates will receive the finished version and be able to read through the findings. They were also allowed to be sent the transcribed document after the interview to see if there was anything they wanted to remove or change.

Chapter 4

Findings

This chapter presents the findings from this study. The aim of this study was to find out how security managers motivate and influence employees' security behavior. To find this out, I looked at the various approaches security managers adopt and also looked at how leadership styles influence the approaches they use to motivate. The research question guiding this study is: "How do security managers seek to motivate and influence employees' security behavior?"

4.1 Leadership styles

The findings show great diversity in leadership styles, which makes it interesting to look at and compare the different approaches adopted by different leadership styles. The findings show seven different leadership styles, including 1) Transformational leadership, 2) Transactional leadership, 3) Benevolent leadership, 4) Servant leadership, 5) Intention-based leadership, 6) Situational leadership, and 7) Others (this one didn't really fit into any other leadership style category).

CISO_1 uses the "Baywatch method", which involves throwing people into deep water and then rescuing them when they are about to drown.

> "[...], I believe in giving people much freedom, but I am always there to help, support, and make decisions if needed. I think it's important to give people concrete tasks that may be a little bigger than what they feel comfortable with, so they have something to strive for and to know that they always have a leader who can help and support them with advice and guidance, and step in if needed."

This statement describes a leader who wants to give the employees some freedom and let them try big tasks on their own before they possibly ask for help. This gives the employees

opportunity to grow over time.

Section_manager describes their leadership style as:

> "My leadership style is fundamentally based on trust in the employees. [...]. I am very concerned that employees get challenges and development opportunities, which are perhaps some of the most important, and then I am concerned with trust and flexibility. [...], but then you know that if you have to work through a whole weekend because there has been an incident, the employees will be there to help, so flexibility and trust go both ways."

Section_manager has a leadership style that is based on trust. Trust in the employees and also allow them to try different challenges and develop accordingly.

CISO_2 uses intentional-based leadership, which is described as:

> "I communicate clearly what goals we have for the business, but then I give the responsibility or the freedom to the business to respond to that goal with their own tools, creativity, or framework."

Further, *CISO_2* describes a principle that they use in their organization which is called 'tight-loose-tight'.

> "In the first phase [tight], we establish the requirements and framework, meaning what needs to be done to be compliant with laws and regulations. Once these are set, we enter a loose period where it's up to those who are subject to these requirements to come up with their own solutions. Whether it's using a certain tool or Excel sheets, it's completely up to them. They have full freedom to decide how to implement the requirements. Finally, in the last phase [tight], we conduct checks to ensure that the requirements set in the first phase are being followed."

Risk_director describes their leadership style in several different ways. First, they describe themselves as a lazy leader, but then they describe their leadership style as situational leadership. They also describe their leadership style as something comparable to servant leadership.

> "Responsibility to show a good example. [...]. So my style, I would say I'm. Ah, I like to put people first, like let them succeed when they need to develop [...]. [...]. It's very core in my thinking. And it is called situational leadership, and it practically means that you acknowledge that [...] the employees, [...] don't

> understand what it is you need to understand [...], and you need to go there and understand their situation and then. Move your style of communication. Move your, you know, presentation, your target on their level and let them develop, you know, from that situation to new gurus."

Risk_director adapts their leadership style and communication depending on the situation and the people around them. *Risk_director*'s leadership style can be compared to servant leadership because they like to put people first and let them succeed.

CISO_3 describes their leadership style as something that can be compared to Benevolent leadership.

> "I'm very focused on making sure my employees thrive in normal times. In a stressful situation where we handle complex security incidents, my leadership style is probably not very democratic."

CISO_4 is keen to be accommodating/approachable.

> "[...] You need to be approachable, visible, and present where things are happening. It shouldn't be a group of scary security people sitting in the corner. This is incredibly important, and it's reflected in my leadership style as well."

CISO_4 believes that the employees shouldn't be afraid to approach the manager/leader, so it's very important to be accommodating.

Security_director uses a soft approach to the employees and takes time to get to know the people.

> "I like to sit down and get to know people to meet them on their terms. This is more a reflection of who I am as a person, but it also reflects how I work in that I try to see how this person, with whom I need to work well, is. To be a little bit on their side and get to know what works and what doesn't work in order to let them play well in their own way."

Service_security describes the security manager role as a combination of technical expertise and people management, understanding people, and dealing with people in different situations.

> "[...] It requires having a good enough technology understanding. So. So the person needs to understand the security, cybersecurity topics, the recent ones and

> upcoming ones. But it's very much about people management, and so that's why understanding people and dealing with people in different situations. [...]. So I think that the manager does need to have a strong technical background to understand the topics of what's happening but also has to have a kind of calm approach to manage the stressful situations because things will pop up [...]."

With this statement, *Service_security* doesn't really describe their own leadership style but gives an example of how the security manager role should be, which is a combination of technical expertise and people management. I would then like to believe that *Service_security* relates this to their own leadership style.

4.2 Motivation

When I conducted the interviews, I asked the candidates about the approach they use to motivate their employees in cybersecurity. I also wanted to know which approach they feel does not work as well and what they would do in the future that they are not already doing.

4.2.1 The need for motivation

I asked the candidates whether they feel that the employees actually need to be motivated and to what extent, to which all answered that the employees need to be motivated.

CISO_1 describes the need for motivation as:

> "They need to be motivated. Yes, they largely need to be motivated. They need reminders on this. Otherwise, I think it's difficult. Yes, we need it. There aren't many in the company with a security background, so I think everyone needs to be motivated on security."

Section_manager states that:

> "They need to be motivated all the time because motivation tends to come in waves, right? If you don't talk about it or remind them, it will fade away. So, there are some things that you need to keep doing all the time, and they also get motivated by updating them with new information regarding the threat landscape, new attack methods, and vulnerabilities, and emphasizing the importance of control. It's also important to praise those who deliver good IT security."

Something that is repeated here by both *CISO_1* and *Section_manager* is the need to remind the employees why security is important.

CISO_2 describes the need for motivation as:

> "Everyone needs to be motivated, including myself, so it's important. It's just a matter of setting up a plan for how to do it. So in large part, everyone needs to be motivated, from the director down to those on the ground. [...]. It's part of the ISMS to ensure a security culture, so if it's not me doing it, I must at least ensure that there is something around it, whether it's mini-courses or campaigns or hiring consultants to hold motivation sessions, and so on."

This statement shows how *CISO_2* feels responsible for motivating the employees, and if it's not them doing it, they need to ensure that it's covered somehow.

Risk_director puts it this way:

> "Well, it depends on your role in security. Umm. When you are not a security person. So you need to be motivated. [...]. So how to get commitment? Engage people who think it's like electricity or water. You know it's always there. It's not my job. Even though they understand that everybody has a role and everybody says, like weak points or I need to. But the rest it's challenging."

CISO_3 states that:

> "They need to be motivated. Everyone needs motivation to do a good job. Of course, you do. Yes, and it is largely because if there was no desire, what should I say? If the motivation were not there, then they would not do a good job, and then they would probably try something else, I think."

Moving on, *CISO_4* states that:

> "I feel that they need to be highly motivated. Of course, there are IT principles, such as zero-trust principles and such, that you can give up on the employees, they will always make mistakes no matter what, and I think that's a little true, but you can also avoid a lot around it, and we as a supplier. We also need good ambassadors who go out to our customers and speak and answer the right questions if they are asked. Right, we can't just rely on technology because we also have a very high trust relationship, and some people may think it's a bit naive that people are allowed to install software on their own responsibility and things like that. You can't stop people from doing all sorts of things, [...]."

Security_ director describes the need for motivation as:

> "How to motivate them? Well, I wouldn't say it's very demanding. No, what I enjoy is writing. I like to post things, and it's fun if I get a thumbs-up. Then it's good, but it can be difficult to measure the response. I think we are at a good level now, but it's important to keep it fresh and changing so that people don't get bored with it. It's an art. [...]. Yes, it's often challenging because you can overwhelm people to the point where it becomes a negative experience, and that's not the intention."

This statement says it can be challenging to balance the frequency and how the message is delivered so it doesn't become a negative, overwhelming experience for the employees. Like *Security_ director* said: "It's an art."

Service_ security states that:

> "I think that everybody in the organization has to be motivated, and as I said, it can't be just. Start that. As some kind of set of rules outside of their daily task, it has to be something that is naturally incorporated into their daily book, and they don't necessarily need to even think about it. They are working according to security because the processes have to be adapted and adjusted in such a way that it's not an extra step they need to do. To ensure security is considered. [...]. Everyone has to be motivated."

In summary, all the interviewees from various organizations agree that the employees need to be motivated, some to a greater extent than others.

4.2.2 Approaches to motivation

CISO_ 1 mentioned multiple ways to motivate the employees. Among other things, *CISO_ 1* believes that it is important to use current things in the media and to use events that have happened. Another thing that *CISO_ 1* mentioned is to give small reminders more often rather than having big e-learning courses all the time. The third thing the interviewee mentioned is having small notes, such as post-it notes, hanging around the organization with security messages. The last thing that was mentioned is to ensure that good guides and advice are available for the employees to access.

> "It is about using current events in the media, in the news, and using incidents that have happened and, yeah, maybe many small reminders rather than big e-learning things. [...]. We have many of those little notes that hang around on the

> mirror on the toilet and hang on glass surfaces, so there is a little note that says, "Did you forget to lock your computer?" and so on. "Remember that personal information is important," so there are many small notes like "Don't click on that link", which I hang around on the mirrors in the bathroom and such. So those small things, and then there is an email address underneath, reminding people to report if something happens. [...]. [...] and then we use the channels we have to ensure that we have good guides, good advice, and such available for people and that they are reminded of where to find this."

This statement shows that there are multiple ways of motivating employees about security. The part about using post-it notes around the organization to remind the employees about security seems to be a very unique and creative way to motivate.

Section_manager believes that awareness and understanding why, e.g., cybercriminals do what they do is the key point in motivating employees.

> "It's more like showing. What? What is perhaps important for them to understand is the rationale behind it. Whether it's a state or cybercriminals doing it, you must explain why it's happening. I have to delve a bit into why China, Russia, and other countries are doing a lot of this. And it's not just for sabotage, but it can also be for intelligence and industrial espionage. And then, we have cybercriminals and explain what motivates them. [...]. To be motivated on a regular basis, it's about having the capacity to assist them with good advice."

CISO_2 uses the mirroring methodology as an approach to motivate the employees.

> "I always try to mirror the position I am speaking to. So if I am speaking to the director of the organization, I speak in a way that he or she understands, for example, using legal compliance as a reference. Because they are often very focused on compliance with laws and regulations, and when they say, "we need this requirement because this law requires it of you", it is your responsibility as a director to ensure that it is taken care of. [...] It's kind of that mirroring methodology."

CISO_2 also mentions that articles are regularly published on various topics that strengthen both the insight and motivation of the employees around security.

> "We also have regular articles that we publish once a month that deal with some topics that we consider important. They also strengthen the employees' understanding and motivation around security, and we try to make it a bit interesting for them as well."

Both *Risk_director* and *CISO_4* mention rewarding as a way to motivate. *Risk_director* mentioned this:

> "So you need to incentivize the goal, you know, if you say that we need to have a, you know, let's say better security awareness in the company, somehow you need to find a way to reward the participant. And I'm not talking about money. I'm simply saying that people need to feel good. They need to be recognized, and somehow you need to figure out what it is."

Further, *Risk_director* mentioned that they introduced a Business Continuity Maturity Model (BCMM) to measure the IT services during the year, and by the end of the year, the employees or the team that had the highest score got a reward. Another thing *Risk_director* use is peer pressure.

> "Some of the teams got it, and they say, 'OK, this is fair. The guidelines are clear and it's repeatable, it's comparable, it's fair criteria, it's doable. There's lots of flexibility in how you do it, [...]. Suddenly you see your services on the, you know, the yellow-red line. And then that's clearly services that are like light green or a dark green like at the top. And they started to kind of 'OK, we can't be worse than the others'. [...] Uh, but some form of incentive reward is a very important part of it. Yeah, I think that's really a, you know, the core. It can't be empty."

As mentioned, *CISO_4* also uses rewarding as a way to motivate.

> "[...] We have rewards for those who report incidents, which can range from reporting a silly phishing email to more serious incidents. This also gives us a good opportunity to show the range of incidents that have been reported in meetings. I have a slide that shows the top 5 recipients of rewards, which shows the range of incidents from serious coding errors to completely idiotic phishing emails that everyone should know not to click on. [...] This has proven to be very effective."

CISO_3 believes in motivating the employees by giving them exciting tasks, always supporting and being there for them, and also speaking a language that they understand.

> "It's about the message you convey often being difficult, so you have to rewrite it into, let's call it, a leadership language. Mm. Yes, it's about being prepared, simply put, and it's about taking up space in a friendly and kind way. Strong but clear. [...]. And I always support them, I mean that. It's about creating time for them, you know. [...]. Through some clear expectations that I have

> communicated to people, I think it's easy to motivate them with exciting tasks, and we definitely have those. Even though risk analysis can be boring in the long run, it's important to provide them with motivating risk analyses that resonate with them at the time."

Security_ director mentioned awareness courses and phishing tests as ways to motivate employees.

> "But the motivation aspect of it is what we have talked about. Letting them be motivated to see and understand it all and do their part of the security focus, and with that, use their private sphere a bit. I think that's a good thing, and let them understand that there is no distinction between work and private life, actually, on the mobile phone you have received from the employer. It can affect both your photos and the employer's salary systems."

Further, *Security_ director* also states that:

> "And many wake up on a Saturday morning to an email that turns out to be a course. And it's like, we're getting closer to something. We've discussed this internally. Is it good or not? Should we only send these spam or phishing attempts as courses from Monday at 8:00 am to Friday at 4:00 pm, right? No, maybe not. We may end up with a no because that's not how it is out there."

This statement says something about *Security_ director* and their organization constantly testing the employees with different phishing tests, whether it is during working hours or evenings/during the weekend. This is something that can go both ways. It can either help to strengthen security awareness among the employees or become something that is seen as negative and overwhelming for the employees.

Service_ security mentioned multiple ways of motivating the employees. First, focus on the basics. Second, don't make it too advanced or too complicated. Third, it has to be relevant to the employee's own job, so it has to be directly applicable. Four, Gamifying, e.g., simulated phishing tests. Five, Understanding. The employees need to understand why something is not allowed or not recommended. And last, speak "the right language", e.g., speak the business language to business people.

> "But what we have found out is that what's working, at least for some of the people, is that by gamifying. So one example is that we use some simulated phishing tests that you get an e-mail [...]. So report it using the tools that we have, and you will start collecting points by acting on those or recognizing those, [...].

> But they need to understand why something is not allowed and not recommended. [...]. So the business management needs to realize the business risks and the business impacts that might happen to their business if security is not followed as we suggest. [...]. So we need to speak the business language to business people. So that will motivate them actually to take security seriously."

Service_ security gives a long "list" of ways or approaches to motivate but doesn't mention which approach is most used or works best. But *Service_ security* mention something about gamifying working for at least some of the people.

4.2.3 Approaches that don't work

In addition to the approaches for motivation, I asked the candidates which approach they feel does not work as well and which they would not recommend using. All the interviewees except *Security_ director* mentioned an approach that they feel does not work.

Contrary to *Security_ director* and *Service_ security*, who believed that phishing tests were a good approach for motivation, *CISO_ 1* believes that this is not an approach that works as well. *CISO_ 1* states that:

> "So we have a deal to conduct free phishing tests, but I have chosen not to use it. I cannot say that it does not work, but I know that in many organizations, it is not well received that they are constantly tested with fake phishing emails, as it is very difficult to distinguish between a phishing email and a genuine one. Usually, when conducting such tests and sending out such emails, special measures must be taken to get them past the filters that are already in place."

This statement says something about *CISO_ 1* not wanting to track the employees and constantly testing them. *CISO_ 3* also mentioned something about not using phishing tests because they don't want to humiliate people.

Section_ manager also mentioned an approach that they think doesn't work if you want to motivate your employees. This is called the "Aunt Sophie's method", which is based on a fictional character from a well-known musical here in Norway. *Section_ manager* described this method as:

> "That's Aunt Sophie's method then. No, so, it's if you go around with your index finger and tell everyone what they are not allowed to do, and expose people who have done something wrong and stupid and such, that I think is very bad, so it's much better to take on this advisor role then."

Section_ manager describes that it is better to be an advisory, helpful manager to motivate and influence the employees than to shout and scold employees for things they may have done wrong. Here I think *Section_ manager* has a very good point, and there are also several candidates who think the same. Both *CISO_ 3* and *CISO_ 4* agree with *Section_ manager* on this. *CISO_ 3* said that:

> "Yes, punishment and scolding. It doesn't work at all."

CISO_ 4 stated that:

> "What doesn't work well? Well, it's things like threats. It's yelling at people, right? These are the kinds of things that have a very 1990s approach to security. It's now such an integrated part of what every business does that it's something that everyone has to take responsibility for, so you can't be a 'policeman' and yell and make a fuss."

CISO_ 2, on the other hand, mentioned security policies as a poor approach to motivating employees.

> "Yes, it's very ineffective to create a security policy that's 30 pages long and demand that everyone reads and understands it. It's completely impossible. [...]. So they fall asleep after page 3 and then ignore the rest."

Risk_ director mentioned an approach that they have never been a big fan of, and that's the control and fear factor approach.

> "Yeah, there's one approach I've never been, never been a big fan of, but. But I know that there are. In some situations, it's just. It is what it is, and that is the control and fear factor approach. So the fear factoring doesn't work you go until and you give a fear factor. Umm, no. You practically give nothing. If you go and give fear factor and you give a solution, how to get you somewhere. So it's always you need to come with you know some proposal. It's an important part of it."

So scaring employees into understanding and taking cybersecurity seriously is a bad way to motivate employees, according to *Risk_ director*.

Service_ security mentioned that penalties and reward is poor ways to motivate employees.

> "Yeah, the penalty and reward, some kind of rewards might be so. So if things, well, you notice that bug bounty programs that are used by some organizations

> that that anyone can report vulnerabilities that they've found in the products, and then they get some rewards or at least some nice words from the company that will get it done. So the reward is something that, yes, you can do, but I don't think it works that well inside the organization on the same course. Of course, there have to be penalties if something is not followed. So yes, those need to be in place, so there has to be some kind of actions taken if people are doing something that they shouldn't, so yes, those need to be in place, but they should be the primary drivers and primary motivation and mechanisms in the organization."

4.2.4 Future approaches

After the interviewees mentioned different approaches to motivate and approaches that don't work as well, I asked them if there was anything they could consider doing in the future to motivate the employees that they are not already doing. The reason why several of them are not using this approach today is mainly due to a lack of capacity to do so. Six out of eight interviewees made suggestions for future approaches.

CISO_1 mentioned that they wanted to create tailored e-learning courses.

> "Yes, I want to create, but it's a matter of capacity. I want to create some more tailored e-learning courses. [...]. But it takes time, though, but to create courses where we maybe base it on things that have happened internally and maybe have some people speaking about things they have received or things that have happened that they could. Yes, we made something that was very relevant."

Further, *CISO_1* mentioned something earlier about phishing tests and how they don't think it's a good idea because of the constant testing and tracking of employees.

> "[...], and I wonder if we will run a phishing test. Instead of storing the data, how could you see that this was not a phishing email if you link it to something else so that it becomes a training instead of just collecting data on who clicks and who doesn't? It may be something we should do. Otherwise, we do a lot of emergency drills, tests, and such, and we have expanded that with more people involved, running scenarios on events and things, which is very useful."

This statement suggests that *CISO_1* would prefer using phishing tests for training rather than collecting the data and tracking who has fallen for the trap and who hasn't.

Moving on, *CISO_2* also had a suggestion for future motivational factors, and this is something they were already in the process of doing.

> "Yes, something we are actually doing right now is to hire more advisors. And one advisor will have a main focus on this exact thing of security culture. So what we are looking at in the future is that this person will not only have a good plan that goes smoothly throughout the year but also go out to the locations we have. We are in 35 different places in Norway. And then be out with those who are actually affected by security. And talk about security and ensure that they understand, but also answer questions if there are things that are unclear about the different requirements we set."

So what *CISO_2* suggests is to have more advisors available who can talk about security and ensure that the employees understand the importance of it and answer questions about unclear things. In this way, the security message can reach more people.

CISO_3 suggested some exciting courses that include everyone in the organization, specifically gamification, as a future possible way of motivating.

> "No, it has to be. I mean, I think we need some new, exciting courses that include everyone, so within the courses, we've heard that gamification is supposed to be the big thing going forward and that it should be cool and fun to take cyber courses. That could be a great motivation to get people to complete them, but it needs to go beyond some kind of plan. All of the vendors around us are really focused on this idea that, yeah, we have these cool gamification courses, but it's not really that cool when it all comes down to it. Something completely new within the realm of cyber training, instead of boring e-learning courses, would be cool."

With this statement, *CISO_3* suggests that gamification could be a great way to motivate employees and make it cool and fun to take cyber courses. This could probably create more employee commitment, so I think it's a good suggestion.

CISO_4 mentioned phishing tests as something they would like to do in the future. They haven't done this before because they haven't had the capacity to do so.

> "We haven't done much of it yet. We haven't had the capacity for it. So we haven't done it very much yet, but it's on the agenda. But then people also need a chance to be up to speed on it, right? So they need training in detecting a phishing email, what to do with it, and so on. "

Service_security mentioned that there is always room for improvement, and the area in their organization that can still be further improved is usability. *Service_security* describes this as:

"I feel that there's always room for improvements, and I feel that the area that can be still further improved is the usability, so even further make the security transparent to the user so we do have this multi-factor authentication are we do have this and that in place that people have to do to log in. OK, we might use some biometric authentications to make it easier, but it's still. In many cases, it's an extra step that the user has to do to continue and to actually complete the process or actions that they want to do. So that's one area that I think still can and should be improved is that they make it even more transparent to the end users. The whole security discussion."

Chapter 5

Discussion

The purpose of this study was to find out how security managers in various organizations seek to motivate and influence employees' security behavior. To find an answer to this, I wanted to take a closer look at different leadership styles in combination with the security managers' approaches to motivation. The research question guiding this study is: "How do security managers seek to motivate and influence employees' security behavior?". This chapter contains a discussion of the previous literature from Chapter 2 and the main findings from my study in Chapter 4.

5.1 The various leadership styles

Previous studies presented a number of different leadership styles in the field of cybersecurity. Several of these studies investigated how leaders with different leadership styles motivate employees' information security policy (ISP) compliance. My study also showed several different types of leadership styles, which I will discuss in more detail in this chapter.

When I conducted the various interviews, I asked the candidates to describe their own leadership style. Several of them described their own leadership style without necessarily pointing to a concrete one, while others described their own leadership style and could also point to a concrete leadership style. As for the candidates who only described their own leadership style and did not point to a known and concrete leadership style, I had to try to place them in a known leadership style category. Here I based the leadership styles from previous studies that are described in Chapter 2.

When I carried out the literature review, I found five different leadership styles in the cybersecurity field. These were Paternalistic leadership, Transactional leadership, Transformational leadership, Passive/avoidant leadership, and Servant leadership. When I looked over the various findings from my study, I could see several characteristics between the leadership styles that the candidates described and the leadership styles from previous studies, which

made it easier for me to place them into different leadership style categories.

As stated in Chapter 2, Guhr et al. (Avolio & Bass, 2004; Bass, 1985, as cited in Guhr et al., 2019) define transformational leadership as a style of leadership that transforms associates to rise above their self-interest by altering their ideals, morale, value, and interests, motivating them to perform better than initially expected. Here I can see characteristics between this type of leadership style and the leadership style that was described by *CISO_1* and *Section_manager*. *CISO_1* believes in giving employees much freedom and also giving them concrete tasks that may be a little bit bigger than they are comfortable with. This way, they have something to strive for, which can eventually help them to grow over time. This can "motivate them to perform better than initially expected", as described in the Transformational leadership style above. I also placed *Section_manager* in this leadership style category based on their description of their leadership style. *Section_manager* described their leadership style as fundamentally based on trust in the employees, and they were also very concerned that employees get challenges and development opportunities.

Further, I saw some similarities between *CISO_4*'s description of leadership style and Transactional leadership. *CISO_4* mentioned rewarding as an approach to motivating employees, which is also mentioned in Transactional leadership. As stated in Chapter 2, Guhr et al. (Avolio & Bass, 2004, as cited in Guhr et al., 2019) state that transactional leadership is mainly composed of 2 dimensions of behavior: contingent reward and active management-by-exception. They also define transactional leaders as leaders who display behaviors associated with constructive and corrective transactions, for example, clarifying what the employee should do in order to be rewarded, as well as monitoring performance, and taking action when problems occur. *CISO_4* believes in rewarding as a way to motivate, and they describe that they have rewards for those who report incidents, which can range from phishing emails to more serious incidents. *CISO_4* states that this has proven to be very effective in their organization.

When I looked at the description of *CISO_3*'s leadership style, I saw similarities and characteristics with both Benevolent leadership (dimension under Paternalistic leadership) and Servant leadership. But, after looking more closely at the literature about both Benevolent leadership and Servant leadership, I choose to place *CISO_3* into the Benevolent leadership style category. *CISO_3* is very focused on making their employees thrive and avoid embarrassing their employees. *CISO_3* mentioned that they don't like to use phishing tests because they don't want to humiliate their employees. This can be compared to the literature about Benevolent leadership because, according to Zhang et al. (2015, as cited in Jiawen et al., 2019), benevolent leaders are sensitive to employees' needs and avoid putting their employees in embarrassment or dilemma. Also, according to Cheng et al. (2004, as cited in Jiawen et al., 2019), benevolent leaders show great concern for the well-being of their subordinates and are willing to make an effort to secure their best interests.

Security_director uses a soft approach to the employees and takes time to get to know the

people. The leadership style that I feel best fits this description is Servant leadership. According to Cleveland and Cleveland (2018), leading is a form of guiding and supporting, being genuine, understanding, developing relationships, and building community. Especially the part about developing relationships fits the description of the *Security_ director*'s leadership style. Also, Albright (2016, as cited in Cleveland and Cleveland, 2018) describes Servant leadership as leaders investing in their employees. "In organizations, servant leaders would be effective in helping their employees adapt to change by learning how the employees process things, and together, work on ways to integrate better within the organization." (Cleveland & Cleveland, 2018)

Two of the remaining candidates described and named their own leadership styles, and the third remaining candidate was difficult to put into a leadership style category. First, I want to address *CISO_ 2*, which uses intentional-based leadership. Intentional-based leadership is described by *CISO_ 2* as: "I communicate clearly what goals we have for the business, but then I give the responsibility or the freedom to the business to respond to that goal with their own tools, creativity, or framework."

Further, *Risk_ director* described their leadership style in three ways. First, they described themselves as somewhat a lazy leader, but then they described their leadership style as Situational leadership. The description of their leadership style can also be compared to servant leadership, but to simplify it, I choose to place *Risk_ director* into just one leadership style category; Situational leadership. With this leadership style, *Risk_ director* adapts their leadership style and communication depending on the situation and the people around them.

Finally, we have *Service_ security*. It was a bit difficult to place *Service_ security* into a leadership style category because they didn't really give a description of their own leadership style. Instead, they describe the role of the security manager in a more general way. This description includes the security manager role as a combination of technical expertise and people management, understanding people, and dealing with people in different situations. I would like to believe that *Service_ security* relates this to their own leadership style, but I still find it difficult to place *Service_ security* in any of the aforementioned leadership style categories. Thus, *Service_ security* ends up in a separate category, Others.

To summarize, after going through the different leadership styles from previous studies and comparing them to the findings from my study, I ended up with a total of seven different leadership style categories. These categories include Transformational leadership, Transactional leadership, Benevolent leadership, Servant leadership, Intention-based leadership, Situational leadership, and Others.

5.2 Approach to motivation

Another essential part of my thesis is how security managers motivate employees. There wasn't much literature about this in previous studies, at least not from a leadership perspective. Many of the previous studies about employee motivation were based on motivation from the employees' perspective and what motivates the employees, but not specifically how security managers motivate the employees. This is something I wanted to find an answer to, and it's a huge part of my study and research question.

As mentioned, there wasn't much literature on which "methods" are used or how security managers motivate employees, but I can find some similarities between the literature from previous studies, which is described in Chapter 2, and findings from my own study.

Something that is mentioned in several previous studies is the importance of awareness of the employees in cybersecurity and how this is the security manager's responsibility. Monzelo & Nunes (2019) listed different responsibilities that the CISO has, including supervising, leading, and training their department and team, and information security risks and strategy training and awareness of the employees. They also state that it is the CISO's responsibility to influence and improve the culture in the organization in order to support information security. In their study, they conclude that: "The CISO role and their mission in organizations may be directly related to the awareness that exists on the matter, and that information security is not only an organizational matter but also a social and cultural theme" (Monzelo & Nunes, 2019). Several of the candidates from my study mentioned the importance of awareness of the employees in order to make them understand the various threats and threat actors that are out there. I believe that if the employees are not aware and understand why this topic is so important, then there is a greater chance of being exposed to attacks, etc. Two of the candidates from my study mentioned that awareness or awareness courses are one of the approaches that they use in order to motivate and influence employees. To give an example, *Section_manager* stated that "What is perhaps important for them to understand is the rationale behind it. Whether it's a state or cybercriminals doing it, you must explain why it's happening." In other words, *Section_manager* believes that awareness and understanding why, e.g., cybercriminals do what they do is the key point in motivating employees.

Another thing that has been mentioned in several previous studies is the importance of good communication skills among security managers or CISOs. In a study conducted by Sveen et al. (2023), one of the findings involving communication is that the CISO's responsibility often relates to and evolves around communication. They state that the most important job of the CISO is to communicate what might be a little more technically demanding for the other leaders to understand, using correct, proper, and understandable business terminology and language. Their study also shows that skills are needed for communicating cybersecurity to everyone in an understandable way, regardless of their background. Another study conducted

by Maynard et al. (2018) states that CISOs are required to have good communication, collaboration, and influential skills so that they are able to work with other business leaders and secure support from senior management and/or board when it's required, and also influence employee behavior. Sveen et al. (2023) also mentioned that it is important for the CISO to communicate well and be able to translate his/her technical expertise into a more fitting language to make other employees and top management understand the cybersecurity risk or solutions better. Some candidates also mentioned this theme as an approach to motivating employees. To give an example, *CISO_3* stated that "It's about the message you convey often being difficult, so you have to rewrite it into, let's call it, a leadership language." Another example from *Service_security* is that you have to speak "the right language", e.g., speaking the business language to business people.

5.3 The different leadership styles in relation to the approaches to motivation

As mentioned before, there wasn't much literature on which approaches are used or how security managers motivate employees, but the candidates that I interviewed mentioned several approaches to motivating employees. To make it a bit clearer, I made a table showing the different leadership styles I have found in my study, as well as the different approaches to motivation that were mentioned by those I interviewed. This overview can be found in table 5.1 below.

Leadership style	**Approach to motivation**
Transactional leadership	• Rewarding
Benevolent leadership (Paternalistic leadership)	• Exciting tasks • Supporting the employees • Speaking a language that they understand

Transformational leadership	• Post-it notes • Small reminders more often rather than having big e-learning courses all the time • Use current things in the media and use events that have happened • Good guides and advice available for the employees to access • Awareness • Making them understand why, e.g., cybercriminals do what they do
Servant leadership	• Awareness courses • Phishing tests
Intention-based leadership	• Mirroring methodology • Regularly publish articles on various topics that strengthen both the insight and motivation of the employees around security
Situational leadership	• Rewarding • Peer pressure

Others	• Focus on the basics • Don't make it too advanced or too complicated • It has to be relevant to the employee's own job, so it has to be directly applicable • Gamifying, e.g., simulated phishing tests • Understanding - they need to understand why something is not allowed and not recommended • Speaking a language that they understand, e.g., speaking the business language to business people

Table 5.1: Overview of the leadership styles and approaches to motivation

Several of the approaches are repeated in different leadership styles, so I do not see that there is necessarily a clear connection between the leadership style and the approaches to motivation. For example, rewarding as an approach to motivating employees can be found in both Transactional leadership and Situational leadership, and awareness or awareness courses can be found in both Transformational leadership and Servant leadership.

The findings from my study show both approaches that security managers use and approach that they don't think necessarily work that well. Some of the approaches that are used by some also turn out to be approaches that others do not think work and therefore do not recommend doing. An example of this is using phishing tests. A couple of the candidates that I interviewed used phishing tests as an approach to motivating employees. There were also two other candidates who believed that this was not a good approach to use, one because they didn't want to track the employees and constantly test them and the other because they didn't want to humiliate their employees. Another candidate mentioned that they wanted to use phishing tests in the future but that they hadn't had the capacity to do it yet. Therefore, security managers have a slightly divided opinion about phishing tests.

Another thing that I found in my study is that rewarding is a good approach to motivation, while others don't think that. The findings show that rewards are not unanimously viewed as an approach to motivation, so here, it is also a slightly divided opinion among security managers.

5.4 Implications for practice

My study contributes to promoting approaches that can help various organizations and security managers motivate and influence their employees' security behavior. These approaches can be found in table 5.1. It can also help raise awareness of how necessary it is to motivate your employees, especially in cybersecurity. My study presents findings like different approaches to motivation and also approaches that are not recommended. This allows security managers to try out different approaches and see what works best for them and also to stay away from the approaches that are not recommended. Further, my study also contributes to showing various leadership styles, which can give an idea of what kind of leadership style security managers have or can use.

5.5 Limitations and future research

This section contains the limitations of this study which I will discuss in more detail, and these points of limitations could impact the study.

- The findings are not measurable in relation to whether the mentioned approaches actually work to motivate the employees
- Lack of previous research studies on the topic
- Time constraints

The findings from this study are not measurable in relation to whether the mentioned approaches actually work to motivate the employees. Due to both limited time and the fact that the thesis or topic should not be too extensive, it was not possible to carry this out now. If I had had more time and also a bigger study, this would have been possible to get an answer. As I mention in section **??** below, it could be an opportunity to interview both security managers and employees to see which approaches are used to motivate and, at the same time, get an answer from the employees whether these methods actually work and to what extent.

Another possible limitation of this study is the lack of previous research studies on this topic. As I have already mentioned in the research gap, most of the previous research on this topic is from the employee's perspective and what motivates the employees, but not how security managers motivate and influence the employees' security behavior. The lack of previous research on this topic shows that there is a need to research it further, but it would have been valuable to have more previous research to compare it with.

The third possible limitation of this study is time constraints. This study was carried out over a period of just under half a year, which places limitations on what can be investigated.

I had an idea to make observations of the candidates in addition to the interviews, but due to limited time, this became difficult to carry out. Most of the candidates were based elsewhere in the country, some even abroad, so this would have taken quite a bit of time with travel and planning.

One of the limitations of this study is that the findings are not measurable in relation to whether the mentioned approaches actually work to motivate the employees, so this is something that could be studied further. If there is time for it, one can, for example, interview both security managers and the employees in the organization. In this way, you can get an answer to which approaches the security managers use to motivate the employees, and at the same time, you can get an answer from the employees as to whether these approaches actually work and to what extent. This process is possibly a bit more time-consuming, so this type of study is more suitable for someone with a longer project time than half a year.

Chapter 6

Conclusion

The purpose of this study was to find out how security managers in various organizations seek to motivate and influence employees' security behavior. This study's research question is: "How do security managers seek to motivate and influence employees' security behavior?" To investigate this further, I interviewed eight security managers from various organizations both in Norway and abroad. The main findings from this study are the different approaches the security managers use to motivate employees and the different leadership styles these security managers adopt.

This study shows that there is not just one approach to motivating employees but several different possible approaches. Some security managers use the same approaches, but there is definitely a variation in these approaches among the different security managers. There are differences in the approaches that are used to motivate in relation to the adopted leadership style, but also similarities across the styles. An overview of the different approaches found in this study is listed in table 5.1 in Chapter 5. This study also shows that security managers have several different leadership styles, and there doesn't seem to be just one ideal leadership style.

To answer the research question, there are multiple ways security managers seek to motivate and influence employees' security behavior, and there is not just one answer or one solution to this question. There are many different approaches that security managers use, and it is difficult to say which approach works best. Security managers should consider their current leadership style and adjust their approaches to motivate and influence employees' security behavior.

References

Amankwa, E., Loock, M., & Kritzinger, E. (2018). *Establishing information security policy compliance culture in organizations.* https://doi.org/10.1108/ICS-09-2017-0063

Anderson, A. B., Ahmad, A., & Chang, S. (2022). *Competencies of cybersecurity leaders: A review and research agenda.* https://aisel.aisnet.org/icis2022/security/security/9

Børresen, C. (2023). *Hva påvirker motivasjonen til medarbeiderne dine?* https://blogg.randstad.no/workforce360-bloggen/hva-pavirker-motivasjonen-til-medarbeiderne-dine

Brekke, A., & Gundersen, M. (2019). *Slik fungerer løsepengeviruset som rammet hydro.* https://www.nrk.no/norge/slik-fungerer-losepengeviruset-som-rammet-hydro-1.14481782v

Cleveland, S., & Cleveland, M. (2018). *Toward cybersecurity leadership framework.* https://aisel.aisnet.org/mwais2018/49

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). *How paternalistic leadership influences it security policy compliance: The mediating role of the social bond.* https://aisel.aisnet.org/jais/vol20/iss11/2

Grassegger, T., & Nedbal, D. (2021). *The role of employees' information security awareness on the intention to resist social engineering.* https://doi.org/10.1016/j.procs.2021.01.103

Guhr, N., Lebek, B., & Breitner, M. H. (2019). *The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory.* https://doi.org/10.1111/isj.12202

Hasib, M. (2014). *Cybersecurity leadership: Powering the modern organization.* Clarendon Press.

Hydro. (2020). *Cyberangrep på hydro.* https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Hydro. (2021). *2019: Cyberangrep på hydro.* https://www.hydro.com/no-NO/om-hydro/var-historie/2018-natid/2019-cyber-attack-on-hydro/

Jiawen, Z., Feng, G., & Liang, H. (2019). *How paternalistic leaders motivate employees' information security policy compliance? building climate or applying sanctions.* https://aisel.aisnet.org/pacis2019/42

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). *Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide.* https://doi.org/10.1111/jan.13031

Maynard, S., Onibere, M., & Ahmad, A. (2018). *Defining the strategic role of the chief information security officer.* https://aisel.aisnet.org/pajais/vol10/iss3/3

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). SAGE Publications.

Monzelo, P., & Nunes, S. (2019). *The role of the chief information security officer (ciso) in organizations*. https://aisel.aisnet.org/capsi2019/36

Myers, M. D. (2022). *Qualitative research in information systems*. https://www.qual.auckland.ac.nz/

Naydenov, R. S., Malatras, A., & Lella, I. (2022). *Enisa threat landscape 2022 : July 2021 to july 2022*. ENISA. https://data.europa.eu/doi/10.2824/764318

Nettskjema. (2023). *Nettskjema*. https://nettskjema.no/

Recker, J. (2021). *Scientific research in information systems a beginner's guide* (2nd ed.). Springer.

Sikt. (2023). *Sikt*. https://sikt.no/

Sveen, H. S., Østrem, F., Radianti, J., & Munkvold, B. E. (2023). *The ciso role: A mediator between cybersecurity and top management*. https://ojs.bibsys.no/index.php/NIK/article/view/1013

The Norwegian National Research Ethics Committees. (2019). *General guidelines*. https://www.forskningsetikk.no/en/guidelines/general-guidelines/

The Norwegian National Research Ethics Committees. (2023). *About the committees*. https://www.forskningsetikk.no/en/

UiO. (2023). *Nvivo*. https://www.uio.no/tjenester/it/forskning/datafangst-og-analyse/nvivo/

van Yperen Hagedoorn, J. M., Smit, R., Versteeg, P., & Ravesteyn, P. (2021). *Soft skills of the chief information security officer*. https://aisel.aisnet.org/bled2021/31

Xiao, Y., & Watson, M. (2019). *Guidance on conducting a systematic literature review*. https://doi.org/10.1177/0739456X17723971

Appendix A

Interview guide

Intervjuguide

Del 1 - Generell informasjon om deg og organisasjonen

1. Hvilken rolle har du i organisasjonen?
2. Hvor lenge har du jobbet i organisasjonen?
3. Hvor lenge har du jobbet med sikkerhet som leder? Har du noen tidligere ledererfaringer?
4. Hva er dine arbeidsoppgaver på dagsbasis?
5. Hva tenker du om rollen og ansvaret som leder for sikkerhet? Er dette et stort ansvar?
6. Hvordan vil du beskrive deg selv som leder? Kom gjerne med noen eksempler på din lederstil.

Del 2 - Sikkerhetskultur

7. Hvordan vil du beskrive sikkerhetskulturen i organisasjonen deres?
8. Føler du at de ansatte følger med på hendelser rundt cyberangrep osv?
9. Er de ansatte opptatt av sikkerheten i organisasjonen?
10. Hva tenker toppledelsen om sikkerhet? Blir det prioritert høyt?
11. Er det noen typer ansatte som har mer interesse av sikkerhet enn andre? Ser du noen forskjell på f.eks. kjønn eller alder?
12. Oktober er nasjonal sikkerhetsmåned. Gjør dere noe spesielt denne måneden, og har det en effekt blant de ansatte innad i organisasjonen?

Del 3 - Motivasjon og ledelse

13. Hva tenker du som leder er viktigst å lære bort til dine ansatte når det gjelder sikkerhet?

14. Hvordan synes du det er å motivere de ansatte når det kommer til sikkerhet?
15. Har du noen spesielle metoder som du bruker for å motivere de ansatte innen sikkerhet? Kom med eksempler.
    a. Er det noen metoder som du føler ikke fungerer like bra? Hvilke isåfall?
16. I hvor stor grad føler du at de ansatte trenger å motiveres?
17. Hva føler du som leder at du kunne bidratt med i fremtiden for å motivere de ansatte rundt sikkerhet?

Del 4 - Security policies

18. Følger dere noen spesielle sikkerhetspolicyer i organisasjonen? Kan du evt. nevne de viktigste?
19. Hvilken virkning tror du det har for organisasjonen og de ansatte å følge sikkerhetspolicyer?

Appendix B

Consent form

Vil du delta i forskningsprosjektet

Leadership and motivation in the field of cybersecurity

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å se nærmere på hvordan sikkerhetsledere motiverer og leder sine ansatte innen cybersikkerhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Dette er et masterprosjekt (studentoppgave/forskningsprosjekt) hvor formålet er å få et bilde av hvordan sikkerhetsledere i ulike organisasjoner motiverer og leder sine ansatte innen cybersikkerhet. Jeg ønsker å se nærmere på lederstiler og metoder som blir brukt for å motivere de ansatte, samt få et innblikk i sikkerhetskulturen i organisasjonen. Forskningsspørsmålet jeg ønsker å analysere er: How can security managers motivate their employees in the field of cybersecurity? Ved å få gode svar på dette forskningsspørsmålet, kan det hjelpe organisasjoner med å se hvilke metoder som fungerer best når det kommer til å motivere ansatte innen cybersikkerhet. Dette kan bidra med å hjelpe organisasjoner på lang sikt, da de ansatte er bevisste og motiverte for å opprettholde sikkerheten i organisasjonen.

Hvem er ansvarlig for forskningsprosjektet?
Jeg er en student (Sandra Cathrine Bjønnes) fra Universitetet i Agder ved fakultetet for samfunnsvitenskap og institutt for informasjonssystemer er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Utvalget er trukket ut ifra den stillingen og rollen kandidaten har i organisasjonen. Da min studie forsker på ledelse innen cybersikkerhet er det hensiktsmessig å intervjue kandidater som innehar en stilling og rolle innenfor dette fagfeltet.

Hva innebærer det for deg å delta?

- Min metode for informasjonsinnhenting er intervjuer. Intervjuene vil bli gjort med digitalt videoopptak, eller lydopptak, og opplysningene som samles inn av intervjuobjekt er:
    - Navn
    - Stilling/rolle i organisasjonen
    - Informasjon rundt din stilling og rolle i organisasjonen

- Hvis du velger å bli intervjuet vil dette ta deg ca. 60 minutter. Intervjuet inneholder spørsmål som [Hvilken rolle har du i organisasjonen?] - [Hva tenker du som leder er viktigst å lære bort til dine ansatte når det gjelder sikkerhet? Hvordan velger du å lære bort dette?] - [Hvordan vil du beskrive sikkerhetskulturen i organisasjonen deres?] og [Følger dere noen spesielle sikkerhetspolicyer i organisasjonen? Kan du evt. nevne de viktigste?]

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Kun behandlingsansvarlig Sandra Cathrine Bjønnes vil ha tilgang til dine opplysninger.
- Kun behandlingsansvarlig Sandra Cathrine Bjønnes vil samle inn, bearbeide og lagre data.
- Tiltak for at ingen uvedkommende får tilgang til personopplysningene dine inkluderer:
    - Navn og annen identifiserbar informasjon vil bli erstattet med kode/pseudonym.
    - Datamateriale vil bli lagret på sikret OneDrive sky-konto under skolens domene med to-faktor autentisering.
    - Personopplysninger og øvrige sensitive data vil bli lagret separat i innelåst/kryptert mappe.

Deltakere vil ikke kunne gjenkjennes i publikasjon. Deltakere vil anonymiseres og refereres til som intervjuobjekt eller evt. annet kallenavn dersom det er hensiktsmessig. Organisasjonens navn vil også anonymiseres. I den sammenheng vil ikke informasjon kunne knyttes til deltaker.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Etter endt prosjekt vil alt av oppbevarte data slettes fullstendig fra alle medier.

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

På oppdrag fra Sandra Cathrine Bjønnes har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

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

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

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

- Institutt for Informasjonssystemer ved Sandra Cathrine Bjønnes sandracb@uia.no og/eller veileder Marko Ilmari Niemimaa marko.niemimaa@uia.no ved Institutt for Informasjonssystemer.
- Vårt personvernombud: Rådgiver/Personvernombud ved IT-avdelingen: Trond Hauso trond.hauso@uia.no +47 936 01 625.

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- E-post: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Sandra Cathrine Bjønnes

Sandra Bjønnes ----------

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Leadership and motivation in the field of cybersecurity*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- □ å delta i intervjuer
- □ at Sandra Cathrine Bjønnes kan bruke opplysninger om meg til prosjektet

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

---

(Signert av prosjektdeltaker, dato)