UiA University of Agder

Master

Information security culture: An investigation into the impact of a large-scale cyberattack

A case study into the changes in information security culture in a Norwegian organisation after a cyberattack

VEGARD MARVIK & RAMI BAKIR

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

This master's thesis marks the end of the master's degree in Cybersecurity at the University of Agder. We would first like to thank our thesis advisor Associate Professor Marko Ilmari Niemimaa of the Department of Information Systems at the University of Agder. Your input and biweekly meetings were very appreciated, and you often got us out of roadblocks by providing valuable insights. We would also like to thank the anonymous participants that gave us some of their valuable time to answer our questions and let us collect valuable data for our research. We would also like to give special thanks to the CTO and CISO, who showed interest in our study and provided us with relevant participants.

Finally, we thank our families for their continuous support and encouragement during our education. Without their help, this would have been an impossible task to accomplish.

Abstract

Cybersecurity and cyberattack have been mentioned significantly more in the news in recent years, which has caused organisations to give higher priority to information security than ever before. Today, many organisations are vulnerable to malicious attacks like ransomware. These attacks can significantly impact an organisation's operations, especially given their reliance on technical systems. This has led to organisations emphasising technical security measures significantly, often overlooking one critical aspect of information security, namely information security culture (ISC).

This empirical study examines how an organisation's ISC changes during a ransomware attack and how it has continued to change in the aftermath. We employ a case study in conjunction with a literature review to evaluate the changes in security culture. Interviews with employees from different professions in this organisation gave us their perspectives on the changes before and after the attack and their thoughts on the implemented measures. To analyse the research, the authors looked into different ISC levels and how they have specifically changed, these levels include artefacts, espoused values, shared tacit assumptions and knowledge. The study analyses how the employees and leadership perceived the changes through these levels.

The research contributes to existing knowledge on information security culture by applying theory to a real-life situation and advancing the understanding of how an attack changes ISC within an organisation. By applying the theoretical framework from Van Niekerk and Von Solms (2010), we address the empirical findings and propose measures for organisations still developing their ISC.

Sammendrag

Cybersikkerhet og cyberangrep har blitt nevnt i mediene flere ganger de siste årene, noe som har ført til at organisasjoner har satt informasjonssikkerhet høyere på agendaen enn tidligere. Ransomware og andre digitale trusler utgjør en massiv risiko for sårbare organisasjoner. Med den avhengigheten organisasjoner i dag har til tekniske systemer, kan slike angrep påvirke hvordan en organisasjon fungerer i stor grad. Dette har ført til at organisasjoner legger stor vekt på tekniske sikkerhetstiltak, men ett aspekt som ofte blir oversett, er informasjonssikkerhetskultur.

Denne masteroppgaven undersøker hvordan en organisasjons informasjonsikkerhetskultur endres som følge av et ransomware-angrep og hvordan den fortsetter å endre seg i etterkant. For å evaluere endringene i sikkerhetskulturen, bruker vi en case-studie i kombinasjon med en litteraturstudie. Ved hjelp av intervjuer med ansatte i forskjellige yrker i denne organisasjonen ga det oss deres perspektiv på endringene før og etter angrepet og deres tanker om tiltakene som ble implementert. For å analysere dette ser forskningen på ulike informasjonsikkerhetskultur-nivåer og hvordan de har endret seg, disse nivåene inkluderer "artefacts", "espoused values", "shared tacit assumptions" og "knowledge". Gjennom disse nivåene analyserer studien hvordan de ansatte og ledelsen oppfattet endringene.

Forskningen bidrar til eksisterende kunnskap om informasjonssikkerhetskultur ved å anvende teori på en reell hendelse og fremmer forståelsen av hvordan et angrep endrer informasjonsikkerhetskulturen i en organisasjon. Ved å anvende det teoretiske rammeverket fra Van Niekerk and Von Solms (2010), tar vi opp de empiriske funnene og foreslår tiltak for organisasjoner som fortsatt er i prosessen med å utvikle sin informasjonsikkerhetskultur.

Contents

Acknowledgements ii

Abstract iii

Sammendrag iv

List of Figures ix

List of Tables xi

1 Introduction 1
- 1.1 Research Questions . . . 2
  - 1.1.1 Research Approach . . . 2
  - 1.1.2 Thesis Structure . . . 2

2 Theoretical Framework 4
- 2.1 Organisational Culture . . . 4
  - 2.1.1 Schein's Corporate Culture Model . . . 4
  - 2.1.2 Changing Organisational Culture . . . 6
- 2.2 Information Security Culture . . . 7
  - 2.2.1 Developing Information Security Culture . . . 8
- 2.3 The Levels of Information Security Culture . . . 10
  - 2.3.1 Artefacts . . . 10
  - 2.3.2 Espoused Values . . . 11
  - 2.3.3 Shared Tacit Assumptions . . . 12
  - 2.3.4 Knowledge . . . 12
- 2.4 Elasticity . . . 13
  - 2.4.1 Elasticity in Information Security Culture . . . 13
- 2.5 The Conceptual Information Security Culture Framework . . . 13

3 Methodology 16
- 3.1 Review Methodology . . . 16
- 3.2 Literature Search and Evaluation . . . 17
  - 3.2.1 Database Selection . . . 17
  - 3.2.2 Exclusion Criteria . . . 17
  - 3.2.3 Literature Identification . . . 18
  - 3.2.4 Selection of Literature . . . 19
- 3.3 Case Study . . . 21
  - 3.3.1 Case Selection . . . 21
  - 3.3.2 Data Collection . . . 22
  - 3.3.3 The Qualitative Interview . . . 22
- 3.4 Data Analysis . . . 23

3.4.1 Reliability and Validity . . . 26
3.5 Research Design Limitations . . . 27
3.6 Ethical Issues . . . 27

4 Findings **29**
4.1 Changes to Artefacts . . . 29
4.1.1 Password Policies and Authentication . . . 29
4.1.2 Security Training and Awareness . . . 31
4.1.3 Communication Channels and Information Dissemination . . . 32
4.1.4 Infrastructure Setup and Security Measures . . . 32
4.1.5 User Engagement . . . 32
4.2 Changes to Espoused Values . . . 33
4.2.1 Rigid Control and Centralised Management . . . 33
4.2.2 Attention from Leadership . . . 34
4.2.3 Security Measures and Policies . . . 34
4.3 Changes to Shared Tacit Assumptions . . . 35
4.3.1 Mandatory Security Training . . . 36
4.3.2 Cultivating a Blameless Postmortem Culture . . . 36
4.3.3 The Impetus for Increased Security Training . . . 37
4.4 Changes to Knowledge . . . 37
4.4.1 Organisational Learning . . . 38
4.5 Leadership Response . . . 39
4.6 Trust . . . 40
4.7 Subcultures . . . 40
4.7.1 Variations in Professions . . . 41
4.8 Overcompensation after the Attack . . . 42

5 Discussion **43**
5.1 Artefacts . . . 43
5.2 Espoused Values . . . 44
5.3 Shared Tacit Assumptions . . . 45
5.3.1 Attitudes Towards Data Security . . . 45
5.3.2 Perceptions of Security Training . . . 46
5.3.3 Communication Culture and Blameless Postmortems . . . 46
5.3.4 Motivations for Completing Security Training . . . 46
5.4 Knowledge . . . 47
5.5 Subcultures . . . 47
5.5.1 Variations in Professions . . . 48
5.5.2 Falling Back into Old Routines . . . 48
5.5.3 Changes in Levels of Culture . . . 49
5.6 Contribution to Research . . . 51
5.6.1 Changes in Information Security Culture after an Attack . . . 51
5.6.2 Subcultures and Variations in Professions within ISC . . . 52
5.7 Limitations of Research . . . 52
5.7.1 Single Case Study . . . 52
5.7.2 Time Constraints . . . 52
5.7.3 Limited Number of Interviews . . . 52
5.7.4 Potential Recall Bias . . . 52

6 Conclusions **54**
6.1 Suggestions for Future Research . . . 55

Bibliography **56**

A Article Overview **59**

B Consent Form **64**

C Interview Guide **68**

List of Figures

2.1 Schein's three levels of culture 5
2.2 Van Niekerk & Von Solms levels of culture 10
2.3 Van Niekerk & Von Solms conceptual framework model 14

3.1 Flow chart presenting the inclusion process 20
3.2 Qualitative data coding 25

5.1 Strong and stable or ideal culture. 50
5.2 Insecure and unstable culture. 50
5.3 Secure and unstable culture. 51

List of Tables

3.1 Participant overview 24
3.2 Theme creation based on codes 26
3.3 Final themes identified after phase 4 & 5 28

Chapter 1

Introduction

Cybersecurity is a topic that has seen a significant increase in its discussion and relevance in the last few years due to a substantial increase in digitisation as well as world events such as the COVID pandemic and the current war in Ukraine, which in turn has increased cybercrime. This increase has made investments into cybersecurity an essential part of any organisation, where large attacks are costing organisations billions in rebuilding their systems, loss of data, liability and customer confidence (AlHogail and Mirza, 2014). IBM (2022) defines a cyberattack as:

> Any intentional effort to steal, expose, alter, disable or destroy data, applications or other assets through unauthorised access to a network, computer system or digital device.

Cyberattacks have various reasons, but all attacks fall into one of three categories: criminal, political and personal and threat actors use different tactics to achieve their goals. In the last couple of years, malware attacks, social engineering, and password theft have been regularly seen as the method of choice for threat actors (IBM, 2022). Ransomware, the second most common type of cyberattack, is sophisticated malware that utilises strong encryption to hold data or systems hostage in exchange for payment and has been used in many attacks worldwide, such as the Colonial Pipeline attack and the attack on the Norwegian aluminium and renewable energy company Hydro (IBM, 2022).

The ransomware attack that targeted Hydro demonstrates the danger of cyberattacks. Despite having a dedicated security team and robust security measures, the attack caused extensive disruption to the company's operations and resulted in significant financial losses (Klevstrand et al., 2020). This incident underscores the vulnerability of organisations when faced with such threats. As such, there are many aspects of security that are possible to invest in, hardware, software, training and more. However, Al Hogail (2015) expresses that solely focusing on investing in the technical aspects of security without considering how employees interact with your systems will eventually be detrimental to the security of one's IT system. Such a focus has led many organisations to experience breaches attributed to intentional or unintentional decisions taken by employees, which has led to many research articles stating that human behaviour is the weakest link in the security chain (Al Hogail, 2015; AlHogail and Mirza, 2014; Connolly and Lang, 2012; Hassan et al., 2017; Ismail, 2022a; Ismail, 2022b). Thus leading to the conversation of the importance of developing an information security culture, which is described by AlHogail and Mirza (2014) as:

> The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in an organisation in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behaviour in a way that preserving the

information security becomes a second nature.

Organisations are, according to Glaspie and Karwowski (2018), investing large sums into technical cybersecurity solutions and neglecting investments into security culture and the human factors, which sooner or later will be harmful to one's IT systems (Al Hogail, 2015). While human errors are the cause for 95% of cybersecurity incidents today (World Economic Forum, 2022) and that undesirable behaviour is directly correlated to an organisation's information security culture, investments into technological cybersecurity solutions are continuing today (Glaspie and Karwowski, 2018). Research has found that an information security culture is the key to increasing security policy compliance (Glaspie and Karwowski, 2018) while also being essential to changing attitudes and perceptions and encouraging desirable security behaviours (Ismail, 2022b). These factors lead the employees to act as a "human firewall" to safeguard organisational information assets and reduce financial and reputational loss (Connolly and Lang, 2012).

Our research aimed to understand how information security culture in an organisation works and how it gets affected by a cyberattack. To address this issue, we interviewed employees in different positions in an organisation that experienced a ransomware attack some years before writing this thesis, where the organisation lost tens of millions of NOK. These interviews will be the basis of a case study into how the employees of this organisation handled security before and after the attack, as well as how the organisations changed their approach towards training and nurturing a security culture.

1.1 Research Questions

The research provided us with an interesting research gap we wanted to explore. To get an idea of how an organisation's information security culture is developed, we identified several articles to provide information; through this process, we identified that there was a lack of research discussing the effect a cyberattack has on an organisation, especially when it comes to the ISC of said organisation. Based on the identified research gap, we propose the following two research questions:

1. How does a cybersecurity incident affect and influence the information security culture in an organisation?
2. How do employees in different positions in this organisation view the impact the attack had on their working environment?

1.1.1 Research Approach

This thesis applies a qualitative approach to answer the proposed research questions. A case study into an organisation that experienced a was conducted, where semi-structured interviews were used to collect data from employees in different positions. A thematic content analysis using a deductive approach was used to analyse the data.

1.1.2 Thesis Structure

The following section provides an overview of the thesis structure and briefly introduces the remaining chapters and their content.

Chapter 2 - Theoretical Framework

The first part of this chapter covers some background information on organisational culture and cultural change in addition to presenting an organisational culture model and concludes with a discussion on changing organisational culture and organisational learning. The second

part of this chapter introduces information security culture and discusses the development of information security culture. Lastly, this chapter presents the information security culture model used as the theoretical framework in our thesis and discusses existing literature on information security culture.

Chapter 3 - Methodology

The approach used to conduct the research for this thesis is covered in this chapter. An explanation of what a literature review is, which method we chose, and why will be covered in the first part of this chapter. Towards the end, the method chosen to collect the necessary data is presented in addition to how the data was analysed. Furthermore, we also cover how we ensured the data validity and reliability of the study and what ethical considerations were made.

Chapter 4 - Findings

Chapter 4 details the findings obtained from the research. The findings are presented in themes, sub-themes, and excerpts from the interviewees.

Chapter 5 - Discussion

In this chapter, there will be a discussion of the findings connected to previous research to provide insights into what the findings mean for ISC. The chapter will address research gaps and provide valuable data that can provide organisations with changes to consider.

Chapter 6 - Conclusions

This chapter will cover the conclusions based on what was discussed in chapter 5 and will be used to answer the research questions. Suggestions for further research and practical contributions/research contributions will also be covered.

Chapter 2

Theoretical Framework

In this chapter, we will briefly explain organisational culture and introduce an organisational culture model created by Edgar Schein. The first part will also include a section on changing organisational culture and organisational learning. Furthermore, a discussion on information security culture and its importance, using Van Niekerk and Von Solms' model as the main theoretical framework in conjunction with the findings from the literature review, can also be found in this chapter. To adequately explain Van Niekerk and Von Solms' model, a brief explanation of the economic concept of elasticity and how the authors have incorporated elasticity in an information security culture setting. Lastly, we present the conceptual model proposed by Van Niekerk and Von Solms and explain that the nett overall effect information security culture has on the organisation's security efforts depends on the strength of the four levels. This research will also discuss the literature found when searching within specific parameters connected to ISC, connect the themes to our theoretical method, and identify the possible gaps in the current literature. Tilahun and Tibebe (2017) discusses the impact of human aspects on technology and suggests that it should be studied more:

> Nowadays, it becomes clear that technology alone cannot lead to satisfactory solutions, and the human aspects cannot be isolated from technology. In this respect, increasing numbers of researchers argue that, to prepare better to tackle the ISS problem, the human element needs to be well studied and addressed.

2.1 Organisational Culture

In order to understand the concept of information security culture, this section will first briefly explain the concept of organisational culture. Culture can be found in every organisation that exists today. As an organisation grows, it develops its culture and subcultures based on occupations, functions and geographies (Schein, 2009). The author further states that culture not only resides within us but also the hidden force that drives most of our behaviour both inside and outside organisations. The biggest mistake when trying to understand culture is, according to Schein (2009), to oversimplify it. While stating that culture is just "the way we do things around here", a more appropriate approach to culture is to realise that culture exists at several levels that must be understood and managed. Schein (2009) presents a model for an organisational culture that has been widely accepted amongst researchers.

2.1.1 Schein's Corporate Culture Model

There are many different descriptions in use for organisational culture (AlHogail and Mirza, 2014; Connolly and Lang, 2012; Ramachandran et al., 2013;). However, a widely used

definition is the one by Schein (2009), where the author describes organisational culture as follows:

> Culture is a pattern of shared tacit assumptions that was learned by a group as it solved its problems of external adaption and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.

As stated above, Schein (2009) expresses that culture exists at several levels that must be understood and managed. They also suggests that culture can be divided into three levels: artefacts, espoused values and underlying assumptions, as seen in figure 2.1.

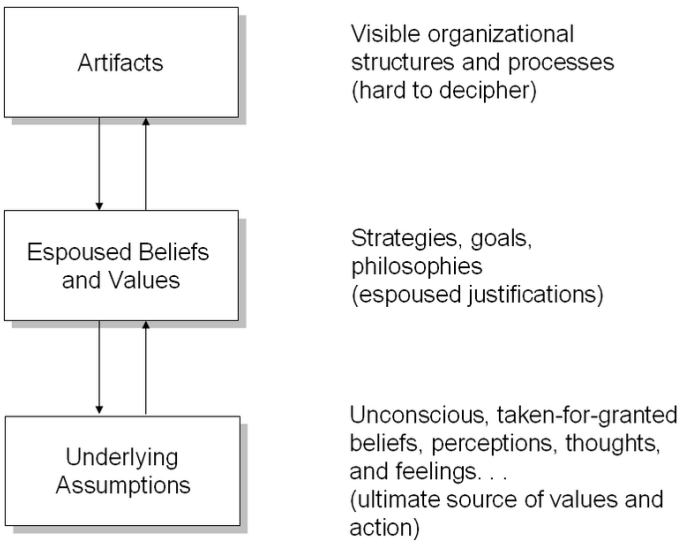

Figure 2.1: Schein's three levels of culture

Level One: Artefacts

According to Schein (2009), artefacts are what you see, hear and feel in an organisation, including visible organisational structures and processes. While one organisation is more casual, another may be more informal and show that culture is apparent and has an immediate emotional reaction upon oneself. However, observing the artefacts alone is not enough to explain why the employees behave as they do, so one needs to explore more profound levels of culture to understand the reasoning for their behaviour. This leads us to level two, the organisation's espoused values.

Level Two: Espoused Values

Schein (2009) describes the espoused values as the reasons an organisational insider would give for the observed artefacts and behaviour patterns. One must ask questions about the organisation's values to find these reasons. The first thing one learns is that the organisation has specific values that are supposed to create an image of the organisation (Schein, 2009). As part of this investigation, an organisation can also provide documentation describing their values, principles, ethics and visions as part of their official viewpoints, which is also what espoused values usually are (Schein, 2009). It also points out that two organisations with very different artefacts can still share the same espoused values. Additionally, the more questions we ask, the more we will notice inconsistencies between the espoused values and the visible behaviour, which tells us that a deeper level of thought and perception drives the observable behaviour (Schein, 2009).

Level Three: Shared Tacit Assumptions

On this more profound level, the shared tacit assumptions are the beliefs, values, and assumptions imposed on the employees by the individuals or teams that started the organisation. Additionally, these assumptions were formed in the early days of an organisation because specific strategies allowed the company to be successful, gradually making these beliefs and values be shared and taken for granted (Schein, 2009). By becoming shared and taken for granted, they form the essence of the organisation's culture. New employees consider the founder's beliefs, values and assumptions to be the cause for organisational success and, therefore, must be right. Moreover, one must remember that the shared tacit assumptions resulted from a collaborative learning process (Schein, 2009).

2.1.2 Changing Organisational Culture

Organisational culture can be a mysterious phenomenon for both insiders and outsiders to grasp and is often invisible to the employees in an organisation (Lacey, 2010). According to Schein (2009), in an organisational setting, humans sometimes have to unlearn something to learn something new because the new behaviour calls for it. Some might resist this change because they are unwilling or unable to do so. Moreover, organisations must consider that resistance to change will occur at some point and find the reasons for it. This is especially true for cultural assumptions because once the cultural elements are established in an organisation, they provide employees meaning, predictability and security (Schein, 2009).

While some employees might try to resist these changes, it will gradually creep into their thinking and lifestyle and shape their outlook into a corporate perspective which influences their everyday views and behaviour (Lacey, 2010). Employees also behave in ways that are consistent with organisational values. When values associated with an information security program do not align with the organisational values, it causes conflict and might contribute to employees acting inconsistently with the IS policies and standards (Kayworth and Whitten, 2010).

Lacey (2010) further emphasises that organisational culture's influence on one's thinking and perception makes it hard to differentiate from one's natural judgement and personality. However, organisational culture is not the only influence on employee behaviour, Lacey (2010) states that their immediate environment, the behaviour of peers, the demands of management, perceived roles, past experiences, cues and prompts in systems and processes and most importantly, the perceived consequences of actions are additional factors that influence employee behaviour.

Lacey (2010) states that before attempting to change the culture, one has to consider the constraints of social networking, which injects fresh perspectives on events and thinking at the expense of dialogues with colleagues seated across the desk. Nevertheless, social networking can also change organisational culture by engaging the employees with a convincing argument that existing assumptions are not valid anymore. Lacey (2010) further highlights that changing attitudes requires a process of self-discovery for each employee, but while individual behaviours are influenced by specific motivators, attitudes and culture go through a more subjective process over a more extended period.

Research states that a healthy security culture consists of an informed awareness of security risks, employees' willingness to report incidents or weaknesses, honesty in assessments of security compliance and lastly, a degree of empowerment to enable staff to take remedial action (Lacey, 2010). Uchendu et al. (2021) also found that employee behaviour is a vital part of an information security culture and expresses that organisations must incorporate change management principles to see positive change. Change management guides and

supports employees towards the change necessary to develop a security culture within an organisation (Uchendu et al., 2021). Al Hogail (2015) supports this statement, stating that there is a positive relationship between ISC and the application of change management principles and concludes that these principles are valuable in creating an effective information security culture. Lacey (2010) emphasises that to change how people function in a working environment, one must have a good understanding of human behaviour and have some knowledge of best practices in marketing communications.

Moreover, Lacey (2010) highlights the importance of separating the need for knowledge, attitude and behaviour changes because they require different methods. Conveying knowledge calls for good, compelling communication, but changing employees' attitudes is a much more challenging task and calls for a personal journey of discovery. The most complex challenge, however, is changing behaviour, as this requires careful attention to a wide range of motivation factors. These factors must be considered when creating an effective change program. However, one must also figure out what the employees know and think about security and the behaviour in their day-to-day work performance (Lacey, 2010).

While Uchendu et al. (2021) found that implementing change management principles has benefits, they also mention that since this framework affects all activity in an organisation, one has to be mindful of resistance to change, especially if it disrupts the working environment. They suggest pairing the change management principles with employee and management knowledge to implement and maintain change. Kayworth and Whitten (2010) asserts that technology risks, legal compliance issues, and constantly changing business requirements are what organisations are facing today. To stay competitive while simultaneously having an effective information security function, they suggest that organisations must achieve three competing objectives:

1. balancing the security of information assets against the need to enable business
2. ensuring compliance
3. maintaining cultural fit

According to Kayworth and Whitten (2010), organisations that achieve these objectives will have a highly effective information security function and related strategy that is business driven and strategically focused.

Organisational Learning

Hassan et al. (2017) discusses the security culture of a healthcare organisation and what they learned performing a qualitative study on said organisation. The research demonstrated that security awareness, security knowledge, and security behaviour are the three key elements that foster the development of an information security culture. These factors necessitate strong commitment from top management to ensure professionals embrace the culture of information security. The study indicates that the emerging field of information security culture is gradually gaining momentum, although previous literature offers limited measurement approaches.

2.2 Information Security Culture

It is assumed that information security culture is a part of the organisational culture as information security has become an organisational function. However, information security culture is only thought of as a subculture of an organisation's overall culture; information security must become a natural aspect of the daily activities of every employee (AlHogail and Mirza, 2014), meaning that they must also align the various subcultures towards a common corporate purpose (Schein, 2009). Da Veiga (2016) also supports this, stating

that an information security culture develops similarly to organisational culture. Connolly and Lang (2012) found that information security culture is regarded as a measure that can help promote vigilant security behaviour of employees and make them comply with security policies. Nevertheless, what is information security culture exactly? There are many definitions used to describe the term information security culture (Martins and Elofe, 2002; Ngo et al., 2005; Malcolmson, 2009; Al Sabbagh et al., 2012), yet in their paper AlHogail and Mirza (2014) adopts the above definitions to create their own which can be found in chapter 1. Other definitions for information security culture can be found in Ismail (2022a) and Connolly and Lang (2012).

While information security culture is assumed to be a subculture of organisational culture, it is an aspect of security that can be difficult to comprehend. Organisations need a clearer idea of what it is and how to improve it. The World Economic Forum (2022) states that 95% of the cybersecurity issues today can be traced to human error, which may indicate a difficulty in understanding how to improve information security culture. According to their definition, AlHogail and Mirza (2014) states that information security culture should influence employees' security behaviour and expresses that this should be done through the organisational culture as it guides the activities of the employees by placing constraints upon their activities and behaviour and defines what they must, can or cannot do. Seeing that human errors are the cause for 95% of cybersecurity issues, information security practices should become part of the corporate culture of an organisation (AlHogail and Mirza, 2014) and guide the employees on how to interact with IT systems to avoid actions that may cause risks (Al Hogail, 2015). Solely focusing on the technical aspects of security, without appropriate consideration of the human interaction with the system, will only lead to increased risks for cybersecurity issues (Al Hogail, 2015). The research further states that regulations that mandate employee behaviour are inefficient at promoting good security-related human behaviour and that enforcing security policies is less effective than when employees know, understand and accept the necessary precautions. Van Niekerk and Von Solms (2010) states that establishing an information security culture in an organisation is necessary for adequate information security, which can help turn employees into security assets instead of security risks.

2.2.1 Developing Information Security Culture

Developing an information security culture is a complex process, and various research discusses how this is best done. According to Alnatheer (2015), information security culture, which is a part of organisational culture, involves employees' behaviour. Ismail (2022a) concludes that SMEs (Small and midsize enterprises) need to develop a culture that prioritises information security and aligns with their business objectives. The author recommends that SMEs develop policies and procedures that align with their organisational culture and provide training to employees on the importance of information security and how to comply with policies and procedures. Research done by AlHogail and Mirza (2014) implores organisations to pay efforts towards building an ISC and to integrate information security practices into the organisation's corporate culture to ensure that the knowledge and skill of employees are at a proper level where they can act appropriately towards security. Al Hogail (2015) provides further research stating that "The culture that promotes good security-related human behaviour through knowledge, artefacts, values, and assumptions is far more effective than regulations that mandate employees' behaviour." Al Hogail (2015) further concludes, that it can be derived from empirical studies that the level of information security culture is strongly linked to the availability of an information security team and the authority given to that team.

Meanwhile, Chen et al. (2015) found a strong direct influence of SETA (Security Education, Training, and Awareness) programs' awareness of security culture in organisations.

Moreover, the authors further emphasise the importance of including the employees while formulating, designing and developing information security policies if the goal is to establish a strong and sustainable security culture in the organisation. These findings are supported by Spears and Barki (2010), which found that users add value to IS security risk management when prioritising, analysing, designing, implementing, testing and monitoring user-related security controls within business processes. Having users participate in this process raises organisational awareness of security risks and controls, which contributes to more effective security control development and performance (Spears and Barki, 2010).

+

Leadership Support and Communication

Glaspie and Karwowski (2018) states that management support is an important factor in cultivating ISC and that consistent support is essential to creating a supportive environment in the organisation. While management support is necessary, their commitment also plays a vital role in influencing good security behaviour, setting an example to the employees of how IS should be viewed (Al Hogail, 2015). Alnatheer (2015) also states that management support is crucial when establishing an information security culture and that strong leadership and commitment are necessary at the initial stage to succeed in the long term. A lack of management support creates an organisational culture where bad security practices are more prevalent (Alnatheer, 2015). Dojkovski et al. (2010) states that managers communicate the importance of information security and related employee responsibilities through awareness, education and training activities but that the managers' influence is even more significant if they learn about the security challenges employees face. Based on the empirical study done by Al Hogail (2015), it can be concluded that there is a strong correlation between the level of an information security culture within an organisation and the presence of an information security team that is adequately empowered and authorised to carry out its duties. Glaspie and Karwowski (2018) further states that management support affects compliance attitudes by facilitating cross-training, knowledge sharing and security collaboration. Sharing security knowledge and collaborating on security goals allows employees to raise awareness while having a positive attitude towards compliance (Glaspie and Karwowski, 2018). Attitude towards compliance is critical, considering it has the most significant effect on information security policy compliance (Da Veiga, 2016).

Variations in Professions Across an Organisation

Ramachandran et al. (2013) suggests that within an organisation, employee behaviour is shaped by both the organisational culture and the professional culture in which they operate. As a result, gaining a deeper understanding of professional culture is essential to comprehending employee behaviour in the workplace. This study focused on developing a characterisation of information security cultures across four different professions. Their findings suggest notable differences in security cultures across these professions, providing valuable preliminary evidence of the varying influences of professional culture on information security practices within organisations. Johnston et al. (2019) found that employee groups within a broader organisation act uniquely in their collective responses to cyberattacks, and even though policies and procedures are dictating how to handle security incidents, each employee group may form its interpretation and enforcement of the policies that influence its members' responses to the incident. Schein (1996) discusses the idea of subcultures within an organisation, where getting a cross-functional project to work is difficult because each team has different ideas, ways of communicating and values. Schein (1996) further states that different teams will have different meanings related to, for example, words: "The word "marketing" will mean product development to the engineer, studying customers through market research to the product manager, merchandising to the salesman, and constant change in

design to the manufacturing manager. When they try to work together, they often attribute disagreement to personalities and fail to notice the deeper shared assumptions that colour how each function thinks." This aspect of subcultures is something we needed to keep in mind when conducting the study, as the organisation in question had several different professions involved, as well as several branch offices.

2.3 The Levels of Information Security Culture

Van Niekerk and Von Solms (2010) states that Schein's three levels of corporate culture could be seen to correspond closely to the behavioural aspects of the "human factor" in information security and that this "human factor" consists of two dimensions, namely knowledge and behaviour. They further state that, due to the co-dependency between these two dimensions, one can not ignore the impact a lack of information security-related knowledge would have on an organisational sub-culture of information security (Van Niekerk and Von Solms, 2010).

One can assume that the average employee has the required knowledge to do their job. It can not be assumed that the employees have the necessary knowledge to perform their job securely (Van Niekerk and Von Solms, 2010). Nevertheless, in the case of information security, knowledge is only required when it is necessary to perform the typical job functions in a way that is consistent with good information security practices. All activities in an organisation need to be performed in a way that is consistent with good information security practices to foster a sub-culture of information security, and knowledge regarding information security is a prerequisite to securely performing any job function (Van Niekerk and Von Solms, 2010). They further state that information security knowledge, or the lack thereof, could be seen as a fourth level to an information security culture, which affects each of the three layers in Schein's corporate culture model.

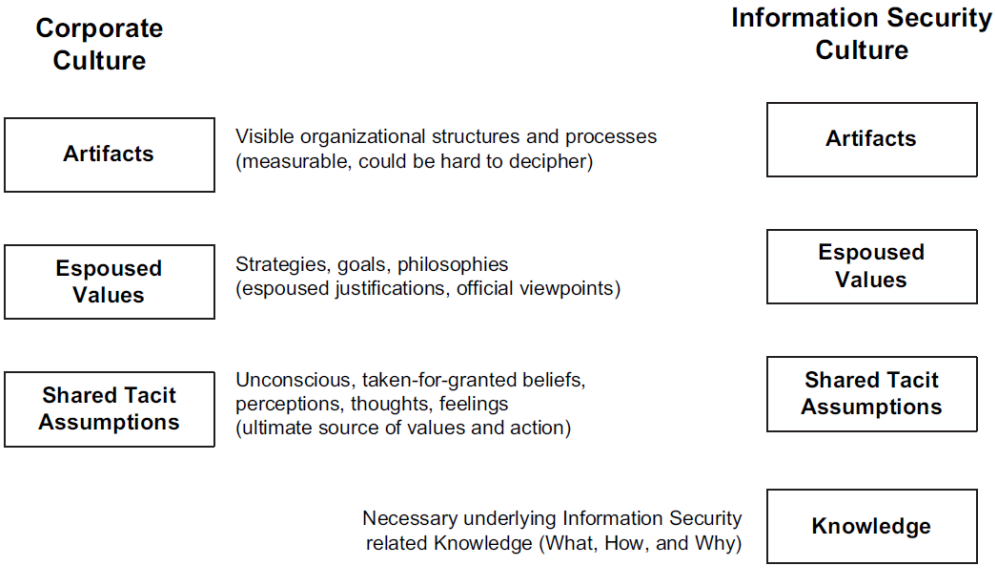

Figure 2.2: Van Niekerk & Von Solms levels of culture

2.3.1 Artefacts

Van Niekerk and Von Solms (2010) describes this level as what happens in an organisation and emphasises that it is impossible to perform day-to-day tasks securely without the necessary skills and proficiencies. They suggest that for the daily tasks to happen securely, the employees must have sufficient knowledge of how to perform them securely. In an article written by Ismail (2022a), they recommend that SMEs evaluate the effectiveness of their information security culture artefacts regularly and make necessary adjustments to improve

their effectiveness. The study also reveals that artefacts such as training programs are particularly effective in improving employees' behaviour towards information security. The author finds that employees who receive information security training are more likely to comply with security policies and procedures and better understand the importance of information security.

Training and Awareness Artefacts

Training and awareness is a foundational piece of all thriving information security cultures, as it provides employees with the required knowledge necessary for adequately using systems, compliance with policies, and handling data (Glaspie and Karwowski, 2018). Da Veiga (2016) highlights the need for organisations to prioritise developing and communicating effective information security policies, as this can serve as a motivating factor to bridge the gap between organisations that currently lack awareness initiatives and those that already have them in place. The study suggests that raising awareness and promoting better communication of information security policies can help eliminate disparities in implementing these policies across different organisations. Chen et al. (2015) found a strong direct influence of SETA programs awareness on security culture in organisations such that a well-implemented and designed program can change employees' perceptions, attitudes and beliefs on security. This was, in turn, found to make employees act on safeguarding information security assets at the cost of extra effort and workload and help create an organisational security culture where each employee assumes responsibility for information security (Chen et al., 2015). However, merely having security policies and expecting employees to fully understand and favourably perceive them will not make the employees automatically comply with them and consequently marginalises the effect the policies usually would have had (Chen et al., 2015). An essential aspect of ISC is the problem of turning employees from security risks to security assets. Glaspie and Karwowski (2018) state that "Computer users who possess adequate knowledge of information security concepts exhibit a more positive attitude towards information security, which results in more positive behaviour. Organisations need to provide employee information systems and security training that is sufficient enough to eliminate errors".

2.3.2 Espoused Values

Information security policy is essential to an organisation's overall security posture and provides a foundation for all other security aspects. The person or team creating the policy must know what it should include to adequately address the organisation's security needs (Van Niekerk and Von Solms, 2010). While the person or team developing these policies must know what to include, they must know various aspects of all professions in a particular organisation. Chen et al. (2015) states that to build a strong and sustaining information security culture, it is necessary to include other employees while formulating, designing and developing new information security policies. It is also suggested to include the employees in developing and implementing monitoring schemes so that feedback on security policy compliance could help foster a positive security culture instead of using monitoring to control them (Chen et al., 2015). Ismail (2022b) on the other hand, found that "IS security culture has a significant influence on employees' attitudes toward security policy and procedures" and that security culture has a significant effect on attitude and normative belief in social engineering resistance. Research has also found that security policies are critical in directing an information security-positive culture (Da Veiga, 2015). The author further states that if employees have not read or understood the security policy, it will not be effective in directing their behaviour, influencing their attitude towards policy compliance or fostering an information security-positive culture (Da Veiga, 2015). Considering that security policies are an essential part of security practices within organisations, some organisations do not

understand the importance of establishing security policies and how substantial the impact on their organisational security can be without them (Alnatheer, 2015).

2.3.3 Shared Tacit Assumptions

According to Van Niekerk and Von Solms (2010), the shared tacit assumptions consist of the beliefs and values of employees. They further state that in an information security culture, knowledge underpins and supports the three levels of corporate culture, and information security can only be ensured with sufficient knowledge. Additionally, these four levels will impact how secure or desirable the overall information security culture will be. To elaborate on this Johnston et al. (2019) discusses how the formal social structure of an employee group has a significant impact on its collective ability to respond to security incidents and that employees often see security as an organisational problem rather than something they play an integral part in. They further suggest that because of this, it is essential that information security managers understand the employees and the various groups associated with them and how these groups interpret security incidents and their organisation's expectations regarding employee response. Glaspie and Karwowski (2018) explains that employees will adopt the attitudes, opinions and practises of their work teams in the absence of expertise and that this is how group attitudes drive the behaviour of individuals.

While Alnatheer (2015) discusses how important security policies are for developing an information security culture and that this is so important because the goal of security culture is to influence the behaviours of employees to comply with the security policies. This suggests that improving the shared tacit assumptions in an organisation, such as security policies, can be an essential step towards improving this level of culture. As well as the way management handles social structures within organisations.

2.3.4 Knowledge

Van Niekerk and Von Solms (2010) adds knowledge as a fourth level of culture. It expresses that this is specific to an information security culture and indicates that this adaption is necessary because one cannot assume that an employee knows to perform their job securely. Furthermore, the authors state that instead of viewing knowledge as a sub-component of Schein's three levels, adding it as a fourth level can more clearly show the effect that knowledge, lack thereof, would have on the overall information security culture (Van Niekerk and Von Solms, 2010). The authors also state that organisations should utilise awareness campaigns to address the problems that a lack of knowledge might lead to in conjunction with helping create a culture of information security. According to research, awareness campaigns are the critical element in ensuring that the knowledge level of an ISC is of adequate strength by instilling aspects of information security in every employee as a natural way of performing their job (Van Niekerk and Von Solms, 2010) An empirical study by Da Veiga (2015) claims that "Employees' knowledge and perception of information security policy rules and procedures influence information security behaviour and potentially the information security culture". While another article by Johnston et al. (2019) discusses how knowledge works in larger groups. Larger groups may have more resources and knowledge to draw upon but may also be less cohesive and less able to coordinate effectively. Similarly, groups with more diversity may have a wider variety of perspectives and knowledge but may also have more difficulty reaching consensus and coordinating. Research done by Dojkovski et al. (2010) suggests that in SMEs, knowledge sharing, cooperation and collaboration at individual and organisational levels help employees learn about information security and that learning processes should be reviewed regularly. Johnston et al. (2019) address the topic of education and knowledge, where the more education you have, the more knowledge you will have in certain areas, which will affect how employees implement a particular security policy or guideline.

They also mention the fact that communication is essential and that rules and procedures must have a rationale for them to be implemented.

2.4 Elasticity

According to their research, Van Niekerk and Von Solms (2010) have used the economic concept of elasticity to explain that change is inherent in any organisation. Elasticity is typically used to measure a variable's sensitivity to change in another variable (Van Niekerk and Von Solms, 2010). However, the speed at which such change occurs depends on the degree of elasticity. Van Niekerk and Von Solms (2010) states that according to economic theory, the market will be in equilibrium if the quantity of goods or services demanded in the market is matched perfectly by the number of goods or services supplied in this market and assuming that all other variables are fixed the price would be perfectly static and predictable. Nevertheless, if a change were to occur in one of the variables, it would create a disequilibrium where the price is more dynamic and difficult to predict (Van Niekerk and Von Solms, 2010). It is important to note that not all systems would have the same inherent degree of elasticity; it could range from infinitely elastic systems to entirely inelastic systems. According to Van Niekerk and Von Solms (2010), an infinitely elastic system creates an increase in supply that does not affect the demand or the price people would be willing to pay. In an entirely inelastic system, on the other hand, the supply and demand would always stay in equilibrium; in other words, they would be locked together.

2.4.1 Elasticity in Information Security Culture

Van Niekerk and Von Solms (2010) argues that the policies and procedures comprising the espoused values in an ISC indicate how much security management demands from employees. Likewise, according to their research, the shared tacit assumptions can reflect how much compliance employees are willing to supply. If these two supply and demand curves were to be modelled, the intersection of these curves would indicate the actual amount of effort employees are willing to give (Van Niekerk and Von Solms, 2010).

If management expectations are in perfect equilibrium with the employee's shared tacit assumptions, the resulting effort employees expended on behalf of the organisation's information security would be perfectly predictable (Van Niekerk and Von Solms, 2010). The research also says that predicting how much effort employees are willing to expend towards the overall security goals would be more difficult if management expects more than what the employees are willing to provide. Furthermore, only with the required knowledge can the willing employees do their security-related jobs.

Van Niekerk and Von Solms (2010) specifies that there is a causal relationship between the artefact level and the other levels of the ISC model, seen in figure 2.2, and the employees' actual behaviour towards information security is the result of the combined effects of the espoused values, the shared tacit assumptions and the underlying security knowledge. As such, stricter espoused values will have an elastic effect on the artefacts, which requires an identical increase in the shared tacit assumptions, knowledge or both levels. With stricter espoused values, the security effort employees are willing to give, or their security knowledge has to increase to align with each other. Without it, it would be difficult to predict the resulting employee behaviour due to the culture not being in equilibrium.

2.5 The Conceptual Information Security Culture Framework

Van Niekerk and Von Solms (2010) expresses that each culture level can positively or negatively impact the ISC and that the overall effect of an organisation's ISC can be seen as an

accumulation of each level. Van Niekerk and Von Solms (2010) proposes a model, seen in figure 2.3, to demonstrate the interaction between the four levels and their effects on security efforts.

This model in figure 2.3 depicts the four levels of ISC, seen in figure 2.2, but includes two additional elements which represent the minimum acceptable security baseline (BL) and the net effect of the culture on the overall security effort (SL). Van Niekerk and Von Solms (2010) explains the different elements in figure 2.3 as follows:

- BL or the minimum acceptable baseline indicates a culture whose net effect would meet the minimum qualifications for an industry standard.
- SL or the nett security level signifies the actual nett effect of the culture on the overall security effort or the average strength of the culture. Depending on its placement, it can either be more secure, less secure or just as secure as the BL.
- AF, or artefacts, represents the relative strength of the artefact level of the culture.
- EV, or espoused values, indicates the relative strength of the organisation's policies and procedures.
- SA or shared tacit assumptions signifies the relative strength of the employees' underlying beliefs or values.
- KN or knowledge, represents the employees' information security knowledge.

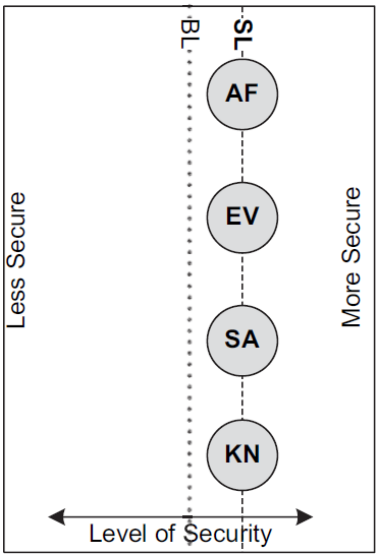

Figure 2.3: Van Niekerk & Von Solms conceptual framework model

All elements representing the various cultural levels can be on either side of the BL or precisely on the baseline, which can be interpreted as a representation of the relative strength of each level (Van Niekerk and Von Solms, 2010). For example, the artefact node to the right of the baseline indicates that artefacts are more secure than the acceptable minimum. However, the same node to the left indicates that the measurable artefacts are not as secure as they should be. The measurable artefacts would be as secure as the baseline requires if the node were precisely on the BL (Van Niekerk and Von Solms, 2010).

Thus, the culture in figure 2.3 can be interpreted as a strong or secure culture because all four levels have greater strength than the BL, which yields a positive nett security level. The nett effect, however, can be positively or negatively influenced depending on how secure the underlying levels of culture are. With all four levels perfectly aligned, it also results in a wholly stable or predictable culture. It can thus be explained as being in perfect equilibrium

or the ideal culture in terms of information security thanks to it being strong and stable (Van Niekerk and Von Solms, 2010).

However, Van Niekerk and Von Solms (2010) emphasises that while the terms strong and stable are used, it does not indicate how pervasive or resistant the culture might be to change. The authors express that a strong information security culture should instead be interpreted as a desirable culture. The same goes for the term stable, Van Niekerk and Von Solms (2010) states that this should indicate how predictable the artefacts or the network security level of the culture would be for any scenario.

The visible and measurable artefacts result from a combination of the espoused values, the elasticity effect of the shared tacit assumptions, and the user knowledge of these espoused values. It is important to note that the artefact level is a reliable indicator of an organisation's overall security from a security perspective, as it accurately reflects day-to-day operations (Van Niekerk and Von Solms, 2010). However, the artefact level becomes more difficult to predict in cases where the different levels are in disequilibrium, and the degree of elasticity determines how long it takes before the system settles into equilibrium. This equilibrium is not achievable in an infinitely elastic system, but a completely inelastic system would always be in equilibrium (Van Niekerk and Von Solms, 2010).

In a security culture, the knowledge level is an obstacle to the elastic effect regarding the degree of elasticity. According to Van Niekerk and Von Solms (2010), the lack of knowledge hinders employees' willingness to act securely. The lack of security knowledge causes an infinite degree of elasticity in the security culture. It inhibits the artefact level from attaining equilibrium because the employees lack the means to supply the desired behaviour. Van Niekerk and Von Solms (2010) emphasises that a system with infinite elasticity does not align unless the underlying cause is addressed. If management wishes to see changes in the artefacts layer, the degree of elasticity needs to be reduced.

Van Niekerk and Von Solms (2010) conceptual model shows that the nett overall effect ISC has on an organisation's IS efforts depends on the strength of each underlying level. Moreover, how stable the culture is also depends on the alignment of the strengths of each level relative to the other levels. A culture where all four levels are stronger than the BL is thus the ideal culture for an organisation. In figure 2.3, all the nodes are stronger than the BL and are also perfectly aligned simultaneously, which is a perfect example of an ideal culture.

This framework will be adapted to study the effect a large-scale attack had on the information security culture in the organisation subject to our case study and how this attack specifically changed the culture.

Chapter 3

Methodology

In this chapter, the researchers will first explain what a literature review is, what review method we chose and why. This section will also describe how we carried out the review and a description of the literature demographics and organisation. The second part of this chapter will explain what a case study is and how it was conducted. The literature review will serve as a foundation for the case study by providing an overview of existing research on information security culture, allowing us to compare and contrast the results with existing theories and empirical evidence.

3.1 Review Methodology

According to the University of Edinburgh, a literature review is an academic analysis showing the author's knowledge and understanding of a specific topic (The University of Edinburgh, 2022). The goal of a literature review is to bring the reader up-to-date with current literature on a topic (Ramdhani et al., 2014) and create a foundation for advancing knowledge and facilitating theory development (Webster and Watson, 2002). The review is meant to allow the author to identify relevant theories, methods and gaps in currently available research by providing an overview of current knowledge (McCombes, 2023). However, it must also include the author's critical evaluation of the material (The University of Edinburgh, 2022). Ramdhani et al. (2014), state that a good literature review gathers information from many sources and contains either few or no personal thoughts in the analysis.

The goals of a literature review can be compiled down to four goals (Schwarz et al., 2007):

- to summarise prior research,
- to critically examine the contributions of past research,
- to explain the results of prior research found within research streams,
- to clarify alternative views of past research (not necessarily integrated together)

To understand how to perform a literature review, the paper "Guidance on Conducting a Systematic Literature Review" by Xiao and Watson (2019) was used as a reference. The paper was used to create a discussion within the group on what sort of review methodology would suit the research the best. The group were reasonably inexperienced in doing proper literature reviews and used the model within the journal to help guide us to our choice. The research paper by Ramdhani et al. (2014) was also of great help by providing us with a step-by-step approach to performing a literature review. In their research paper Ramdhani et al. (2014), they start by explaining what both a literature review and systematic literature is. They then explain the steps of a literature review and how to perform it and provide a template for setting up the paper.

Xiao and Watson (2019) provides a great explanation of the different categories of review methodologies one can find. Based on their explanation, we applied a descriptive review methodology to analyse the literature. The authors explain that a descriptive review methodology aims to find existing knowledge on our subject and argue if it answers our hypothesis (Xiao and Watson, 2019). One can find several methodologies within the descriptive category. However, we decided to apply the narrative review method as our primary approach when analysing the literature because it is the most common type of descriptive review and the least rigorous and time- and resource-consuming (Xiao and Watson, 2019). This review type fits well in regards to our research question, in addition to being a review type that is easily understandable for new researchers. It is further stated that narrative reviews are less concerned with assessing evidence and more focused on gathering relevant information that provides context and substance to the author's overall argument (Kastner et al., 2012, in Xiao and Watson, 2019). The authors further state that the data extraction process is informal and that the synthesis is generally a narrative juxtaposition of evidence.

3.2 Literature Search and Evaluation

3.2.1 Database Selection

Before choosing which databases to work with to identify literature, there are essential factors to consider that can impact the literature review's quality. One such factor is that the database must be trustworthy and dependable enough to provide us with literature we can use in our thesis. Some databases provide the users with filtering options that only show peer-reviewed articles presenting us with literature we know is trustworthy and dependable. Another factor to consider when deciding which database to use is the possibility of applying advanced search terms such as language and date filters and using boolean operators in the search query.

With the criteria presented above, we agreed on using Scopus, Senior Scholars' Basket of Eight and JSTOR as our literature-searching databases based on previous experience and recommendations from our colleagues. With the keywords previously identified, we can now start searching for relevant literature of good quality and reliable sources.

3.2.2 Exclusion Criteria

The initial search for relevant literature produced a large amount of literature, many unrelated to our topic. In order to reduce the amount of literature, we would have to look through and find the most relevant literature for our topic; the authors decided to add inclusion and exclusion criteria to narrow down the results. As stated above, if the database provided us with the option of only returning peer-reviewed articles, it would be chosen to ensure the quality and trustworthiness of the articles.

To narrow down the results, we applied the following exclusion criteria:

- Exclude papers written in languages other than English
- Exclude position papers, conference papers and reviews of papers
- Exclude papers published before 2010

These exclusion criteria, combined with our keywords and advanced search capabilities of the databases, will provide us with the literature needed to identify the research gap where our thesis will fit and whether the research problem is relevant and worth investigating.

3.2.3 Literature Identification

As stated in section 3.2.1, we filtered the results only to receive peer-reviewed articles; however, only one of the three selected databases provided that option, Senior Scholars' Basket of Eight. The rest of the searches were conducted according to our exclusion criteria.

According to Xiao and Watson (2019), using broader keywords in the search query will retrieve more detailed and inclusive results but will return more irrelevant articles. More precise keywords will, in comparison, improve the precision of the search but might result in missing articles. In exchange, they state that authors should balance the degree of exhaustiveness and precision (Xiao and Watson, 2019).

In the case of this thesis, the authors agreed upon using a combination of broad and precise keywords, thus having access to a large number of articles to choose from. The keywords we chose for this search were, and were combined by the use of boolean operators:

- cybersecurity
- incident
- attack
- effect
- culture
- information
- security
- systems

Scopus

Considering that one of our criteria is to exclude results written in languages other than English, the search query must be modified to meet the criteria. With that in mind, we added the publishing criteria to the query so that the final search term used was this:

1. TITLE-ABS-KEY (cybersecurity OR (cyber AND security) AND incident AND (effect AND culture)) AND PUBYEAR > 2009 AND (LIMIT-TO (LANGUAGE , "English"))
2. TITLE-ABS-KEY (cybersecurity OR (cyber AND security) AND attack AND (effect AND culture)) AND PUBYEAR > 2009 AND (LIMIT-TO (LANGUAGE , "English"))
3. TITLE-ABS-KEY (information AND systems AND security AND culture) AND PUBYEAR > 2009 AND (LIMIT-TO (LANGUAGE , "English"))
4. TITLE-ABS-KEY (information AND security AND culture) AND PUBYEAR > 2009 AND (LIMIT-TO (LANGUAGE , "English"))

The four searches resulted in a total of 2701 potentially relevant articles. However, due to search numbers 3 and 4 in the list above having most of the results, we decided to only look through the first page of these two searches. The final number of potentially relevant articles amounted to 58 articles across these four searches.

JSTOR

Below is the search queries used in JSTOR. However, as one can see, the searches do not include the date exclusion criteria in the query. Instead, exclusion criteria can be added

through the filtering options available on the website, where we excluded publications before 2010 and limited the results only to include journals and research reports. Additionally, we have decided to only do the two searches in the list below because the queries only retrieved the same results.

1. (((((cybersecurity) OR (cyber security)) AND (incident)) AND (effect)) AND (culture)) AND la:(eng OR en)
2. ((((information) AND (systems)) AND (security)) AND (culture)) AND la:(eng OR en)

These two searches alone provided us with 38785 potentially relevant articles. Considering that this massive number of articles would take too long to look through, we landed on checking the first three pages of each search. The final number of potentially relevant articles was 150 across these two searches.

Senior Scholars' Basket of Eight

Seeing that only Senior Scholars' Basket of Eight provided the option of retrieving peer-reviewed articles, that option was always checked when searching this database. The following search terms were used with the date range set between 01/01/2010 and 31/12/2022:

1. (cybersecurity or (cyber and security) and incident and effect and culture)
2. (information AND systems AND security AND culture)

As one can see, only two searches were done in this database because similar results were retrieved. The total number of results retrieved from these two searches amounted to 1017 potentially relevant articles; however, with search number two in the list above containing the most results, we decided to only look through the first page. In total, these two searches yielded 41 potentially relevant articles.

Ultimately, our list consisted of 248 articles, which would undergo a screening process to decide whether they could be used in the literature review.

3.2.4 Selection of Literature

As mentioned in section 3.2.2, we created exclusion and inclusion criteria to narrow the list of potential articles from 248 to a more reasonable number. To reduce the number of articles, we created a list consisting of four criteria that each of the 248 articles would have to go through. The criteria are as follows:

1. Remove duplicates
2. Remove articles with irrelevant titles
3. Remove articles where the abstract proved irrelevant to our research
4. Remove articles where full text was not available
5. Remove articles where the full text was out of scope for our theme

The first step is according to the list to remove duplicate articles found in all the searched databases. After a thorough look at the list of 248 articles, 15 articles were removed, thus leaving us with a total of 233 articles left to go through the next step. Based on the second iteration, we removed 28 articles based on irrelevant titles, leaving 205 articles left. In the third iteration, we aimed to remove articles where the abstract proved irrelevant to our research; this amounted to 27 articles, leaving us with 178 articles left for the fourth step. In the second to last step, we removed all articles where the full text was unavailable, even if the text could have been relevant to our research, which amounted to 11 articles. After

removing 11 articles in the fourth iteration, we had 167 articles in step five. In the fifth and last step, we removed all articles where the text was out of the scope of our theme, which amounted to 145 articles and left 22 articles for us to use in our literature review displayed in Appendix A.

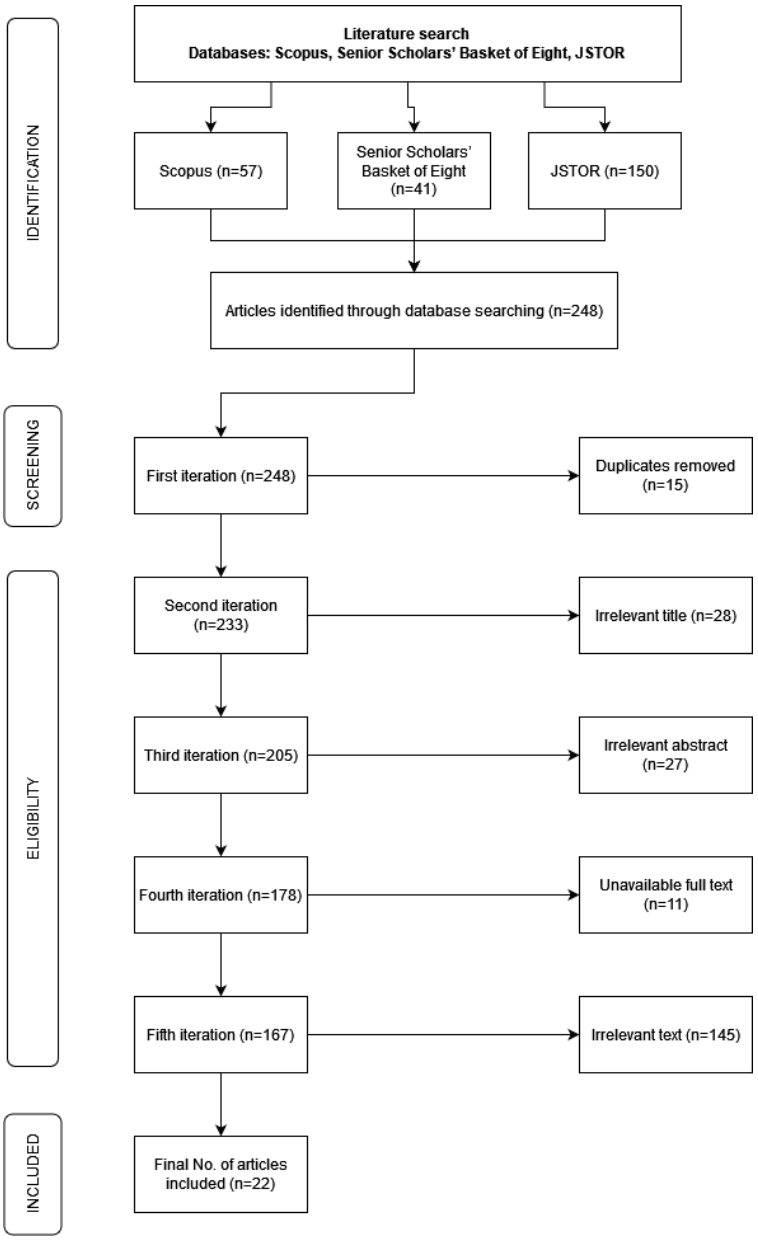

Figure 3.1: Flow chart presenting the inclusion process

Now that the literature collection and screening process is completed, the next step will be to break down each article and identify the vital information within them. As stated in section 3.1, the focal point of a narrative review is to gather relevant information that can provide both context and substance to the author's overall argument (Xiao and Watson, 2019).

While most of the literature used was found using the methods stated above, some literature was recommended to us by professors at the university after completing the review process. After discussing and analysing the articles, we concluded they were worth using as they explained concepts that provided more depth to the study.

3.3 Case Study

As mentioned in chapter 1, a case study into an incident will be conducted to investigate how security culture in an organisation works and how it gets affected by cyberattacks. This study will explore the culture of a Norwegian organisation operating in the private sector, which suffered a significant ransomware attack that cost them several million NOK.

Yin (2009) defines case studies as:

> an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.

Seeing that the definition proposed by Yin is rather tricky to understand, another definition has been suggested by Oates (2006), where he defines a case study as a study that focuses on one instance of the 'thing' that is to be investigated. The 'thing' referred to by Oates (2006) is, in this case, how culture in an organisation is affected by cyberattacks.

In order to address the research questions, a decision of whether to use a single case study or multiple cases needs to be made prior to any data collection (Yin, 2009). The author further states that a single case study is appropriate under several circumstances and gives five reasons to justify it:

1. If a case study represents the critical case in testing a well-formulated theory,
2. If a case study represents an extreme case or a unique case,
3. If a case study is the representative or typical case,
4. If a case study is a revelatory case, or
5. If a case study is the longitudinal case, i.e., studying a case at different points in time

While a single case study might be justifiable according to the five reasons above, Yin (2009) mentions that multiple case studies are preferred over single-case studies due to the analytic benefits from having two (or more) cases may be substantial. Furthermore, single-case designs require careful investigation of the potential case to minimise the chances of misrepresentation and to maximise the access needed to collect the case study evidence. The author also mentions that single-case studies are vulnerable, seeing that one will have put "all your eggs in one basket" (Yin, 2009).

Even though Yin (2009) recommends doing multiple-case studies over a single-case study, in this thesis, we will conduct a single-case study. In this case, a single-case study is justifiable under reason number five: longitudinal case as provided by Yin (2009). While there are more advantages to doing multiple-case studies compared to a single-case study, a single-case study allows us to get a deeper understanding of the subject in addition to being less time-consuming in comparison to multiple-case studies (Gustafsson, 2017).

3.3.1 Case Selection

Considering that we are looking into changes in culture due to cyberattacks, the target organisations would naturally be the ones that have suffered an attack in the past. The plan was first to have two organisations as the case participants and interview six candidates in each organisation. However, due to time constraints and difficulties in getting research candidates to participate, we decided against this and agreed upon a single-case study instead and interviewing ten people in different positions in that organisation.

Experiencing a cyberattack is a sensitive topic for many organisations, and seeing that many of them never go public due to fear of losing reputation, customers and other business-related

considerations. However, we knew there were organisations which have gone public with the attack they suffered, and it is these organisations which we are targeting for our study. That led to us creating the criteria below, which were used to find these organisations:

- Have suffered a cyberattack in the last couple of years
- Have made public announcements of the attack
- Have managed to rebuild their systems
- Have implemented changes regarding security throughout the organisation
- Is now operating as normal

Based on our criteria, different news outlets were searched to identify which businesses could be contacted. Emails were sent to those in charge of communication or others in high-ranking positions. Out of 11 emails sent, only two came back with a positive answer, but seeing that we are committed to a single-case study, we based our choice on previous studies and how much media coverage the attack received.

As stated earlier, we are looking to interview people in different positions as this allows us to investigate how security culture across professions in an organisation differs. The investigation allows us to examine how security culture in an organisation functions and how effective a cyberattack is on the organisation's approach to the different aspects of cybersecurity.

3.3.2 Data Collection

The best approach to study the effect a cyberattack has on an organisation and gather data is by conducting interviews, as it allows us to look at the chosen case within its real-life context (Oates, 2006). The author further states that the knowledge gained from studying this case might also be relevant to other situations. This approach is also supported by Myers and Newman (2007), where they stated that the most crucial data-gathering tool is qualitative research interviews.

Our goal is to understand how a cyberattack changes an organisation's overall culture compared to before the attack. Going in-depth into this instance allows us to obtain as much detail as possible on the culture before and after the incident so that it can be compared to indicate aspects of culture that organisations deem the most important.

3.3.3 The Qualitative Interview

Semi-structured interviews are the most used type within qualitative research in the information systems domain (Myers and Newman, 2007). In our quest to determine the effects of a cybersecurity incident on an organisation's culture for the case study, semi-structured interviews will be used to collect the necessary data. One of the main advantages of semi-structured interviews is, according to Kallio et al. (2016), that it facilitates reciprocity between the interviewer and participant and allows the interviewer to ask follow-up questions based on the participants' responses. Semi-structured interviews are also described as having incomplete scripts, necessitating the researchers' improvisation (Myers and Newman, 2007). DiCicco-Bloom and Crabtree (2006) further emphasises the improvisation and states that semi-structured interviews are organised around open-ended questions, with other questions emerging from the dialogue between the interviewer and the interviewee. This approach supports a more descriptive interview type, which can produce a detailed description of an event as the interviewees perceive it. Their views are then used to generate subjective understanding, and by using the perspectives of multiple individuals, one can arrive at a

comprehensive and multi-faceted description or conceptualisation. Through this conceptualisation, researchers can create interpretive understanding (Recker, 2013).

Interview Preparation

As the quality of the interviews depends on prior research, research into the specific company and the incident they suffered was done, as well as reading through the articles from our literature study. Kallio et al. (2016) explains that a semi-structured interview approach requires a certain level of previous study in the research topic area, and if no prior research is done before creating the interview guide, it affects the implementation and analysis of the data collected. The authors further state that an interview guide should not be followed strictly and that the main point of it is to offer a structure for the discussion happening in the interview (Kallio et al., 2016). In his article, Turner III (2010) explains that Creswell also supports this view by stating that flexibility is needed when asking questions and further states that the questions should allow the interviewer to dig deep into the experiences and knowledge of the participant to gain the most information from the interviews.

Conducting the Interview

While interviews should be conducted face-to-face, due to time constraints and the fact that the interviewees are based in different locations in Norway, we decided to conduct them through video-conferencing software. A technical test beforehand to ensure everything was in order was also done to ensure no technical difficulties occurred during the interview. To prepare ourselves further, we drew inspiration from McNamara's eight guidelines for the interview preparation stage. According to McNamara (1999), the first step is to conduct the interview in a setting with little distraction, while in our case, they will be conducted through video-conferencing applications.

Although McNamara (1999) places explaining the purpose of the interview second on the list, our approach was to address the terms of confidentiality instead, found in third place, and get consent to record the interview, even though we sent out a consent form, which can be seen in Appendix B. With that taken care of, the interviews always started with a couple of preliminary questions before moving on to the main questions. Considering that McNamara (1999) recommends not relying on memory to recall the interviewee's answers, we would regularly confirm that we were still recording in case of technical difficulties. Based on the semi-structured interview approach, follow-up questions were asked in case we missed a relevant point or if the interviewee mentioned something of interest. The interviews were successful, and we were able to interview the candidates seen in table 3.1. During the interview process, some questions were deemed unnecessary due to the questions providing little to no data. The interview guide can be seen in full in Appendix C.

3.4 Data Analysis

After each interview, the next step involved transforming the data from audio and video to a textual format. While converting raw data into textual data, the researchers were careful to add or remove words to improve the interview flow. The interviews had a lot of the classic vocal disfluencies, e.g., "like", "you know", "um", and "so", which were deemed irrelevant to the analysis and were promptly removed. While the transcribed interviews tell one story in a more condensed and simplified way, the researchers want to clarify that the actual events that happened were much more detailed and eventful than what the interview subjects might remember and can communicate.

Once the transcription process was completed, the researchers started coding the interviews. Coding is the process of analysing and reducing qualitative data to meaningful information

ID	Role	Years in organisation
P1	Employee	27
P2	IT Manager	7
P3	IT Teamlead	23
P4	Technical Staff	3.5
P5	Accounting Manager	15
P6	Accounting Officer	20
P7	Employee	30
P8	Marketing	23
P9	Digital Manager	10
P10	Employee	14

Table 3.1: Participant overview

by assigning labels or tags as units of meaning to either words, phrases, paragraphs or entire documents (Recker, 2013). According to various research papers (Azungah, 2018; Bingham and Witkowsky, 2021; Linneberg and Korsgaard, 2019; Thomas, 2006), coding can be classified into two categories: inductive coding and deductive coding. Inductive coding involves creating codes directly from the data, while deductive coding involves using pre-defined codes (Linneberg and Korsgaard, 2019).

To analyse and code the qualitative data, the researchers applied the thematic content analysis method and a deductive coding approach. Thematic content analysis is described as a descriptive presentation of qualitative data by identifying common themes in the texts provided for the analysis (Anderson, 2007) and for identifying repeating patterns in the data (Kiger and Varpio, 2020). A deductive approach to coding the data can help researchers apply theoretical or conceptual frameworks and help create codes based on the components of the theoretical framework being used and sorting the data into the predetermined theory-based categories (Bingham and Witkowsky, 2021).

We used the six phases proposed by Braun and Clarke (2006) as an inspiration to guide us through the thematic analysis process. While these six phases help guide us through the process, they emphasise that these are not rules and express the importance of applying flexibility so that they fit the research questions and data. The six phases are as follows:

1. Familiarise yourself with the data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

As stated earlier and in line with phase 1, a comprehensive reading of the transcriptions was done to ensure they were correct. As for phase 2, considering that a deductive coding approach can help apply theoretical frameworks, the information security culture levels found in section 2.3 were used as the codes in phase 2. While the four levels of information security culture were used as the initial codes, we later decided to categorise them according to before and after the attack had occurred. Braun and Clarke (2006) advises that researchers during phase 2 should (a) code for as many themes as possible, (b) keep relevant surrounding data not to lose context, and (c) data may fit into several codes.

Following an intercoder reliability approach, we coded the interviews separately to get each

Codes	Interview Extracts
Artefacts	There wasn't really any security training earlier.
Espoused Values	We've had an open culture of communication in my part of work.
Shared Tacit Assumptions	I hope the organisation soon realises that this is something we all need - in regards to password managers.
Knowledge	I realised that backups were necessary since there weren't any backup systems for Apple computers, like I work with.

Figure 3.2: Qualitative data coding

researcher's findings, which were then processed together to check if the findings were similar. Intercoder reliability, or ICR, is a numerical measure of the agreement between different coders regarding how the same data should be coded (O'Connor and Joffe, 2020). The coding process starts by developing a coding frame containing the analytically essential data. The coding frame, usually a list of codes, may be organised according to higher-order code categories accompanied by definitions and example data extracts (O'Connor and Joffe, 2020). The codes are gathered into themes or narratives that are interpreted according to the relevant theory after completing the coding process (O'Connor and Joffe, 2020). They further state that, after the development of the coding frame, it is systematically applied to the data, which are then broken down into smaller parts and given specific labels that identify their meaningful content for analysis.

Figure 3.2 depicts a small extract of how we coded the data based on the four levels of information security culture. To code the data, we gave each information security culture level a colour to distinguish between them; the culture levels after the attack were given a lighter colour. For each interview, we would carefully mark statements from the candidates that we felt would fit into one of the categories.

While most of the data will be coded into a specific topic, there is also a chance that it might fit into other codes. This makes it so that some of the information might be used on different topics as the topics are very interlinked; for example, artefacts are connected with shared assumptions and knowledge.

With all the findings collected in a separate document, we could move on to phase 3. During this process, we analyse our findings with our codes to see how they can combine to form an overall theme. Braun and Clarke (2006) suggests creating a thematic map to sort the codes into different themes. However, we instead used a table to visualise the themes we found, as seen in table 3.2. Based on the analysis, the collection of themes in table 3.2 serves as the candidate themes extracted from the data. Although we used Van Niekerk and Von Solms (2010) four levels of ISC as the initial codes and separated them into before and after the attack, in phase 3, they were combined to form an overall theme instead.

Table 3.3 gives an overview of the theme that was identified in both phases 4 & 5. While phases 4 & 5 are combined in this table to distinguish between the two phases, themes identified in phase 4 but later removed in phase 5 have been struck through to indicate their removal. The merging of the two themes in table 3.3 was only done due to space restrictions.

According to Braun and Clarke (2006), phase 4 involves refining the themes found in phase 3, and in this phase, it will become clear that some themes might not have enough data to warrant a different theme, that two different themes can be combined instead or that some

Phase 3
Artefacts
Espoused Values
Shared Tacit Assumptions
Knowledge
Organisational learning
Awareness and training
Personal interest
Leadership response
Trust
Policy
Policy compliance
Contradictory statements
Subcultures
Variations in professions
Overcompensation after the attack

Table 3.2: Theme creation based on codes

themes can be divided into separate themes. During this phase, one rereads the collected material for each theme from phase 3 and considers whether they form a meaningful pattern (Braun and Clarke, 2006). All the themes from phase 3 were kept, in addition to adding new themes which reflected the data that we had.

Braun and Clarke (2006) explains that in phase 5, one must further "define and refine" the themes from the previous phase, which the authors mean finding the "essence" of what each theme is about. During this refinement process, we identified some of the themes found in phase 4 that did not fit into the "story" we were trying to tell and several main themes and sub-themes were also identified. The final list of themes and how they are sorted can be seen in table 3.3.

Finally, phase 6 details the final analysis and the write-up of the report by providing sufficient evidence of the themes within the data (Braun and Clarke, 2006). We separated the themes in Table 2 and wrote about each theme using the interview data. This way, we can inform the readers of this paper on how the interview data relates to each theme. Braun and Clarke (2006) states that arguments concerning our research question using the data must be made, which can be found in chapter 5, combined with existing literature.

3.4.1 Reliability and Validity

Oates (2006) states that to corroborate one's findings and enhance validity, one should use more than one data generation method, also called method triangulation. While this method is more time-consuming due to producing more data, it will likely improve the quality of one's research by allowing the researchers to gain several ways to answer the research questions (Oates, 2006).

Seeing that we are using both interviews and a literature review to produce data, method triangulation allows us to corroborate the findings from the interviews with the data from the literature review and increase the confidence of our findings if the data shows any consistency across these two methods (Oates, 2006).

3.5 Research Design Limitations

Our research methodology is anchored on collecting data from individuals who have undergone a cyberattack in their respective organisations. Despite this, we acknowledge that there may be some restrictions regarding the data we can acquire. In our case, we ask the participants to reflect on the events before, during and after the attack and recount them as detailed as possible. Since memory is highly fallible (Green, 2009), the participants might recount the events, which causes inaccuracy and affect the collected data. Myers and Newman (2007) have also addressed the potential problems that might occur in qualitative interviews, the applicable pitfalls to be aware of for these interviews are listed below:

- Artificiality of the interview - asking a stranger to give opinions under time pressure
- Lack of trust - the interviewee may choose not to divulge information that they consider to be sensitive and can result in incomplete data gathering
- Lack of time - interview length can mean that the data gathering is incomplete or the creation of opinions under time pressure
- Ambiguity of language - the questions may be unclear for the interviewees, and it is not always clear that they understand the questions they are asked

3.6 Ethical Issues

Seeing that the qualitative data were collected using interviews means that we would be recording the participants and collecting various information about them. Since we are processing personal data in this research project, we must ensure that the planned processing is per data protection legislation. Sikt, or Norwegian Agency for Shared Services in Education and Research, provide a form researchers can use when processing personal data in a research project, which they must have received at least 30 days before the data collection begins.

Our Sikt application was approved with reference number 723826. The process of filling out the form included creating the interview guide and a consent form, seen in Appendix B, for the participants, which they needed to sign before starting the interview. Processing and storing personal data was all done in accordance with what was provided in the notification form.

We encountered some complications while trying to find an organisation willing to provide us with interview candidates. A list of the potential organisation was made, scouring through different news outlets trying to find potential organisations. After sending several emails to different companies with either negative answers or no answers, we eventually found an organisation willing to cooperate with us. All the organisations we tried to interview had suffered an attack in the last couple of years. However, some might have been covered in the media extensively or had not released any information about the attack. An implication that we were aware of and had taken into consideration.

Phase 4 & 5	Theme Type
Artefacts	Main theme
Password Policies and Authentication	Sub-theme under AF
Security Training and Awareness	Sub-theme under AF
Communication Channels and Information Dissemination	Sub-theme under AF
Infrastructure Setup and Security Measures	Sub-theme under AF
User Engagement	Sub-theme under AF
Espoused Values	Main theme
Rigid Control and Centralised Management	Sub-theme under EV
Attention from Leadership	Sub-theme under EV
Security Measures and Policies	Sub-theme under EV
Shared Tacit Assumptions	Main theme
~~Shared Tacit Assumptions Before the Attack~~	~~Sub-theme under SA~~
~~Shared Tacit Assumptions After the Attack~~	~~Sub-theme under SA~~
Mandatory Security Training	Sub-theme under SA
Cultivating a Blameless Postmortem Culture	Sub-theme under SA
The Impetus for Increased Security Training	Sub-theme under SA
Knowledge	Main theme
~~Personal Interest~~	~~Sub-theme under KN~~
~~Awareness and Training~~	~~Sub-theme under KN~~
Organisational Learning	Main theme
Leadership Response	Main theme
Trust	Main theme
~~Policy~~	~~Main theme~~
~~Policy Compliance~~	~~Sub-theme under Policy~~
~~Contradictory Statements~~	~~Sub-theme under Policy~~
Subcultures	Main theme
Variations in Professions	Sub-theme under Subcultures
Overcompensation After the Attack	Main theme

Table 3.3: Final themes identified after phase 4 & 5

Chapter 4

Findings

This chapter presents the findings obtained from the comprehensive examination of information security culture within the organisation. Through an in-depth case study analysis using a thematic content analysis method, the study aimed to explore the various aspects of information security culture and its impact on an organisation's overall security. The interviews were conducted with ten different participants in an organisation attacked a few years before this research was planned. Table 3.1 in chapter 3 gives an overview of the participants interviewed. These findings offer the readers essential observations into the organisation's information security environment and call attention to areas of improvement. The findings will add valuable data to existing research on information security culture and provide recommendations for improving security culture and promoting a secure environment within the organisation.

4.1 Changes to Artefacts

Artefacts are what actually happens in an organisation according to Van Niekerk and Von Solms (2010). They further state that day-to-day tasks are impossible to do securely if an employee lacks the necessary knowledge on information security practices. Such artefacts are an essential aspect of improving the security culture in an organisation as it directly affects the other ISC levels. Thus the changes to artefacts in the aftermath of an attack can provide valuable insights to organisations on what is considered essential artefacts for someone already harmed.

4.1.1 Password Policies and Authentication

The organisation swiftly enhanced their password policies and authentication measures after realising they had insufficient policies and weak authentication methods. P1 provides details on the implementation process:

> So when the network came back up and stuff, they started implementing 2FA requirements on everything, you know, and these authentication apps became mandatory.

While some may find the updated password policies frustrating, most participants recognise their necessity and have taken steps to further enhance their account security by implementing two-factor authentication on all accounts. P7 summarises the changes as follows:

> Passwords, I believe, are something that ranks high on the list of frustrations for many people. Some systems require a new password every other month, which makes it even harder to remember. I can't disagree with that. It's a hassle, and

> sometimes you have to log into Google twice during a workday. And that's not the only thing—you can hardly start a program today without having to log in.

However, P1 specifically showed more dissatisfaction with the improved password policies and authentication methods and compared it to being in prison, stating:

> If you imagine entering a building, I think it should be enough to unlock the front door and have access to all the rooms in that building. The situation is such that you have to unlock the front door and all the other doors inside the building as well. It can be compared to how a prison works and it feels a bit like that, all the doors inside the house are locked too, and it seems unnecessary. A master key and let us come in and work in peace, that's my wish.

Furthermore, P3 reported a significant level of employee dissatisfaction with how the implementation of 2FA was carried out, leading to frustration among staff members:

> There was a lot of pain around 2FA (two-factor authentication), and there is a lot of pain around how long a Google mail session should last. It almost caused riots for a period when they tightened the requirement to log in again with 2FA once a day.

Considering the implementation of the new password policies, P3 states that the policy clearly says not to reuse passwords and that they must be complex. However, they are not helping the employees to handle this change the new policies come with. P3 express their concern regarding this change with the following statement:

> I find that a bit painful because we're asking people to do something that's strictly impossible without tools.

When asked about the effectiveness of password managers in complying with new password policies, the participants expressed varying views. While some were uncertain or unfamiliar with password managers, others used them voluntarily. P1 stated that they had subscribed to a password manager service due to their experience with technical systems that required several passwords. Other participants disclosed that they maintain their passwords written down in a notebook. P6 also have their passwords in a notebook, but further states:

> I have the most important passwords in my head, and then there's something called "forgotten password," which is quite handy.

In that regard, P4 highlights the usefulness of password managers as tools that can aid employees in effectively managing the new password policies:

> I generalised the thought of having a password manager with a metaphor about employees needing more crutches to stand on. I hinted at it earlier, but it hasn't been taken very seriously in our organisation.

However, when asking P2, the IT manager, about password managers and if it will be implemented in the future, they stated the following:

> We don't have any plan for it, but it has been discussed before. At a technical level, we do use it, but currently, there is no direct plan to implement it. I know the question has been raised before.

P1 has suggested switching to biometric authentication due to their dissatisfaction with the new password policies. They explain that biometric authentication would be a better option:

> I think that there is something that would have been a way to make things easier. [...] It's much easier to just put your finger on a button or look into a camera to log in, rather than dealing with those damn passwords all the time. Especially

> if there has to be a password for every door in this house. That is probably my suggestion if something better were to be done, to make handling security easier.

4.1.2 Security Training and Awareness

Before the attack, security training was not given the necessary attention and user awareness was not considered a top priority. However, the incident caused a shift in perspective, highlighting the critical role of security training. Particularly, P1 stresses the insufficient training that was in place before the incident:

> The security training before the attack and what has changed. It's something I can't remember there being so much emphasis on before the attack. Of course, there has been some focus on it, but I haven't felt that it was a highly prioritised issue. It has probably been prioritised from the IT side and such, but as a user, it hasn't been a topic that has had a strong focus, at least not in my experience.

P3 also supports P1's statement and further elaborates on how it was:

> The security training before the attack, well, it wasn't very extensive. Much of it was hidden in an ICT (Information and Communication Technology) regulation that not many people read.

Several participants, including P6, support the statements made by P1 and P3 regarding insufficient security training before the attack. P7, who has been with the organisation for the longest time, mentioned receiving some emails about computer viruses during their earlier years with the company, but this does not negate the fact that there was a lack of comprehensive security training. P6 could not remember receiving training, reinforcing the claim's validity. While P7 has been with the organisation for the longest, P4 has been with the company for the shortest and claims there might have been some conversation about security during onboarding.

While no training existed before the attack, everything changed in the months after the attack. P2 explains the training measures they implemented after the attack:

> We have implemented a training program where users receive occasional emails with small courses, and in addition to that, we have an intranet that is utilised. If there are specific events or matters that our users need to be aware of, we have a push channel on our intranet where we share information. Furthermore, we have developed a portal along the way where general security information is provided. So those are the main channels. Additionally, we also have user guides and other resources available. So there are several different channels in place.

According to P2, the security training program was developed as short courses because previous experience showed that employees do not read long user manuals. P2 gives additional reasons for choosing short courses over the more comprehensive user manuals or more time-consuming workshops:

> The majority only read the first three lines and then they get tired before reaching the essence. And setting aside time for one or two-hour courses intermittently doesn't work well in the situation we're in.

The effectiveness of the training program is viewed differently by the participants. P3 believes that the current training is appropriate but suggests a gradual increase in difficulty. P6 and P9 believe it successfully imparts knowledge about security to employees, while P4 considers it too fundamental and prefers customised training.

4.1.3 Communication Channels and Information Dissemination

As previously stated, P2 mentions the implementation of the Intranet and security channels after the attack, but only some employees agree that was enough. P1 suggests that meetings or workshops would help them learn more:

> If we could have conducted some workshops and such, I believe it would be the best way to learn, raise awareness, and ensure that everyone is on board, most importantly. Anyone can simply skip over workplace information they don't feel like reading, but it's not as easy to avoid an obligatory workshop on IT security, so to speak.

This statement is also supported by P7, where they state that physical IT at the location of work would be a significant improvement:

> Yes, that's true. I would really like to hear and see someone who was in our premises and could have given some presentations and talked about it, physically present. The courses we received via email after the attack are very informative, but I believe we could have become even more aware of the situation if we had a local IT department.

On the other hand, P1 suggests that the information they are now receiving is much better than previously and thinks the organisation handled it professionally:

> As mentioned, there wasn't much focus before, but afterwards, there has indeed been a lot of emphasis. There has been a significant amount coming from central IT, and I found the information to be very good. I feel that they central IT have kept us well informed, and I have felt secure regarding personal data. So, in my opinion, they have handled this in a very, very professional manner from central IT when it first happened.

4.1.4 Infrastructure Setup and Security Measures

As mentioned previously by other participants, the infrastructure and security measures in the organisation were almost nonexistent or severely aged before the incident, to the extent that there was little to no security training. P3 describes his view on security in hindsight:

> In hindsight, it is crystal clear that with the state the setup was in, it was only a matter of time before something happened.

P3 offers a comprehensive report of the consequences following the attack, as the organisation had to implement substantial modifications to its infrastructure. However, other contributors were unable to provide extensive details regarding the incident:

> The most noticeable thing is, of course, what happened to the on-premise setup that the IT-department is responsible for. It had to be rebuilt from scratch with backups. The rebuilt infrastructure was designed with a completely different level of security compared to before. The old infrastructure showed signs of ageing, while the new one was built based on a rather paranoid mindset at the time. As a result, a lot of measures were implemented to address the most paranoid scenarios.

4.1.5 User Engagement

P1 acknowledges an increased focus from the IT department but points out that security is not essential in their experience, as mentioned in section 4.1.2. Despite the organisation's significant strides in security training and awareness, there remains a need to address other security considerations, particularly user engagement. An effective method proposed by P2

for gauging user awareness is conducting simulated phishing emails. This approach can be valuable in enhancing user engagement:

> Yes, we test by conducting activities such as sending phishing emails. So that's mainly the area where we test the users. This is something new since the attack.

This is further elaborated on by P5, where they were asked if they could be used as the sender of the fake e-mails to test how the users would react to such e-mails. Which resulted in the participant receiving phone calls and e-mails from users about the e-mail, suggesting raised awareness:

> But afterwards, more of those videos and questions came up. I was asked if they could use me as the sender of fake emails to see if people would click on the links. I found that to be very useful. Some people called me, and others sent emails asking if it was true that I had done this. There are probably many who have clicked on that link and received a message saying it wasn't a good idea. I think that has been great. It makes people more aware of who is sending emails and why, and so on.

In addition, although some participants have mentioned a lack of user engagement, P1 has reported increased engagement:

> I have even heard of people on placement who are requesting the courses if they haven't received them in time. There has been a shift in the security culture throughout the entire organisation.

However, some other participants suggested that having a physical person with knowledge about security to talk to would be more beneficial for the branch offices where they were situated, as P7 mentioned in section 4.1.3.

4.2 Changes to Espoused Values

While espoused values may be explicitly communicated and publicly promoted, their accurate alignment with individuals' or organisations' actual behaviours and practices can vary. Notably, there can be a discrepancy between the stated values and those demonstrated in practice, often called enacted values. Espoused values play a significant role in shaping the identity and culture of individuals and organisations. In the case of this organisation, they can serve as guiding principles, influencing decision-making processes, shaping behaviour, and establishing expectations for employees and leaders.

4.2.1 Rigid Control and Centralised Management

The espoused values in the organisation experienced changes after the attack, and one of those changes was more centralised management and much stricter control of systems and apps. P7 discusses the changes they experienced:

> If we're talking about the corporate level, I must definitely say that we have seen a change since the attack. Everything has become much stricter, and it seems like the technology/IT department has a completely different focus on the subject after the attack than they did before. There can be no doubt about that.

Furthermore, P6, an employee from a branch office, discusses how IT works and how centralised it has become.

> We don't have any IT expertise at the service centre; it is centralised in Oslo, and they can't assist everyone at once.

This is also discussed by P1, an employee who showed higher than average IT interest, where they discuss how previously they were allowed to do a lot more regarding computers and systems. Now it has become more rigid and centralised:

> Perhaps it has become more rigid. In the past, I was allowed to have my own computer because they knew what I was doing, and I think they saw that I took security seriously, so I was allowed to be a local administrator on my own computer. I am no longer allowed to do that. It's a specific thing that no one is allowed to do anymore. Everything needs to be centrally controlled in relation to such things.

4.2.2 Attention from Leadership

There was also understandably a severe change in how leadership viewed security and how their values regarding the topic saw a drastic change. Previously, they had no involvement outside of hiring a Chief Information Security Officer. P2 addresses this:

> Are you referring to the overall management here? Yes, there's no doubt that it has gained more attention on the agenda, even among the leadership, compared to before. It reaches all the way up to the board, for that matter, where reporting on how we're doing has changed significantly. It goes up to the corporate management and the board. No matter how you look at it, it's the top management that ultimately conducts risk assessments and decides what is acceptable and what is not. But yes, there's a completely different focus now, although it also needs to be maintained. It's an area they would prefer not to spend their time on, as they would rather focus on running a successful business. But that's how it works.

While the participants that were centrally located reacted to the changes as very positive and understandable and, in general, did not have many concerns, there were different opinions from the branch offices, where several participants addressed the lack of communication from leadership as well as concerns about their voices not being heard. P7 addresses this:

> Yes, there was a lack of information, and I believe many of us felt that our voices were not heard. The image archive in a newspaper may not have seemed important to some, but for us, it was actually quite significant. It had a great impact, perhaps more than we initially thought. Some of us were more dependent on it than others.

This is also addressed by P10, where they suggest that the leadership has responsibilities above what employees do when it comes to knowing about security and that they need to realise the importance of their actions and lack of knowledge might have:

> Support from leaders is definitely something that is necessary. Leaders need better knowledge about security so that the rest of the employees can contribute to a better security culture. I don't think the leaders are aware of the legal responsibility they have regarding GDPR and data processing. It's important for those who travel to Russia, but what about those who go to the courthouse - there are more of them. Should they use mobile data or Wi-Fi or Wi-Fi with VPN at the courthouse? Some are not aware of what VPN is; they think it's a login service.

4.2.3 Security Measures and Policies

Overall, the employees in the organisation had little difficulty adjusting their values to align with the new security narrative, as indicated by P5's statement:

> No, I don't think I can say that. It was very strict when we resumed operations, and I believe that was the risk of uploading something with a virus that could cause further errors. It would have been catastrophic. I think it was necessary for it to be strict and for us not to take any action until we were certain.

However, there were also some concerns towards specific new policies and processes. P2 discusses one of these concerns:

> It wasn't straightforward to introduce client monitoring, to put it that way. It involved simple things like knowing your whereabouts at all times. As long as you're connected to a network, we can determine your affiliation and such, but it's not as easy to navigate as it's portrayed in TV shows. However, there's still a considerable amount of information being stored. So, there was some processing required before they considered it a wise decision. It was definitely not a straightforward process.

Another employee, P3, further elaborated on this, discussing the implementation of EDR (Endpoint Detection and Response) and the concerns it brought to the union representatives:

> We had a big discussion about the implementation of EDR (Endpoint Detection and Response). The union representative was involved, and there was a lot of fear and uncertainty surrounding the implementation of that measure.

Although there were inadequate security measures before the attack, P5 acknowledges that some measures were in place:

> What we have always had as a security measure with us is that if emails come in requesting urgent payments, it should never go out without being verified by both me and the sender on the phone. We have also had the same policy on the supplier side, where we never pay an invoice unless we are completely sure that it is a correct invoice and that it comes from the right place. We have always had these kinds of security measures.

Another sparsely discussed aspect was the importance of investment into security and if leadership saw the importance of it. P2 uses a metaphor to discuss its importance relating it to an insurance policy:

> The biggest disadvantage of security is how much it costs. It's like home insurance; it's just in the way, costing a lot of money throughout the year until something happens, like a fire, and then it's good to have after all. It's a similar situation here, it's like an insurance policy.

While there were not many policies in place at the time of the attack, P10 explains:

> There was actually quite a lot going on (policy wise) before this happened, but (the attack caused) a pretty significant shift in pace (in implementing the new measures and policies).

4.3 Changes to Shared Tacit Assumptions

The organisation's shared tacit assumptions are an aspect that can be difficult to change as they are primarily unspoken and may be unconscious and require an organisation-wide change where the majority of the employees need to be of the same mindset when it comes to performing tasks. As such, in an organisation of this size with branch offices, the assumptions some leaders think are correct are only sometimes shared with employees, for example, in a branch office. This can be observed in a comment by P7:

> I believe that for most people, their attitude towards data security is: "This doesn't concern me." It's like saying, "That's something for the tech people to handle." Since we don't have an IT department in our office, our attitude is more like "Out of sight, out of mind".

This assumption is also shared by P1 in section 4.1.1, where they state that the new measures give them the same feeling as being in prison and that they would rather be without them so that they can do their job.

However, other participants contradict these statements and emphasise how successful the new security training has been and how it has raised the employees' awareness in general. P6 further elaborates on the matter:

> We have become much more aware of it than we were before. We have become more conscious of data breaches, cybercrime, and similar things than we were before, at least in my case.

P4 also shared that the company had trust in employees not performing malicious tasks that would harm the system, for example, hacking into it. They further state the importance of policies and routines:

> I'm not sure, but the thing is that we follow the established procedures. There is nothing preventing me from exposing secrets in production right now, for example. It's possible to do it; I don't know if there are mechanisms in place to address that. I could probably hack into it, so the routines that are set to follow up on this become important.

4.3.1 Mandatory Security Training

All participants reported receiving the training program via email. However, there were discrepancies in their accounts regarding whether the security training was compulsory. P7 asserted that the training was mandatory for him and his colleagues, and they completed it because they had no other option. P1 also attested to the mandatory nature of the security training, stating:

> Attending the security training was mandatory, so it wasn't just a suggestion, it was a requirement.

However, P4 contradicts their statements and says that they have not faced any consequences for not doing them, which indicates that there are no clear policies on whether or not the training is mandatory:

> I've started receiving some emails and security training courses. I glanced at it earlier, it's about secure domains, HTTPS, and whether I should click on this link and things like that. I haven't completed the course yet, I just checked it out earlier, and I haven't faced any consequences for not doing it, so I don't know how the follow-up on that is.

4.3.2 Cultivating a Blameless Postmortem Culture

Another new addition to the values in the organisation was the ability to communicate openly without worrying about receiving blame, and P3 confirms this:

> We have had a communication culture that has been heavily influenced by openness, at least in my part of the world.

P3 further elaborates on the implementation of "blameless postmortems" as a new way of communicating:

> We value transparency, and it's important that it's safe to admit making mistakes. We have what we call "blameness postmortems," primarily focused on availability and that side of the world, but we carry the same culture when it comes to information security as well. It's human to make mistakes, whether it's a sysadmin who may have made an error or someone who clicked on a link in an email that shouldn't have been clicked. We need to maintain that culture throughout. Speak up, talk about it.

4.3.3 The Impetus for Increased Security Training

As mentioned in section 4.3.1, there were varying opinions on whether the security training program was mandatory. When asked if incentives could motivate employees to complete the training program, several participants mentioned that incentives should not be necessary for the employees to complete the training, and P6 states explicitly:

> I believe that as an employee, you should do your best to contribute to the success of the company.

On the other hand, when asking P4 the same question and providing them with examples of possible incentives like badges or titles, they state this:

> Well, it's certain, I mean people are really fond of badges, research clearly shows that, so it's definitely a great incentive in my opinion.

Contrarily, P2 is unsure if incentives would have enticed the employees to increase their knowledge but mentions that explaining why also does an excellent job.

P7 agrees with the statement from P6 and summarises it as such:

> Ideally, you shouldn't need either an ice cream or a carrot to complete them. It's a continuous process that you have to keep up with all the time. One should actually be grateful for having access to these courses.

P10 is also in agreement with P6 and P7 and elaborates:

> No, I think the best motivator is to create a strong knowledge layer throughout the company.

Other participants mentioned that knowing they can get inflicted by a cyberattack makes them more aware of the dangers associated with such attacks and motivates them to be more careful. As mentioned in 4.1.3, workshops on security and a person knowledgeable on cybersecurity and IT also acts a motivator to raise the knowledge level across the organisation, which the following statement by P7 also outlines:

> Yes, I believe that people would probably have taken it more seriously if a person had spoken to them instead of just receiving a questionnaire that they are expected to go through and mark as completed. It leaves little room for the opportunity to ask questions or provide comments when it is presented in that manner.

4.4 Changes to Knowledge

Knowledge is mentioned as the 4th level of ISC in Van Niekerk and Van Solms' model, and in the case of this organisation is a level that was found severely lacking before the attack. As mentioned in 4.1.2, the participants mentioned that there was close to no awareness training, which will severely affect employees' knowledge of security. P2 discusses the importance of establishing a baseline level of knowledge among all employees and users:

> I can't think of anything off the top of my head, but what is perhaps most important is the competence of everyone at the right level. It's clear that our users need a different level of competence and awareness compared to what we do. It's two different worlds, but ensuring that our users are reminded of this from time to time to keep it somewhat fresh is important because it's incredibly easy to fall into the belief that everything is safe and fine because nothing is happening.

After the new awareness training programs were implemented, as mentioned in 4.1.2, the organisation saw a change in employee knowledge levels. P1 expresses some of their new knowledge:

> Before, maybe the personal and work-related aspects would overlap and such, but now I absolutely don't install anything that I'm not 100 percent sure I need for work. That applies to both my Mac and the iPhone I use daily for work.

This increase in knowledge is also supported by P9, where they discuss the threat of ransomware:

> Yes, I must say. I have become more aware of what kind of industry it actually is and how well organised it is. It's not just some fools sitting around fooling around individually, but there are actually large digital factories, as far as I understand - many of them from Russia.

However, it was revealed that a few employees lacked knowledge when asked for their opinions on the current level of security. P6, in particular, seemed disinterested in the topic:

> No, I don't think I'm capable of answering that. To me, it seems quite secure compared to how it has been before. I'm not sure if I'm the right person to answer that.

While one worrying thing is that P4 addresses the way of learning as passive and that they gain knowledge by gaining a baseline by things one hears or does. While not necessarily negative, it highlights that some employees do not get enough targeted security training:

> Now I'm a bit naive here, but from my perspective as someone who doesn't have in-depth knowledge in this area, it seems like there are many recurring things, and you hear about them and gather a sort of baseline for a knowledge base on what's smart to do or not smart to do, or what to be aware of, for example, when setting up a firewall somewhere, you just need to allow the traffic that should be allowed through, and things like that. It's basically just wisdom from experience, work experience, and informal conversations.

4.4.1 Organisational Learning

What new essential aspects does the organisation consider that they did not before? Another critical factor is the organisational learning that took place during and after the attack. When asked about the changes in security measures, P3 explains:

> So what has changed since then is firstly that we received a fairly thorough security training during the attack for entirely natural reasons. Secondly, a digital security training platform has been introduced afterwards. A lot of the work on awareness-raising and training of developers and more advanced users happens largely through taking responsibility for their own solutions.

Another employee also addresses this when discussing how the attack's aftermath went and how the security chief addressed the company. P1 describes the meeting:

> The security chief gave a very good presentation to us in a company-wide meeting where everyone was present, and we learned a lot. Of course, one could say that

> it went in one ear and out the other, as it was a bit technical, but I still believe the impact is that people have become more aware of security, and combined with the training, it seems to be effective. At least for me.

The IT department's increased emphasis on security has resulted in significant changes, including more extraordinary stringency measures, as noted by P7:

> If we're talking about the corporate level, I must definitely say that we have seen a change since the attack. Everything has become much stricter, and it seems like the technology/IT department has a completely different focus on the subject after the attack than they did before. There is no doubt about that.

Many of the participants mention the strictness of the new security measures. In a question about the changes, P1 describes some measures related to users:

> But now there is an absolute stop and we can no longer have any shared users. So when we lend out a PC to someone who is placed here for 2 weeks, a user must be created for that person, and they are not allowed to use a shared user account that we used before. Everything is personal now.

P2 describes a new way of testing employees by sending them phishing emails when asked for more details about specific measures:

> When we test, we primarily focus on the area of connection, for example, when sending phishing emails. This is something new that we're testing after the attack.

The most occurring topic when asking the participants about changes is the new courses they go through. P7 describes the course:

> What I have noticed the most is the increased awareness of data security. We have received numerous emails and information about data security, and especially a good amount of training courses, which we receive regularly. You receive an email with a course or questionnaire you must go through, and this provides continuous awareness and education on what you should know.

The organisation gained valuable insights from the attack and swiftly implemented stricter security measures. Additionally, they rolled out a comprehensive employee training program on security protocols.

4.5 Leadership Response

Top management's viewpoint on security saw drastic changes after the attack, as seen in section 4.2.2. However, they also supported their employees during the attack with regular updates on the progress during this period, as explained by P1:

> As for the first thing that happened, of course, it was regular information through a one-way channel. [...] The CISO gave us a very good presentation on what has happened and the progress they are making, in a meeting where all employees were present.

P10 also confirm the statements by P1 and explains:

> (Top management) were very quick to provide information about what they knew and didn't, and what they were working on to restore the system.

One participant stated that even though the attackers may have stolen personal data, they still felt safe due to how it was handled. Other participants also mention that top management has kept them very well informed and that they have handled the attack professionally. P2 also explained that cybersecurity and its importance had gained significant attention

among the employees, top management, and the board. P3 explains that one of the essential decisions top management made was:

> But the most important measure in the organisation was probably (implementing) the digital security training platform that all employees are required to participate in.

P6 also praises the introduction of the training platform and states:

> The company has done a tremendous job of teaching us about security, what kind of links to click, what to look for in fake emails, and everything like that.

4.6 Trust

A common denominator in many interviews is the confidence the interview participants place in the IT department or the "IT-guys" as they have been called. P1 explains that even though they are frustrated at some of the implemented measures, they think highly of them and the job they are doing:

> That is highly commendable, and one understands that Rome wasn't built in a day. I know they are working tirelessly down at Central IT to improve the systems and do a good job. I have confidence in them, even though I may get frustrated and annoyed with things, it's not directed towards them.

In conjunction with P1, P7 also places much confidence in those who handle security to ensure the organisation is secure:

> I rely on those who are responsible for data and security to have the necessary knowledge and to set up the necessary security in the systems we use.

As a member of the technical staff but not directly involved with security, P4 also rely on the employees responsible for security to ensure they are protected, but states they provide support when necessary:

> I trust those who handle security in the organisation to know what's best, and we do our best to follow the procedures or address any vulnerabilities that may arise together.

As the accounting manager, P5 stated that they did not have any additional backup solutions but that they relied on the IT department to handle that for them:

> But IT is in charge, and I would assume that they have equally good, if not better, backup solutions.

P6 explains that since they lack general computer knowledge, they place a good amount of confidence in the "IT-guys":

> I'm not an IT person, so to speak, so I'm very clumsy with those things. We're the type of people who need everything explained in simple terms. Ideally, we'd like IT to do things for us, and that's fine.

4.7 Subcultures

Since the organisation in our case study has many branch offices besides the main office, we quickly discovered that the organisation had several subcultures within these branch offices. Whereas the main office might have some thoughts on security, the branch offices might have similar views but differ on some values and knowledge. This gets addressed by P3, where he explains the difficulty of having branch offices:

> Yes, well, firstly, we are organised somewhat sub optimally. As I mentioned, we have a sister company, and in terms of security, that's not a good solution. This was made very clear to us during this attack. An attacker doesn't care at all about how we are internally organised. That is probably the most glaring issue. Also, it's important to note that we are not there yet, and we will never reach the point of having all the measures that should have been implemented.

This is also often mentioned as a frustration for several of the participants, where they feel that more communication and measures such as a local IT or security personnel would help them with security. P1 describes their frustrations:

> Things are very centrally controlled, and everything that comes from the big beast down in Oslo can sometimes feel distant. In a way, it would have been helpful if we had a security officer in each company.

In another branch office, they also discuss how IT is centralised and that they cannot help everyone at once. P6 describes it:

> We don't have any IT expertise at the service center; it is centralised in Oslo, and they can't assist everyone at once.

We can also see further frustrations in the statement mentioned by P7 previously in section 4.2.2, where he suggests that he does not feel like he has a voice when it comes to measures and that the main office can at some times feel like they do not communicate enough to the branches, especially during the attack and clean up.

4.7.1 Variations in Professions

Subcultures are often linked to variations in professions within different offices. For instance, one office may have mostly accountants, while another may have IT professionals. These differences in professions were evident in the responses of the participants. For example, an accountant might require a lot of IT assistance, as explained by P6, who worked in accounting:

> We have had IT guys come and sit here one day a week over a long period of time to help us adapt to the smartest possible way of working, in relation to the desktop and the things we use the most, so that we don't have to switch back and forth so much. It has been invaluable to us that they could help us work as smartly as possible, because in the beginning it was very inefficient, we worked very clumsily and inefficiently and we didn't like that.

The accounting and development departments have divergent views on security. Where accounting depends on the IT department for security, the development team actively prioritises it as part of their daily tasks. P3 has shared some of their security improvement strategies:

> But by the way, in the development department, we have regular what we call "professional development weeks", where the entire week is dedicated solely to professional development. The format can vary a bit, but we've had a lot of emphasis on security, everything from ethical hacking to emergency preparedness, etc. It's been very successful. It's the management who introduced the idea that we should spend time on this. We are a group of 3-4 people who are what we call supervisors, and we are the ones who put together the program.

4.8 Overcompensation after the Attack

An attack on the scale of what was experienced by this organisation causes a somewhat paranoid perspective when rebuilding the systems and implementing new policies and measures, as explained by P3 in section 4.1.4. P2 does admit that they did tighten the security too much immediately after the attack and that finding a balance between security and user experience is an ongoing process which is not as easy as it seems:

> User-friendliness and security are not a simple and straightforward task. [...] We did tighten it too much in the beginning, which heavily impacted the user experience, so it's an ongoing process to adjust the systems to make it easy for users to access while also ensuring enough security. However, unnecessary adjustments are not required, but some tuning is always necessary.

P3 further explains in section 4.1.1 that tightening the 2FA login window was one of the measures where the security department overcompensated and hindered the employees in their work. P3 mentions that some of the measures were implemented in a rush causing a somewhat sub-optimal solution for a few of the measures:

> To give an example off the top of my head, we use Citrix for some of our solutions. So now when you connect with VPN, you also open up Citrix. I would imagine that if we had the time to properly discuss this and receive input from more members of the team, we would probably choose a web-based solution, maybe a cloud-based version of Citrix or something along those lines, as an example. Additionally, I think we would also choose to handle on-premise Active Directory differently than we currently do.

Chapter 5

Discussion

This chapter will present our empirical findings in relation to our research questions (RQ) and the literature review. Within this chapter, our empirical findings from chapter 4 will be compared and contrasted against existing knowledge that is addressed in chapter 2. Our contribution will add to existing knowledge and provide new insights into how an organisation's ISC changes and possibly improves after a large-scale cyberattack. This will also provide avenues for further research and some suggestions for organisations similar to the one in question. We seek to answer the two following RQs as a way of educating the readers on how a cybersecurity incident affects and influences the culture in an organisation:

1. **How does a cybersecurity incident affect and influence the information security culture in an organisation?**
2. **How do employees in different positions in this organisation view the impact the attack had on their working environment?**

5.1 Artefacts

The interviews revealed that security training and awareness were severely lacking; however, our studies indicate that the organisation had placed it higher on the agenda, which included extensive work on cybersecurity and hiring a Chief Information Security Officer (CISO) a few months before the attack. Several interviewees explained that the scale of the cyberattack impacted almost all aspects of the organisation and caused the company to suffer losses of several million NOK.

Our study shows that the organisation previously relied on more extended user manuals that covered the security training, while other observations indicated that the training was hidden within an ICT regulation document that went unnoticed by employees. The lack of security training and awareness leaves the employees ill-prepared to recognise and respond to security threats. The organisation took steps to improve this by implementing security training through short informative courses that the employees receive by email. Shorter courses are preferred over more densely written information by the employees (Al Hogail, 2015). Raising the knowledge and awareness level has been proven effective at improving employee behaviour towards information security, making employees more likely to comply with the security policies (Ismail, 2022a).

In addition to implementing a new security and training program, the company also implemented communication channels where the CISO shared crucial information on security both during and after the attack. However, our findings suggest that this method might not effectively engage the employees because one can easily skip reading the information

provided. Instead, several interviewees suggested having occasional workshops on security as an additional method to learn and raise employee awareness on security matters.

The research suggests that even though the courses are informative, knowledge and awareness could be elevated with the presence of a person well-informed on security to engage in discussions or give presentations on security at the branch offices. These findings correspond with what has been found by Glaspie and Karwowski (2018), where it is stated that engaging in activities focused on commitment to security goals with like-minded colleagues positively affects security compliance.

Our findings suggest that although there is some dissatisfaction with the user engagement part of the training program, it does not negate the fact that it has been effective at imparting knowledge and raising awareness across the organisation, as the interviews revealed. In conclusion, the organisation has successfully created a security culture as the components needed to create it consist of information security training and awareness (Alnatheer, 2015), both of which the company has managed to establish after the attack.

Although the knowledge and awareness levels have risen, it is clear to say that they should be at a different level. In addition to needing a security training program, the interviews revealed insufficient policies and weak authentication measures. The company decided to implement new password policies and more complex authentication methods to protect its information and systems in the future. While the interviewees recognised the importance and necessity of these new policies and authentication methods, several participants expressed frustration and dissatisfaction with how they were carried out.

As previously noted, our data found that security training was severely lacking before the attack. However, another area identified as vulnerable during the interviews was the infrastructure setup, which due to its condition, was only a matter of time before something happened. The data further indicates that after the attack, the IT department had a somewhat paranoid mindset and that, due to the age of the infrastructure setup, it was rebuilt with a much higher level of security than before. The research indicated that the general user experience suffered immediately after the attack, which may result from the measures implemented based on the paranoid mindset caused by the attack. Furthermore, the data also reveals that the 2FA login window was one of the measures which employees considered too rigid and caused a hindrance in the employee's working activities.

5.2 Espoused Values

The findings suggest significant changes in the organisation's espoused values following the cybersecurity incident. Several key aspects of the change in espoused values can be identified: rigid control and centralised management, increased attention from leadership, and the alignment of security measures and policies with established values.

Firstly, there was a notable shift towards more rigid control and centralised management of systems and applications. The technology/IT department appeared to have a different focus on security after the attack, leading to stricter controls and centralisation. Previously, employees had more autonomy, such as being local administrators on their computers, but now there is a need for centralised control. This change indicates a shift towards a more centralised approach to security management, likely driven by recognising the importance of maintaining strict control over systems and minimising possible vulnerabilities.

Secondly, there was increased attention from leadership regarding security. Prior to the incident, leadership had limited involvement beyond hiring a CISO. However, security gained more attention on the agenda after the attack, including at the board level. The reporting on security performance changed significantly, indicating that leadership became more involved

in risk assessments and decision-making related to security. This is similar to the findings of Al Hogail (2015) that management commitment plays a vital role in influencing good security behaviour. While leadership recognised the importance of security, our data reveals that concerns were raised about a lack of communication and feeling unheard, particularly from the branch offices. This suggests that although there was increased attention, there might have been a need for better communication and engagement with employees throughout the organisation.

Thirdly, the employees in the organisation generally had little difficulty adjusting their values to align with the new security narrative. They recognised the necessity of strict security measures and understood the potential risks of not adhering to them. However, there were concerns expressed about specific policies and processes. For example, implementing client monitoring and EDR (Endpoint Detection and Response) raised fears and uncertainties among employees. This indicates that while employees generally supported increased security measures, there was a need for clear communication and addressing concerns related to specific policies and technologies.

Overall, the findings demonstrate a shift in espoused values towards more centralised control, increased attention from leadership, and an overall acceptance of the importance of security measures. However, there were also concerns about communication, employee engagement, and the potential impact of specific policies on privacy and autonomy. These findings highlight the complex nature of espoused values after a cybersecurity incident and the need for organisations to balance security requirements with employee concerns and engagement carefully.

The noticed changes in espoused values can be described with the analogy "Once bitten twice shy" whereas, as an organisation, the security aspect was widely ignored by the employees before the attack. However, when they got "bit", people suddenly changed their attitude and learned a new respect for security. If security was not tightened, they might get "bitten" again and lose monetary value. The consensus that stricter security might actually be reasonable and not an obstacle was widely accepted by the organisation.

5.3 Shared Tacit Assumptions

This section will discuss the shared tacit assumptions in information security culture based on the findings. These shared tacit assumptions play a crucial role in shaping the overall information security culture within the organisation. The insights shared by the participants shed light on various aspects of an information security culture within the organisation, including attitudes towards data security, training program perceptions, communication culture, and motivations for completing security training.

5.3.1 Attitudes Towards Data Security

As stated by Uchendu et al. (2021) in section 2.1.2, human behaviour is a vital part of an information security culture, and to change how people function in a working environment, one must have a good understanding of human behaviour (Lacey, 2010). The authors further adds that changes to knowledge, attitudes, and behaviour requires different methods, which management must consider when attempting to develop a healthy information security culture. Another factor that must be considered is resistance to change that will occur at some point in the process (Schein, 2009).

The interviews revealed that the organisation is in a phase where resistance to change is visible, especially concerning the new password policies and the implementation of two-factor authentication. Our research suggests a general dissatisfaction with these new measures, evidenced by statements such as feeling imprisoned and perceiving them as unnecessary. This

interviewee further said: "Just give me the master key and let me work in peace". While these statements might be considered somewhat extreme, other examples show dissatisfaction with the new measures. Considering that human behaviour is the weakest link in the security chain (Al Hogail, 2015), attitudes such as this put the organisation at risk because there is a direct relationship between attitude and behavioural intent (Glaspie and Karwowski, 2018).

The findings indicate a shift in awareness and consciousness regarding data breaches, cybercrime, and related issues. This increased awareness suggests a growing recognition of the importance of data security. The observations made in our research highlight this shift, where participants reported having become more conscious of data breaches compared to before. This change in perception can be attributed to various factors, such as the rise in cyber threats, increased media coverage of security incidents, and the new security training program. Several researchers have also found training and education to aid in changing employees' attitudes and behaviours (Alnatheer, 2015; Da Veiga, 2016;) and help increase the possibility of employees complying with security policies (Sikolia and Biros, 2016).

Furthermore, the "prison" metaphor used in Section 4.1.1 suggests that individuals may perceive data security as something that is handled by specialised technical personnel rather than considering it a shared responsibility. This attitude can result in a lack of personal accountability and a tendency to overlook security measures. The absence of an IT department in the branch offices further reinforces the perception of data security as "out of sight, out of mind". These shared tacit assumptions indicate a need to promote a culture of collective responsibility for data security, similar to the findings of Sikolia and Biros (2016). Their research shows that organisations that value solidarity experience more favourable outcomes when adopting technology and that cultures that prioritise people tend to have more success when using information technology and achieving desired outcomes (Sikolia and Biros, 2016).

5.3.2 Perceptions of Security Training

Regarding the security training program, there are discrepancies among the participants and its mandatory nature. Some participants stated that the training was mandatory, while others claimed they had not faced any consequences for not completing it. This inconsistency suggests a need for more transparent policies or communication regarding the mandatory nature of the training. The organisation should establish clear guidelines and communicate them effectively to ensure consistent participation in security training programs. To facilitate this, the guidelines should be accessible to all employees.

5.3.3 Communication Culture and Blameless Postmortems

The participants' statements indicate the presence of an open communication culture within the organisation. This culture encourages individuals to speak up, admit mistakes, and engage in blameless postmortems to identify and learn from security incidents. The emphasis on transparency and recognising human fallibility contribute to a culture that fosters continuous learning and improvement in information security practices.

5.3.4 Motivations for Completing Security Training

The participants express differing views on the need for incentives to motivate employees to complete security training. Some participants believe that responsible employees should contribute to the company's success without the need for external incentives. Others highlight the potential effectiveness of incentives like badges or titles in motivating employees to engage in training activities. These varying perspectives suggest that individual motivations differ, and a combination of intrinsic and extrinsic motivators could effectively promote participation in security training programs. Al Hogail (2015), on the other hand, found that

incentives and deterrence is an essential factor in motivating employees to comply with information security practices and preventing bad security practices, a thought which is shared by other researchers as well (Pearlson et al., 2022; Glaspie and Karwowski, 2018).

Furthermore, participants highlight the importance of knowledge sharing and having someone knowledgeable in cybersecurity and IT within the organisation. Workshops on security and access to expertise in the field can act as motivators for raising the overall knowledge level. The opportunity for interaction, asking questions, and receiving clarification enhance the effectiveness of training initiatives and ensures a deeper understanding of information security practices. These findings match what has been found by Al Hogail (2015) as awareness-raising initiatives and as a method of reducing the gap between what the organisation does and what the employees know.

In conclusion, the shared tacit assumptions within the organisation's information security culture reflect a growing awareness of data security concerns. However, there are still challenges related to attitudes towards data security, clarity of policies regarding training program requirements, and the need for effective communication and motivation strategies. To strengthen the information security culture, the organisation should emphasise collective responsibility, establish clear policies and guidelines, foster an open communication culture, and consider a combination of intrinsic and extrinsic motivators to encourage employee participation in security training programs.

5.4 Knowledge

The level of knowledge within the organisation's information security culture (ISC) underwent significant changes following the security incident and subsequent implementation of awareness training programs. Our research found that the organisation lacked security training and awareness programs, indicated by the significant gap in employees' understanding of security practices. Without security training and awareness programs, the organisation will still be at risk due to the employees being the weakest link. Considering that security knowledge and perception of security policies influence security behaviour (Da Veiga, 2015), it emphasises the importance of having security training and awareness programs to turn employees from security risks to security assets.

The findings uncovered a clear difference in information security knowledge among the participants. Some interviewees emphasise the importance of security; however, comments such as: "Is it necessary for it to be like this" about the new policies and measures indicate a lack of understanding of why they are in place and their importance. Our findings indicated a clear difference in the understanding of information security and general IT knowledge among some participants compared to others in our study. This corresponds with findings by Al Hogail (2015), which indicates that without the know-how to use the provided technologies efficiently, it increases the risk of errors that negatively impacts the organisation. However, the findings also suggest that the security knowledge in the organisation has significantly improved after the attack; employees have demonstrated a much greater understanding of security practices and their relevance to their daily and work life. The training and policies have given the employees better decision-making, for example, knowing what applications or software they can install. This can indicate a shift in how employees think and displays a more security-conscious mindset.

5.5 Subcultures

Within the organisation examined in this case study, it became evident that subcultures within the ISC exist across different branch offices. While the main office may share specific

thoughts and perspectives on security, the branch offices often exhibit similar views while differing in some values and knowledge. These subcultures within the organisation can pose challenges when implementing consistent security practices and fostering a unified security culture. When implementing changes, one might not expect that the culture will change uniformly.

As highlighted by our findings, one of the main factors contributing to subcultures is the organisational structure, which is not optimised for security. The presence of branch offices and the lack of a unified approach to security became apparent during the attack. The attackers disregard the internal organisational structure, making it crucial to address these issues and improve the relationships and values between these offices. Centralising control and decision-making can also lead to frustrations among the branch offices, as expressed by participants who desire more localised IT or security personnel.

Our research found that IT support is centralised in the main office, resulting in a limited capacity to assist everyone simultaneously. This limitation hampers the timely resolution of security-related issues and reinforces the sense of detachment and frustration among employees in the branch offices. The absence of local IT expertise in certain branch offices further exacerbates employees' challenges.

Moreover, the participants expressed frustrations regarding the central office's lack of communication and involvement in addressing security concerns within the branch offices, particularly during the attack and subsequent cleanup. The perception of a communication gap suggests the existence of subcultures within the organisation, where branch offices may feel disconnected from the central decision-making and implementation processes.

The presence of these subcultures displays that to make significant changes to the culture in a larger organisation such as this; one would need to involve all of the branch offices with communication as well as proper guidance from preferably someone physically present to ensure an overall improved and streamlined ISC in the entire organisation. Al Hogail (2015) emphasises that the level of information security culture is strongly linked to the availability of an information security team and the authority given to that team.

5.5.1 Variations in Professions

In addition to variations caused by organisational structure and communication, subcultures in organisational culture can also arise from differences in professions across different offices (Schein, 1996). Our findings, however, suggest that these subcultures also exist within ISC. For instance, accounting departments may heavily rely on IT support for security-related matters, while development teams may actively prioritise security in their daily tasks. This divergence in perspectives highlights the importance of tailored approaches to security awareness and training, considering the unique requirements and knowledge levels of different professional roles within the organisation. These variations in professions and their related approaches to security contribute to forming subcultures within the organisation. The organisation must recognise these differences and implement strategies bridging gaps in knowledge and practices, fostering a unified and cohesive security culture.

5.5.2 Falling Back into Old Routines

One of the key concerns that emerged from the interviews is the fear of falling back into old routines regarding information security culture within the organisation. Despite the significant impact of the cyberattack and the subsequent efforts to enhance security measures, there is a genuine worry that, over time, the organisation may revert to its previous state of complacency. This apprehension stems from several factors discussed by the participants.

Firstly, the high level of trust in the IT department or the "IT-guys" plays a crucial role. While the interviewees expressed confidence in the capabilities and dedication of the IT personnel, one must recognise that trust alone may not be sufficient to sustain a strong security culture. It is acknowledged that frustration with specific security measures can lead to a complacent attitude where individuals assume that the IT department will handle everything, absolving them of their responsibilities. This mindset poses a risk of complacency and a potential return to old habits and vulnerabilities.

The participants highlighted the difficulty of central control and communication from the main office, leading to a sense of detachment and a perceived lack of influence in security-related decision-making. Secondly, subcultures within different branch offices further compound the concern. The varying perspectives, values, and knowledge across different offices make ensuring consistent security practices throughout the organisation challenging. This lack of alignment among offices increases the risk of inconsistency and potential regression into old routines.

Participants noted that certain departments, such as accounting, heavily relied on IT support and assistance, while others, like the development team, actively prioritised security as part of their daily tasks. This divergence in attitudes and practices could lead to a fragmentation of the overall security culture, making it challenging to sustain a unified and proactive approach to information security across the organisation. Furthermore, the variations in professions within different offices contribute to the worries about falling back into old routines.

The aftermath of the cyberattack also highlighted the risk of overcompensation in response to the incident. The attack's immediate aftermath led to tightened security measures, adversely affecting user experience and productivity. While adjustments were made to strike a balance, there is a concern that reactionary measures implemented in haste may not be the most optimal or sustainable solution in the long run. This apprehension further reinforces the fear of reverting to old routines as the challenges of finding the right balance between security and user experience persist.

The organisation must foster a strong and pervasive information security culture to mitigate the worries of falling back into old routines. This involves continuous education and awareness programs to ensure that employees remain vigilant and proactive in their approach to security. Regular communication channels and feedback mechanisms should be established to bridge the gap between the main and branch offices, promoting a sense of involvement and ownership among all employees. Additionally, ongoing evaluation and adjustment of security measures are necessary to ensure they are effective, efficient, and user-friendly, minimising the temptation to revert to old, less secure practices.

By addressing these concerns and actively promoting a culture of information security, the organisation can strive to avoid falling back into old routines and maintain a robust security posture in the face of evolving threats.

5.5.3 Changes in Levels of Culture

As mentioned in the previous discussion, all the levels of cultures saw significant change; some levels improved a lot, and other levels saw improvement but could still be significantly improved upon to get an idea of where the business was before the attack and how its levels changed or improved. We will use the conceptual framework to create models that reflect the culture before and after the attack.

As explained in section 2.5, figure 5.1 can be explained as being in perfect cultural equilibrium and representing the ideal culture in terms of information security since its both strong and stable. All four levels have greater strength than the baseline (BL), resulting in a positive

nett security level. The nett effect can, however, be positively or negatively influenced depending on how secure the underlying levels of culture are.

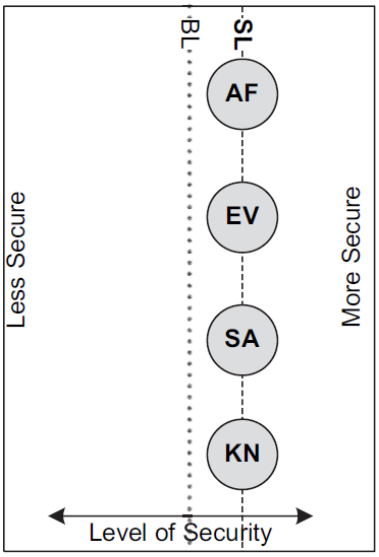

Figure 5.1: Strong and stable or ideal culture.

Figure 5.2 depicts the average security level before the attack based on our findings, which suggests that the nett security level was significantly below the recommended baseline suggesting that an attack would be hard to prevent. In this culture, neither of the levels is of sufficient strength to meet the minimum acceptable baseline, with the artefact and the knowledge levels being significantly lower than the other two. The employees lack the required knowledge and do not have the desired beliefs and values, and due to the espoused values and shared tacit assumption being below the minimum acceptable baseline, and it can not be guaranteed that the employees have the desired behaviour, resulting in an undesirable culture. Considering that stricter espoused values have an elastic effect on the artefacts, in the culture in figure 5.2, there needs to be an increase in knowledge level for the levels to align.

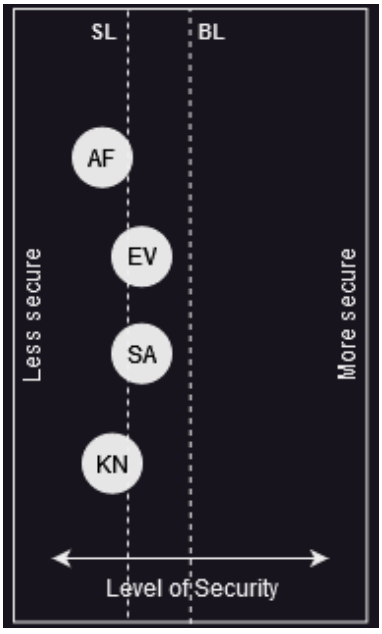

Figure 5.2: Insecure and unstable culture.

Figure 5.3, on the other hand, depicts where we estimate that the findings show where the

levels are at currently. The model shows that the security nett line has improved slightly above the recommended baseline but is still far from the ideal culture model as shown in 5.1. Considering that the employees show an adequate level of knowledge, it negates the fact that they do not have the desired beliefs and values, resulting in a slightly more secure culture than the minimum acceptable baseline. In this culture, the employees might behave insecurely regarding specific security controls if the controls conflict with their beliefs or hinder them from doing their job effectively. This shows that security should still be a highly prioritised aspect of the organisation, but to address the gap between the espoused values and the shared tacit assumptions, the employees need to be included in developing the espoused values. By including the employees in the process, the organisation can reduce the gap making the culture more predictable and thus more desirable.

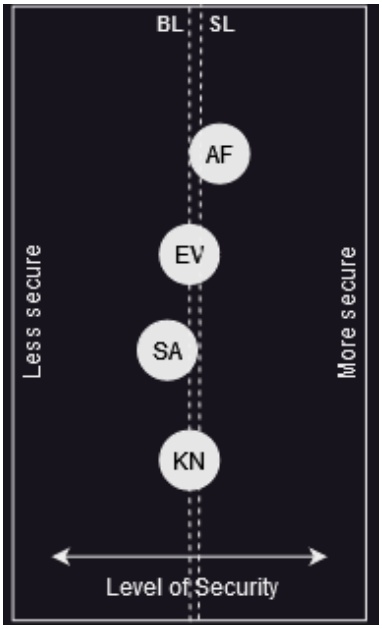

Figure 5.3: Secure and unstable culture.

Figure 5.2 and 5.3 have been used to visually explain the culture in the organisation we studied before, compared to how it currently is after revising the information security strategy.

5.6 Contribution to Research

This research makes several contributions to the field of information security culture (ISC) by shedding light on previously under-explored aspects and providing specific recommendations for organisations. The following points highlight the key contributions of this study:

5.6.1 Changes in Information Security Culture after an Attack

One significant contribution of this research is exploring the changes in information security culture within an organisation following a cyberattack. While previous studies have examined pre-attack information security practices and post-attack response strategies, the focus on transforming information security culture in the aftermath of an attack is relatively limited. This research fills this gap by uncovering the shifts in attitudes, behaviours, and perceptions towards information security within the studied organisation. Understanding these changes contributes to a deeper understanding of the dynamics of ISC and provides insights into the adaptive strategies organisations employ to enhance their security posture.

5.6.2 Subcultures and Variations in Professions within ISC

Another contribution of this research is the exploration of subcultures and variations in professions within the organisation's information security culture. By recognising the existence of subcultures and the diverse professional backgrounds of employees, this study highlights the importance of considering contextual factors and individual perspectives in shaping information security practices. The findings reveal differences in attitudes, knowledge, and responsibilities among various departments and roles, emphasising the need for tailored approaches to foster a cohesive and effective information security culture. This understanding can assist organisations in developing targeted training programs, communication strategies, and policies that address the specific needs and challenges of different professional groups.

5.7 Limitations of Research

While this research provides valuable insights into the organisation's information security culture following the cyberattack, it is important to acknowledge the limitations inherent in the study. These limitations impact the generalisability and depth of the findings. The following points highlight the key limitations of this research:

5.7.1 Single Case Study

The research is based on a single case study, focusing on one organisation that experienced a cyberattack. More time and more interviews would have made it possible to develop the interview guide further to collect more specific answers and details. As a result, the findings may not represent other organisations or industries that have suffered similar attacks. The specific context, organisational structure, and culture of the studied organisation may limit the generalisability of the findings to a broader population. Therefore, caution should be exercised when applying these findings to other organisations without considering their unique characteristics.

5.7.2 Time Constraints

Due to time constraints, the research was conducted within a limited time frame. The interviews and data collection were conducted within a specific period, which may have impacted the breadth and depth of the information gathered. A longer research duration would have allowed for a more comprehensive understanding of the post-attack information security culture and the long-term effects of the incident. The time constraint may have limited the ability to capture changes and adaptations that occurred over an extended period.

5.7.3 Limited Number of Interviews

The study relied on limited interviews with participants from different branches and the central office. While efforts were made to ensure diversity and representation across different departments and roles, the sample size was relatively small. As a result, the findings may only encompass part of the organisation's full range of perspectives and experiences. Including more interviews from each branch office and the central office would have provided a more comprehensive understanding of the information security culture across various units.

5.7.4 Potential Recall Bias

The interviews relied on the recollection of the participants regarding the events and actions taken during and after the attack. As the attack occurred several years prior to the research, recall bias is possible. Participants may not accurately remember all the details and specific measures taken, potentially leading to inaccuracies or incomplete information. While efforts

were made to mitigate this bias by asking participants to reflect on their experiences, the potential for memory lapses or subjective interpretations remains.

Chapter 6

Conclusions

This thesis explored the changes in information security culture in an organisation before and after a significant cyberattack. This study has explored the various aspects of ISC, including the cultural levels identified by Van Niekerk and Von Solms (2010) and other topics such as subcultures, variations in professions and the changes happening within the organisation. The study used a qualitative research approach through a case study with the data collected using semi-structured interviews. The empirical findings, in conjunction with the findings from the literature review, have provided insights into the information security culture within an organisation, specifically related to the changes an organisation experiences in the aftermath of a cyberattack.

The study has shed light on the existence of subcultures within ISC, on which there was previously limited information. While subcultures within an organisational culture are well-discussed, the same can not be said for ISC. Recognising the possibility of subcultures in ISC in an organisation setting is crucial for developing targeted approaches and addressing the specific needs of different departments and professions. Thus, by addressing these concerns, an organisation can better its security awareness and training approach.

The research has also provided organisations with recommendations that can be used to foster a positive security culture. Organisations can also use these recommendations to improve their current information security culture to reduce the risks to their IT systems. Based on the research, we recommend they consider the following suggestions:

- Consider the human part of cybersecurity and how human behaviour and attitude connect to develop a strong and healthy information security culture.
- To develop an ideal ISC, it is essential to have functioning security training and awareness programs and develop appropriate policies and processes.
- Including employees with various backgrounds in developing and implementing new security policies to ensure that the needs of various employee groups are considered.
- Consider having a physical IT presence in branch offices to improve security awareness and knowledge as well as give employees another source of information that is easily accessible.
- Establish communication channels that are easily accessible with information regarding different security aspects that can be understood by all employees regardless of their technical competence level. This is especially important both during and after an attack.
- Be aware of subcultures and work towards the organisational culture and subcultures being in unison; this could be done with better communication and more involved

management.

To conclude, this study contributes to the existing ISC knowledge by applying a theoretical framework to a real-life case to explore the changes an organisation underwent after a cyberattack; the findings highlighted the existence of subcultures and the variations of security knowledge and awareness in different professions. For an organisation to foster a strong and healthy information security culture, we have provided some recommendations that companies should consider applying to reduce the risks to the IT systems. Cybersecurity constantly changes; organisations must continuously revise and rework their information security approach to safeguard their assets.

6.1 Suggestions for Future Research

The research on the organisation's information security culture (ISC) has provided ideas on several essential aspects. However, there are still areas that should be further explored to deepen the understanding of ISC and its impact on organisational security. The following suggestions for future research aim to address these gaps and provide valuable insights into ISC.

The first direction that future researchers should look into is comparative studies. Conducting comparative studies across multiple organisations could provide more valuable insights into the variations in ISC and how these variations impact an organisation's overall information security practices. By analysing organisations that are different in size, location and industry sectors, researchers could identify the commonalities and differences in how their ISC functions; this could be used to find success factors and factors that lead to the worsening of culture. A more precise idea of best practices could be developed by performing such a study.

Second, researchers should look into how leadership can shape the information security culture within organisations. Valuable insights can be gained by analysing the influence management has on behaviours, values and decision-making processes and its impact on information security policies. Understanding their role would allow organisations to develop strategies for cultivating a strong security culture from the top down.

The final suggestion is to examine the influence of organisation structure on ISC. While the research has provided the findings of subcultures due to large branch offices, further investigation into this topic can give a more detailed understanding of how an organisation's structure affects it and how different the cultures in different structures are.

Bibliography

Al Hogail, A. (2015). Cultivating and assessing an organizational information security culture; an empirical study. *International Journal of Security and Its Applications*, *9*(7), 163–178.

Al Sabbagh, B., Ameen, M., Wätterstam, T., & Kowalski, S. (2012). A prototype for hi 2 ping information security culture and awareness training. *2012 international conference on E-learning and E-technologies in education (ICEEE)*, 32–36.

AlHogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–7.

Alnatheer, M. A. (2015). Information security culture critical success factors. *2015 12th International Conference on Information Technology-New Generations*, 731–735.

Anderson, R. (2007). Thematic content analysis (tca). *Descriptive presentation of qualitative data*, 1–4.

Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative research journal*, *18*(4), 383–400.

Bingham, A. J., & Witkowsky, P. (2021). Deductive and inductive approaches to qualitative data analysis.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77–101.

Chen, Y., Ramamurthy, K. (, & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Connolly, L., & Lang, M. (2012). Investigation of cultural aspects within information systems security research. *2012 International Conference for Internet Technology and Secured Transactions*, 105–111.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151.

Da Veiga, A. (2015). The influence of information security policies on information security culture: Illustrated through a case study. *HAISA*, 22–33.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314–321.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Enabling information security culture: Influences and challenges for australian smes.

Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A literature review. *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17- 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8*, 269–280.

Green, M. (2009). Eyewitness memory is unreliable. *Retrieved April*, *28*, 2011.

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study.

Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. (2017). Information security culture in health informatics environment: A qualitative approach. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6.

IBM. (2022). *What is a cyberattack?* Retrieved May 27, 2023, from https://www.ibm.com/topics/cyber-attack

Ismail, O. (2022a). Designing information security culture artifacts to improve security behavior: An evaluation in smes. *The Transdisciplinary Reach of Design Science Research: 17th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2022, St Petersburg, FL, USA, June 1–3, 2022, Proceedings*, 319–332.

Ismail, O. (2022b). Relationship between culture and user behavior in the context of information security systems: A qualitative study in smes. *Digital Economy. Emerging Technologies and Business Innovation: 7th International Conference on Digital Economy, ICDEc 2022, Bucharest, Romania, May 9–11, 2022, Proceedings*, 115–128.

Johnston, A., Di Gangi, P., Howard, J., & Worrell, J. L. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, *20*(3), 3.

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954–2965.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive*, *9*(3), 2012–52.

Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: Amee guide no. 131. *Medical teacher*, *42*(8), 846–854.

Klevstrand, A., Bugge, W., Christensen, J., & Magnus, C. H. (2020). *Hackerangrepet mot hydro enda dyrere enn tidligere antatt: Ny prislapp på 800 millioner kroner*. Retrieved May 22, 2023, from https://www.dn.no/bors/hydro/brasil/norsk-hydro/hackerangrepet-mot-hydro-enda-dyrere-enn-tidligere-antatt-ny-prislapp-pa-800-millioner-kroner/2-1-898620

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13.

Linneberg, M. S., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative research journal*, *19*(3), 259–270.

Malcolmson, J. (2009). What is security culture? does it differ in content from general organisational culture? *43rd Annual 2009 international Carnahan conference on security technology*, 361–366.

Martins, A., & Elofe, J. (2002). *Information security culture*. Springer.

McCombes, S. (2023). *How to write a literature review | guide, examples, & templates*. Retrieved February 15, 2023, from https://www.scribbr.com/methodology/literature-review/

McNamara, C. (1999). General guidelines for conducting interviews.

Myers, M. D., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and organization*, *17*(1), 2–26.

Ngo, L., Zhou, W., & Warren, M. (2005). Understanding transition towards information security culture change.

Oates, B. J. (2006). *Researching information systems and computing*. Sage Publications.

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International journal of qualitative methods*, *19*, 1609406919899220.

Pearlson, K., Schwartz, J., Sposito, S., & Arbisman, M. (2022). How verizon media built a cybersecurity culture. *MIS Quarterly Executive*, *21*(2), 6.

Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2013). Variations in information security cultures across professions: A qualitative study. *Communications of the Association for Information Systems*, *33*(1), 11.

Ramdhani, A., Ramdhani, M. A., & Amin, A. S. (2014). Writing a literature review research paper: A step-by-step approach. *International Journal of Basic and Applied Science*, *3*(1), 47–56.

Recker, J. (2013). *Scientific research in information systems: A beginner's guide*. Springer.

Schein, E. H. (1996). Three cultures of management: The key to organizational learning. *MIT Sloan Management Review*.

Schein, E. H. (2009). *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

Schwarz, A., Mehta, M., Johnson, N., & Chin, W. W. (2007). Understanding frameworks and reviews: A commentary to assist us in moving our field forward by analyzing our past. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *38*(3), 29–50.

Sikolia, D., & Biros, D. (2016). Motivating employees to comply with information security policies. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2016*(2), 2.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503–522.

The University of Edinburgh. (2022). *Literature review*. Retrieved February 15, 2023, from https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, *27*(2), 237–246.

Tilahun, A., & Tibebe, T. (2017). Influence of national culture on employees'intention to violate information systems security policies: A national culture and rational choice theory perspective.

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The qualitative report*, *15*(3), 754.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476–486.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii–xxiii.

World Economic Forum. (2022). *The global risks report 2022*. Retrieved March 3, 2023, from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of planning education and research*, *39*(1), 93–112.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.

Appendix A

Article Overview

Article title	Keywords	Publisher	Link	Date	Citations
User Participation in Information Systems Security Risk Management	Regulations, User participation, information security, security risk management	MIS Quarterly	https://doi.org/10.2307/25750689	2010	617
Impacts of comprehensive information security programs on information security culture	SETA programs, security culture, security policies, security monitoring	International Association for Computer Information Systems	https://doi.org/10.1080/08874417.2015.11645767	2015	203
The impacts of organizational culture on information security culture: a case study	Case study, Information security, organisational culture, security culture	Springer New York LLC	https://doi.org/10.1007/s10799-015-0252-2	2015	132
Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study	security culture, policy, assesment	Emerald Group Publishing Limited	https://uir.unisa.ac.za/bitstream/handle/10500/23161/Comparing%20the%20information%20security%20culture_Information%20and%20Comp%20Sec%202016.pdf;jsessionid=BEBDCF57F9DFC8DDB51760EC5BD8D2CE?sequence=4	2016	105
Information security culture: A definition and a literature review	security culture	IEEE	https://ieeexplore.ieee.org/document/6916579	2014	93
Human Factors in Information Security Culture: A Literature Review	security culture, incentives, deterrence, training, awareness	Springer, Cham	https://doi.org/10.1007/978-3-319-60585-2_25	2017	78

Information security culture critical success factors	Critical Success Factors, Information Security Culture, Organizatio n Culture	Institute of Electrical and Electronics Engineers Inc.	https://doi.org/10.1109/ITNG.2015.124	2015	61
Enabling Information Security Culture: Influences and Challenges for Australian SMEs	Information security culture, small and medium enterprises	Association for Information Systems	https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e192a9639cacdbffad8c520740818af3719000cc	2010	46
Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study	security culture, (ISCF), Behavioral research, Human egnineering	Science and Engineering Research Support Society	https://doi.org/10.14257/ijsia.2015.9.7.15	2015	42
An Information security culture model validated with structural equation modelling	Awareness, Compliance , Empirical model, Information security culture, Manageme nt, Policies, Theoretical model	University of Plymouth	https://uir.unisa.ac.za/handle/10500/19061	2015	36
The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study	information security policy, security culture, human behaviour	University of Plymouth	http://hdl.handle.net/10500/19060	2015	35
Variations in information security cultures across professions: A qualitative study	security culture, security behaviour, professions	Association for Information Systems	https://doi.org/10.17705/1CAIS.03311	2013	34

It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups	Collective security efficacy, information security, Socioecological theory, Social Disorganization Theory, Employee Groups, Thematic Analysis	Association for Information Systems	https://core.ac.uk/download/pdf/301379202.pdf	2019	26
Information security culture in health informatics environment: A qualitative approach	security culture, health informatics	IEEE Computer Society	https://doi.org/10.1109/ICRIIS.2017.8002450	2017	17
Investigation of cultural aspects within information systems security research	national culture, organisational culture, security culture	IEEE UK/RI Computer Chapter Infonomics Society	https://ieeexplore.ieee.org/abstract/document/6470994	2012	13
Motivating Employees to Comply with Information Security policies	Information security, Grounded Theory Methodology, Intrinsic Motivation, Compliance with IS Policies	Association for Information Systems	https://aisel.aisnet.org/jmwais/vol2016/iss2/2/	2016	4
Influence of national culture on employees' intention to violate information systems security policies: A national culture and rational choice theory perspective	security culture, national culture, internal threats, human behaviour	Association for Information Systems	https://aisel.aisnet.org/ecis2017_rip/2	2017	3

Reviewing the Interrelation Between Information Security and Culture: Toward an Agenda for Future Research	information security and culture, review of current research	CEUR-WS	https://ceur-ws.org/Vol-2966/paper4.pdf	2021	2
Relationship Between Culture and User Behavior in the Context of Information Security Systems: A Qualitative Study in SMEs	security culture, security behaviours, end users	Springer, Cham	https://link.springer.com/chapter/10.1007/978-3-031-17037-9_8	2022	0
Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs	security culture, SMEs, security behaviours	Springer, Cham	https://doi.org/10.1007/978-3-031-06516-3_24	2022	0
Building a Security Propaganda Machine: The Cybersecurity Culture of Verizon Media	security culture, incentives, employee behaviour	Association for Information Systems	https://aisel.aisnet.org/misqe/vol21/iss2/6	2021	0

Appendix B

Consent Form

Vil du delta i forskningsprosjektet "The importance of cybersecurity culture in organizations"

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

I denne masteroppgaven skal vi undersøke hvordan sikkerhetskultur i organisasjoner påvirker en organisasjons fullstendige sikkerhet, og om det er noe som burde bli lagt mer vekt på. Vi ønsker å undersøke hva bedrifter som har stått overfor angrep har å si om hvordan sikkerhetskultur var med på å bidra til angrep og om den har sett endringer i etterkant.

Hvem er ansvarlig for forskningsprosjektet?

Vegard Marvik og Rami Bakir er to studenter fra Universitetet i Agder ved Institutt for Informasjonssystemer, og er ansvarlige for dette prosjektet. Vårt ansvar er å designe intervjumetoden, datainnsamlingen og behandlingen av data.

Hvorfor får du spørsmål om å delta?

Vi spør deg om å være med, fordi du er vurdert til å være en relevant kilde til informasjon. Du er i utvalget, fordi du var ansatt før, under og etter angrepet av bedriften og har med det erfaring med hvordan det var å jobbe i bedriften i denne tidsperioden. Samtidig har du også informasjon om endringene som ble innført som følge av angrepet sammenlignet med hvordan ting var før tiltakene ble implementert.

Det er frivillig å svare på spørsmålene og i din rett å velge hvilket svar du gir.

Hva innebærer det for deg å delta?

Hvis du har lyst å delta i forskningsprosjektet, vil vi ha et intervju med deg. Intervjuene vil bli gjort med digitalt videoopptak og opplysningene som samles inn av intervjuobjektet er:

- Navn
- Stilling/rolle i organisasjonen
- Informasjon rundt din stilling og rolle i organisasjonen

Spørsmålene vil handle om din egen vurdering av hendelser som ledet til angrep og hva som har blitt endret i etterkant, med fokus på sikkerhetskultur. Intervjuet vil ta ca. 45 minutter.

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.
Tiltak for at ingen uvedkommende får tilgang til personopplysningene dine inkluderer:

- Navn og annen identifiserbar informasjon vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data, f.eks.: CIO1 for IT-lederen i en bedrift fremfor navnet til personen
- Datamaterialet vil bli lagret på sikret OneDrive sky-konto under skolens domene med to-faktor autentisering
- Personopplysninger og andre sensitive data vil bli lagret separat mappe

Deltakere vil ikke kunne gjenkjennes i publikasjonen. Deltakerne vil anonymiseres og refereres til som intervjuobjekt eller med kode som nevnt ovenfor, dersom det er hensiktsmessig. Organisasjonens navn vil også anonymiseres. I den sammenheng vil ikke informasjon kunne knyttes til deltaker.

Personer som vil ha tilgang til dine personopplysninger er som følger:

1. Vegard Marvik, Masterstudent
2. Rami Bakir, Masterstudent
3. Marko Ilmari Niemimaa, Førsteamanuensis (Veileder)
4. Lucia Herrera, Stipendiat (Veileder)

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 31.12.2023. Opptak skal være slettet så snart de er transkribert, og all personlig identifiserende informasjon blir slettet.

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, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Vegard Marvik og Rami Bakir har NSD - Norsk Senter for Forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med person regelverket.

Hvor kan jeg finne ut mer?

Har du spørsmål om studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Institutt for Informasjonssystemer ved Vegard Marvik: vegarm17@uia.no og Rami Bakir: ramib@uia.no og/eller veileder Marko Ilmari Niemimaa: marko.niemimaa@uia.no

- Vårt personvernombud: Rådgiver/Personvernombud ved Institutt for Informasjonssystemer: Trond Hauso: personvernombud@uia.no

Ved spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD - Norsk Senter for Forskningsdata AS på telefon: +47 73 98 40 40

Med vennlig hilsen,
Vegard Marvik, Rami Bakir,
Marko Ilmari Niemimaa og Lucia Herrera

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "The importance of cybersecurity culture in organizations", og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervjuet
- ☐ at Vegard Marvik og Rami Bakir kan gi opplysninger om meg til prosjektet og at mine opplysninger behandles frem til prosjektet er avsluttet den 31.12.2023

(Signert av prosjektdeltaker, dato)

Appendix C

Interview Guide

Formål

- Vi ønsker å intervjue ansatte i forskjellige stillinger for å høre om hvordan de opplevde at sikkerhetskulturen i bedriften ble påvirket av et dataangrep sammenlignet med før angrepet skjedde og hva slags endringer som ble oppfordret av ledelsen. Informasjonen gitt i intervjuet vil bli anonymisert slik at verken navn eller bedrift vil kunne gjenkjennes, dette er også godkjent av NSD.

Introduksjonsspørsmål

1. Kan du fortelle oss litt om din rolle/stilling i din organisasjon?
2. Hvor lenge har du jobbet for din organisasjon?

Hovedspørsmål

Angrep

1. Kan du fortelle oss litt om angrepet og hva slags konsekvenser det hadde for bedriften?
2. Hva slags sikkerhetstiltak ble innført som følge av angrepet?
3. Hvordan var sikkerhetsopplæringen før angrepet og hva har endret seg?
4. Hva er den mest merkbare endringen som du har opplevd som konsekvens av angrepet?

Dag til dag

5. Vet du mer om det globale risikobildet nå, enn det du gjorde før?
6. Hvordan endret dag til dagen din, noen spesifikke prosesser?
7. Føler du at det trengs flere endringer i henhold til sikkerheten i bedriften?
8. Føler du at noen av endringene var unødvendige?
9. Var det noen sikkerhetstiltak du følte gjorde jobben din vanskeligere, og hvorfor?
10. Har noen av de innførte sikkerhetstiltakene møtt motstand fra ansattgruppen i bedriften? Hvorfor?
11. Snakker du om cybersikkerhet med andre medarbeidere? Hvis ja, hva slags diskusjoner oppstår?

Læring

12. Hvordan blir kunnskap i henhold til sikkerhet delt eller formidlet til ansatte?
13. Tror du at måten du lærer om sikkerhet på er effektiv, tror du noe kunne blitt gjort bedre? svart
14. Blir ansatte oppfordret til å øke sin kunnskap i henhold til sikkerhet?
15. ~~Var representanter fra de forskjellige arbeidsgruppene (revisor/rådgivere o.l.) med på utformingen av de nye sikkerhetstiltakene?~~

Kultur

16. Har du sett endringer i verdiene og målene til bedriften?
17. Har du merket/opplevd noen vesentlige endringer i sikkerhetskulturen etter angrepet sammenlignet med før?
18. Hva føler du at du bidrar med til å gjøre arbeidsstedet sikrere? Hvorfor?

Motivasjon

19. Blir dere oppfordret til å bidra til en bedre sikkerhetskultur i bedriften?
20. Føler du at incentiver hadde bidratt til øke sikkerhetskulturen/kunnskapen hos den enkelte og hva slags incentiver mener du er best? Gi eksempler på incentiver!
21. ~~Hva slags incentiver hadde motivert deg til å lære mer om sikkerhet/bidra til økt sikkerhet i bedriften?~~