How to Measure Security Culture at Organization X

Jenni Gyllenberg

Haaga-Helia University of Applied Sciences
Degree Prorgramme in Communication Management
Thesis
2025

Abstract

Author(s)
Jenni Gyllenberg

Degree
Master of Business Administration

Thesis title
How to Measure Security Culture at Organization X

Number of pages and appendix pages
98 + 11

Most information and cyber incidents involve a human component – often an employee making a simple mistake that grants attackers access to systems or data. To mitigate this risk, organizations should consider implementing an effective security awareness program focused on creating a strong security culture to better protect their assets.

The objective of this study is to investigate how security culture can be measured at Organization X. Although the organization places a strong emphasis on security culture, it has been struggling to identify the appropriate methods for assessing the impact of its annual security awareness program and the culture cultivated through its activities.

The literature review in this thesis introduces concepts and frameworks related to security culture, including information security and cybersecurity, security awareness, and organizational culture. It also explores available models for measuring security culture.

This thesis examines how security culture can be measured and how selected measurement techniques can be applied to Organization X. It aims to serve as a valuable resource for other security professionals seeking to evaluate their security culture.

The measurement methods developed to analyze the security culture of Organization X were created in 2024. The research methods included multiple interviews, workshops, and brainstorming sessions. The developed measurement techniques were implemented at Organization X in 2024, and it is recommended that they be applied on a monthly and annual basis.

Keywords
security culture, security awareness, communication, organizational culture, cybersecurity, information security

Table of contents

1 Introduction

In today's digital landscape, organizations must continuously adopt new measures to safeguard their systems and assets. The time when physical threats represented the primary security risks has passed, and these traditional risks have evolved into new challenges, particularly in the areas of information and cybersecurity. This thesis originates from the commissioning organization's need to assess whether the actions and behaviors of its employees' are helping to protect it against potential threats.

1.1 Background

According to the World Economic Forum, 71% of Chief Risk Officers believe that cyber risk and criminal activity have a significant impact on their organizations. Furthermore, cybersecurity was identified as the world's fifth-largest risk, following misinformation and disinformation, extreme weather events, state-based armed conflicts, and societal polarization. The World Economic Forum also highlights growing concerns among organizations that cyberattacks will not only persist but also become increasingly sophisticated. High-income countries, including the Nordic nations, rank cybersecurity even higher and within their top three risks. This stresses the critical importance of cybersecurity in the Nordics and reflects a serious apprehension regarding the potential escalation of threats in this domain. World Economic Forum (2025, 15-30.)

Factors such as the ongoing geopolitical tensions, the emergence of new technologies, and the adoption of Artificial Intelligence (AI), alongside the evolving nature of cybercrime, contribute to an increasingly intricate cyber landscape of uncertainty and complexity. In 2024, the world experienced a notable increase in cyberattacks, with a significant rise in incidents, including fraud, phishing, and social engineering attacks. Given that such attack types typically target employees, organizations must exploring new methods to train their staff to defend against these threats. (World Economic Forum 2024, 12-24.)

Successful cyberattacks commonly result in data breaches, which occur when unauthorized individuals gain access to sensitive or confidential information. This is often accomplished by manipulating employees into taking actions that provide access, such as clicking on links in phishing emails. In 2023, the average cost of a data breach reached 4.88 million US dollars, marking a 10% increase from the previous year. Data breaches are not only costly but also challenging to detect. On average, it takes 258 days to identify and contain a breach, allowing attackers significant time to inflict damage. The most expensive incidents are typically the result of malicious insiders—employees who intentionally harm their organization. Such insider attacks average a cost of 4.99 million

US dollars. While investing in proactive security measures like firewalls, multi-factor authentication, and security awareness training can be expensive, these costs are significantly lower than the potential financial impact of a cyberattack. (IBM 2024, 8-13.)

Digitalization and the rapid shift of employees moving to work from home due to COVID-19 have put even more pressure on organizations and employees to focus on cyber safety. Currently, most information security incidents stem from human error. Since technology alone cannot shield organizations from all threats, and employees can pose significant security risks while also serving as vital defense mechanisms, organizations must strategically equip their workforce with the appropriate tools to counteract and safeguard against cyberattacks. To achieve this, organizations should foster a robust security culture, encouraging employees to adopt the right precautions.

In 2024, security professionals reported social engineering (89%) as the human risk they were most concerned about, followed by password management and authentication (45%), detecting and reporting incidents (43%), and artificial intelligence (31%). Social engineering includes attack types such as phishing (email-based), smishing (text-based), and vishing (phone-based), which are becoming more advanced and targeted with the use of artificial intelligence. According to statistics, in 2023, approximately 9 million phishing attacks were registered worldwide, making it the most common cybercrime type. The second most common type was personal data breaches, with 1.66 million reported cases. The statistics confirm that the human element is heavily involved in the most common cyber-attacks, which calls organizations to ensure their employees receive adequate awareness and training to identify and protect against attacks. (SANS Institute 2024, 9; Petrosyan 2024.)

An organization’s security culture has a significant impact on employee behavior, which was demonstrated in a study conducted in 2021 on 97,661 employees across 1,115 organizations. The study analyzed how susceptible employees were to phishing. Unsurprisingly, the results showed that employees working for organizations with a poor security culture were more likely to open phishing emails and interact with them. However, what was surprising was how significant the difference was. Employees at organizations that had a poor security culture were 52 times more likely to provide their user credentials in a phishing simulation than employees with a good security culture. This means that in organizations with a good security culture, one in one thousand employees was likely to be deceived into providing their credentials, whereas in organizations with a poor security culture, the ratio was one employee out of just twenty. (Eriksen, Petrič and Roer 2021.)

Mature organizations that understand information and cyber risks focus on shaping the security behaviors of their employees and measuring the organization's security culture. This thesis originates from a case organization's need to measure security culture as part of its security awareness program. The organization has a strong focus on security culture, but has been struggling to find the correct ways to measure the effects of the annual security awareness program and the culture they are creating through their activities.

This thesis investigates how a framework for measuring security culture can be designed and how it can be individually applied to Organization X. The intention is for this thesis to serve as a tool for other security professionals who wish to measure their security culture by outlining key research on the topic, existing methods, and the concrete measurements that were created for Organization X.

1.2 Problem Statement

At an Information Security Forum seminar held in Spring 2024, security professionals from across large organizations raised the question of how to measure the security behaviors and attitudes of employees. None of the organizations present had metrics in place to measure security behavior or security culture, or knew of an organization that did. This was seen as a significant challenge, and it was commonly agreed that organizations are struggling to understand and identify the measurements and methods that should be used and how they can be applied.

Based on academic and professional research, a commonly approved model to measure security culture does not exist. This thesis explains what methods have previously been studied, why a commonly used model does not exist, and why tailoring measurements based on the organization can give more value-added results. Furthermore, while this thesis focused on designing concrete measurement methods for Organization X, the created measurement models can easily be applied and adjusted to other organizations.

1.3 Research Questions

The objective of this research is to define security culture as part of an organization's overall culture and to examine how it can be measured. This thesis provides tools to understand the challenges of culture and managing an organization's security culture.

The main research question for this thesis is:

Q1. How can an organization-specific framework for measuring security culture be designed and validated within the context of Organization X?

Three sub-questions supporting the main research question:

Q2. What are the key dimensions of security culture as identified in current academic and professional literature?
Q3. Which methods and indicators are most effective in measuring security culture in practice, and how can they be adapted to fit the context of Organization X?
Q4. What are the limitations and potential future developments in measuring and improving security culture in organizations?

1.4 Scope and Limitations

This thesis provides a literature review of key models, concepts, and frameworks to explain topics related to security culture and methods that have been used by researchers to measure security culture. The scope has been limited to the most cited and often referred to studies.

Interviews with relevant stakeholders and industry professionals were used to provide independent input and expertise, and the work was conducted in workshops and during brainstorming sessions. The measurement methods that were chosen solely reflect the needs of Organization X and are limited to this organization.

The security culture results from the methods applied to Organization X are not included in the scope or presented in this thesis. Hence, this thesis is limited to explaining the research, its process, and the methods chosen to measure security culture at Organization X.

1.5 Significance of the Study

This thesis outlines a set of tools that can be used to measure security culture on a monthly and annual basis. By applying these measurement tools, Organization X should be able to quantify the present security culture, thereby gaining insight into the behaviors and attitudes employees have towards security, how this is manifested and reflected in key metrics. The results should be analyzed to pinpoint high-risk areas that need to be addressed in the organization’s security awareness program. Chosen awareness activities should focus on strengthening the attitudes and behaviors that are in line with the Organization’s values and focus on protecting the organization against harm.

While the measurement methods created in this thesis have specifically been made for Organization X, they can be utilized by other organizations. Some parts can be applied directly to any organization, whereas some elements should be tailored. The main benefit of this thesis is to help Organization X, however, it can also benefit any other organization

looking into measuring security culture. It provides value by providing a comprehensive overview of existing academic and professional research around security culture metrics, examples of measurement tools, and the tools applied to the commissioning company.

1.6 Commissioning Company

Organization X is a large company that serves customers through global offices across the world. The company has four main business areas that serve both consumer and corporate customers.

The thesis was commissioned by the Chief Security Office at Organization X, which is a unit responsible for monitoring and assurance activities in relation to information and cybersecurity, including being responsible for the company's security awareness activities.

1.7 Structure of the Thesis

This thesis includes five chapters. The first two chapters (Introduction and Theoretical Framework) form the theoretical part of the thesis and include an introduction to the thesis and a literature review. These are followed by the empirical part of the thesis (Methodology, Results, and Discussion), which includes chapters describing the methods used to collect and analyze data, outlines the data and results from conducted interviews and workshops, and provides answers to the investigative and research questions.

2 Theoretical Framework

The previous chapter provided an introduction to this thesis, its topic, relevance, and the research questions it will address. In this chapter, the focus will be on the conducted literature review, which outlines key definitions, concepts, and models relevant to this research. It also includes a critical review of previous research and potential gaps.

2.1 Information and cybersecurity

The terms information security and cybersecurity are often used in the same way, however, they have a slight difference. They are regularly defined at a high level, and hence, definitions can often vary. The National Institute of Standards and Technology (NIST) categorizes information and cybersecurity as separate yet connected to each other.

Von Solms and van Niekerk (2013) suggest that cybersecurity exceeds information security, as it is not limited to only protecting information, but also other assets. Taherdoost (2022), on the other hand, defines the difference between information and cybersecurity to be information. Information security aims to protect all information, regardless of where it is, whereas cybersecurity focuses solely on information in cyberspace. By this definition, Taherdoost concludes that cybersecurity is a part of information security.

2.1.1 Information Security

The International Organization for Standardization (ISO) has published an information security standard, ISO/IEC 27002, which defines information security as the “preservation of the confidentiality, integrity and availability of information” (ISO/IEC 27002 2005, 1). The United States Committee on National Security Systems (CNSS 2010) defines information security in slightly more detail as the "protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." The CNSS definition includes not only information but also information systems.

The confidentiality, integrity, and availability of information are mentioned in the ISO definition of information security, and these three words (confidentiality, integrity, and availability: CIA) are often referred to as the CIA triangle and widely used in the field of information security. ISO defines confidentiality as the means to ensure information is not available or disclosed to unauthorized instances. Integrity is defined as the means to protect the correctness and completeness of information, and availability as the means to

ensure access to information when requested by an authorized entity. The CIA triangle is a key principle in information security, and it enables information security professionals to consider how to guard an organization's data. (Taylor, Alexander, Finch and Sutton 2013; Death 2023, chapter 1.)

Confidentiality is a cornerstone in information security, as it includes the restriction of information, in essence, the act of protecting it. Protecting information ensures it cannot be used for unlawful or unwanted purposes, which could result in legal or financial penalties or undesired consequences to organizations or individuals. Ensuring the integrity of information guarantees that only people with the appropriate security clearance can update, change, or delete information. If the integrity of information cannot be guaranteed, it is impossible to confirm whether the information in question is correct. Information should be available and accessible when needed, otherwise, it is no longer information, but unimportant data. (Taylor et al 2013.)

In information security, the asset that must be protected is always the information itself. (von Solms & van Niekerk 2013, 97) Information is a wide term and can take on various forms, from written and spoken to physical and electronic, and beyond. Vacca (2013, chapter 1) states that it is not sufficient for an organization to secure its technical infrastructure, as this will not protect all information assets, as not all assets are dependent on technology. Information does not necessarily need technology to exist or to ensure its protection. Thereby, according to Vacca (2013, chapter 1), information security goes beyond information technology.

Protecting information is not limited to technology alone, it also includes all other forms. Hence, information security includes not only protecting technology but also the various forms in which information can be expressed, seen, and heard. As the world has become more digital, so has information. A vast amount of information has been moved from physical assets to digital forms, from paper forms to digital forms, books to ebooks. Organizations no longer keep important information on customers, employees, or processes on paper, but have moved it to digital form with the help of technology. Hence, protecting technology is often highlighted when referring to information security. While information today is mostly in digital format, it is important to understand that information security goes beyond technology and continues to include other important areas, such as printed material or discussions. (Taylor et al 2013.)

When an organization understands what its most important information assets are, it can implement proper measures to protect them. A good information security professional understands their organization's business, which will enable them to recognize where

important information, such as trade secrets and intellectual property, exists and what impact its destruction, alteration, or theft could result in. (Death 2023, chapter 1.)

2.1.2 Cybersecurity

The United States of America's Cybersecurity & Infrastructure Security Agency (CISA) defines cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (CISA s.a.). The United Kingdom's National Cyber Security Centre (NCSC) similarly defines cybersecurity as the function of protecting devices and accessed services from theft or damage, and the prevention of unauthorized access to personal information. (NCSC 2022)

The European Union Agency for Cybersecurity (ENISA) defines information security as a subset of cybersecurity and cybersecurity to compromise "all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats'. They continue to further define cybersecurity to cover "prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigations of cyber incidents". Cyber incidents are defined by ENISA as "any occurrence that has an impact on any of the components of the cyberspace or the functioning of the cyberspace, independent if it's natural or human-made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions". (ENISA 2017.)

Von Solms and van Niekerk (2013) highlight that many publications often use the terms information security and cybersecurity analogously. For the two terms to correspond, their definitions would also need to apply to both. Von Solms and van Niekerk (2013) argue that while this is most often true, there are examples where the definition of information security does not apply, for example, in cyberbullying. The loss of confidentiality, integrity, or availability of information cannot be applied to cyberbullying. Therefore, it is suggested that while the two terms can mostly be used equally, cybersecurity can be seen as protecting more than just information.

According to Death (2023, chapter 2), cybersecurity threats are "risks or vulnerabilities compromising the confidentiality, integrity, or availability of digital information, systems, or networks". This definition limits cybersecurity to digital formats (information, systems, and networks), whereas information security comprises all formats, including physical.

Grubb defines cybersecurity as the act of identifying threats, calculating the risks associated with those threats, and handling those threats accordingly. This is done by

using the CIA triad model to find out which threats are on the horizon. (Grubb 2021, Chapter 1.)

It is evident in literature that information security and cybersecurity are often mixed and treated as synonymous. In many cases, the terms are used in the same context and text, while the intention is to describe only one of them. This is common as the two areas overlap in many ways and are often used interchangeably. NIST's definition of cybersecurity mentions that it is the protection, damage prevention, and restoration of electronic communication services and systems. The challenge with information security and cybersecurity lies in the fact that cybersecurity is a part of information security, yet certain parts of information security are not included in cybersecurity, such as physical data. (NIST s.a.)

In this thesis, information security will be addressed as the act of protecting information in all formats, and cybersecurity as the digital protection of data, systems, and assets.

2.2 Security Awareness

Security awareness is an element that can be applied to both information and cybersecurity. According to Roer (2015, chapter 1), there is no commonly agreed upon definition of security awareness; hence, the definition changes based on the definer. Siponen (2000) defines security awareness as the "conditions in which users within an organization are aware of -ideally committed to - their security mission".

In today's digitalized world, organizations are forced to constantly implement new measures to protect their systems and assets. Digitalization has enabled organizations to develop better services and solutions, but this has also resulted in new threats and risks to information and systems. As both information and systems are highly important for organizations to function, they need to ensure both are adequately protected. (Rizal & Setiawan 2023.)

New technology to fight cybercrime is constantly being developed, however, technology will never be able to protect against all existing threats as cybercriminals around the world are always one step ahead, relentlessly seeking to find gaps and loopholes to exploit vulnerabilities. They are not only attacking digital solutions but also focusing efforts on manipulating people. It is often underlined that humans are the weakest link in security, accounting for most security incidents. For this reason, they should be a focus area for any organization seeking to protect itself. (Hayden 2015, chapter 1.)

While employees can act as an extra layer of defense, they can unfortunately also act as an extra attack vector. An attack vector is defined as a method that criminals use to

breach or infiltrate their victim. Cybercriminals have learned that they can bypass technology and security controls by manipulating employees to act on their behalf. Since technology cannot provide full protection, companies must ensure their employees are equipped with the tools they need to fight these challenges, turning them from enabling attacks to defend against them. To do so, organizations should develop an effective security awareness program. (Hayden 2015, chapter 1.)

A security awareness program supports the development and implementation of security policies and establishes the boundaries of acceptable and unacceptable behavior among employees. It aims to limit risks by executing training and communication activities to ensure employees understand relevant security threats and risks, have the knowledge to identify them, and are thereby able to make the right decisions to prevent attacks and breaches. (Gardner & Thomas 2014, Introduction.)

According to SANS Institute (2021), an organization has three types of weaknesses: technical, process, and people. Most security professionals focus on the technical side, such as fixing system weaknesses, but this is not the only type organizations should concentrate on. Most organizations have processes, policies, and procedures in place, but it is not enough for them to exist; they must also be well-designed, implemented, and known to employees. If employees are unaware of them, they cannot comply. The last type of weakness, people, is the most significant one. People are often referred to as the “last line of defense” and are involved in all stages of security, from planning to implementation. People are responsible for the two other weak types: technical and process, and when everything else fails (technology, processes, and controls), people are sent to solve the problem. For people to be equipped with the right level of knowledge on what actions to take, an organization should have an effective security training and awareness program. (Carpenter 2019, chapter 1; Death 2023, chapter 1.)

Chaudhary, Gkioulus and Katsikas (2022) outline the various actions of a security awareness program to include, for example:

- Bringing risks and threats to employees’ attention
- Informing about the consequences of threats
- Providing information about threat actors, their methods, and interests
- Explaining the signs and ways to identify threats
- Promoting existing security measures
- Encouraging employees to use those measures to mitigate threats
- Ensuring employees understand why security is important and what their role is

According to Carpenter (2019, chapter 2.), there are four main reasons why organizations implement security awareness programs: compliance, information dissemination, behavior

shaping, and culture shaping. Understanding “why” a security awareness program is being created will help define “what” actions a program should consist of.

Figure 1. The four reasons why organizations create security awareness programs (Carpenter 2019, chapter 2)

A security awareness program is an important component in protecting organizations against cyberattacks and is therefore often required by regulation or auditors. There are several global and national regulations across industries that require organizations to, for example, conduct annual security training, implement certain policies and practices, or inform employees of security risks and their responsibilities to comply with procedures to reduce risks. Lack of compliance with such laws and regulations can result in significant sanctions or fines. (Carpenter 2019, chapter 2.)

Regulation can be used to justify a security awareness program and investing in it; however, organizations that only focus on compliance often do the bare minimum and simply ensure they run the activities required to be compliant. The challenge: compliance does not necessarily mean that an organization is secure. It can leave significant gaps and a lack of behavior change. (Carpenter 2019, chapter 2.)

In Carpenter’s model, organizations can also choose to focus on information dissemination. As Figure 2 shows, this is the next step from being simply compliance-driven. The intention is to concentrate on information sharing. Focus is put on running communication activities, such as publishing information, and news and informing about policies and guidelines. This approach also provides only limited benefits as such programs are either formulaic or provide information without ensuring the information leads to behavior change. (Carpenter 2019, chapter 2.)

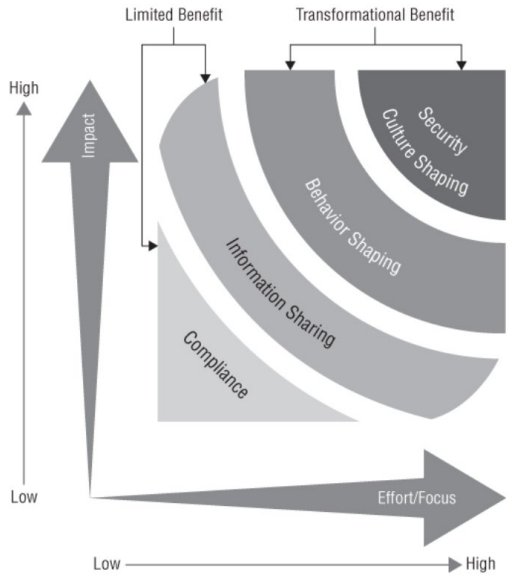

Figure 2. How each of the four “whys” map to a level of effectiveness (Carpenter 2019, chapter 2)

Carpenter highlights that focusing on behavior shaping and shaping security culture creates the most impact. It is also worth highlighting that these two approaches require the most effort. Behavior shaping seeks to influence and manage how employees act, whereas security culture shaping takes a step further because it not only focuses on the actions employees take but also focuses on changing the organization's values, beliefs, and attitudes, in other words, the essence of culture. (Carpenter 2019, chapter 2.)

If an organization is faced with a situation where processes, controls, and technology fail, the last line of defense will inevitably be its people. Hence, people play a crucial role in providing corrective measures and are the main target group for security awareness programs. (Carpenter 2019, chapter 2.)

In 2011, the SANS Institute created the Security Awareness Maturity Model, which was created in collaboration with more than 200 awareness officers. The model has some of the same elements as Carpenter’s model (2019), as it also emphasizes that more mature and successful programs focus not solely on compliance, but behavior and culture change. The SANS Institute model was designed to enable organizations to identify and compare the maturity level of their Security Awareness Program. This model includes five stages: non-existent, compliance-focused, promoting awareness and behavior change, long-term sustainment and culture change, and strategic metrics framework. According to SANS Institute, the most mature security awareness programs focus on behavior and culture change, and measuring the program’s outcome and value to the organization and

its leaders. A more detailed overview of the Security Awareness Maturity Model can be found in Appendix 1. (SANS Institute Security Awareness Report 2024.)

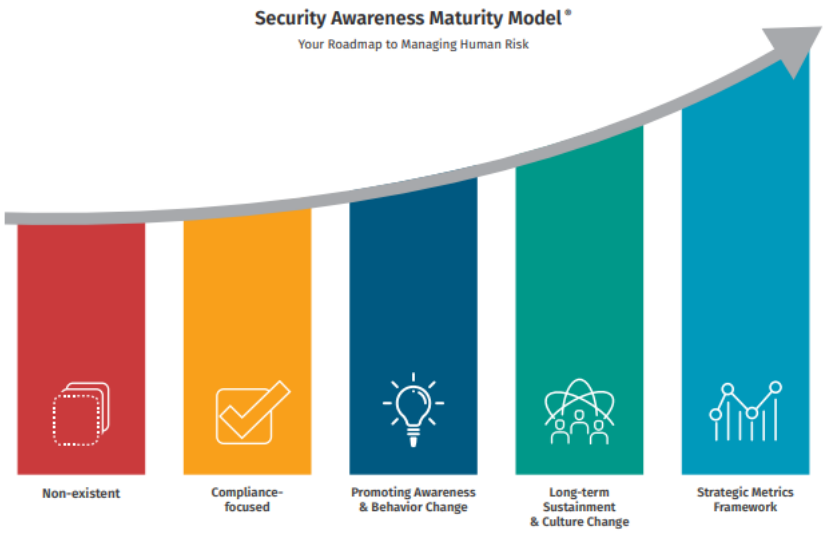

Figure 3. Security Awareness Maturity Model (SANS Institute 2011)

Security awareness is about changing employees' behavior to make the right decisions and to take the right course of action. According to Carpenter (2019, chapter 2.), the challenge lies in the assumption that employees will simply change their behavior if they are provided with the right information and reasoning. Carpenter explains that while people are aware and understand why they should do something, it does not mean they will act in the preferred way. For example, speed limits are set to ensure everyone's common safety; they are mandatory by law, yet many still neglect to obey them. Drivers understand the legal requirement, they understand the reason and risk, but they are willing to accept the risk, knowing they are doing the wrong thing.

Carpenter, therefore, highlights that while a person is aware of something, it does not automatically mean that they care about it, and consequently, if a person does not care about something, they are also unlikely to change their behavior. Hence, the key to changing human behavior is to create a security awareness program that is built based on understanding how to inspire employees to exemplify certain beliefs and behaviors. The messages and topics should resonate with employees and make them relevant and meaningful. (Carpenter 2019, chapter 2.)

Gardner and Thomas (2014, chapter 1) have a different approach from Carpenter, which centers more on the role of a security awareness program to explain company policies, in particular the ones that focus on the usage, incorrect usage, and personal consequences of not obeying the company's communication and information technology rules. While

Gardner and Thomas recognize that making security risks personal for employees, such as explaining how much data their employer holds on them and the possible repercussions if a criminal gains unlawful access to that data, their focus is still on compliance as the ultimate driver for behavior change. (Gardner & Thomas 2014, chapter 1.)

Schroeder (2017, chapter 3) claims that for employees to change their behavior, they must want to change because the change addresses something they want. In other words, change lasts only once a behavior can be replaced by another behavior that provides someone with something they want or need more. For employees to change, they must also be capable of changing and willing to change.

2.2.1 Risks and Vulnerabilities

At its core, security is about managing risks. The security function of an organization varies depending on the company in question and can include functions such as physical security, information, and cybersecurity, as well as data privacy and compliance. Each function has its own responsibility area and looks at security risks from its perspective. (SANS Institute 2021.)

No organization can eliminate all possible risks; they can only reduce the probability and frequency of risks. Hence, the purpose of security is to ensure risks are managed and kept at an acceptable level. Organizations need to define what risk level is acceptable, also known as defining a risk appetite. They must thereafter conduct a risk assessment, which enables an organization to decide which risks need to be prioritized and how to ensure they are kept at an acceptable level. According to Death (2017, chapter 1), a risk assessment forms the basis of a security program, describing the elements of change in an organization. (SANS Institute 2021.)

Understanding the current threat landscape is essential in designing a successful security awareness program. Threats come in many forms, and a good security organization understands the threats it is expected to encounter. Criminals are constantly using new and more sophisticated ways to attack organizations; it is, therefore, crucial to stay on top of recent developments to ensure a security awareness program also addresses recent threats. This is the only way to ensure employees are well-equipped to handle all threats. (Death 2017, chapter 1.)

All organizations are potential targets for criminals. Criminals target their victims in multiple ways, from trying to gain access to their systems, data, or facilities, to stealing goods or even vandalizing them. To protect their assets, organizations need to ensure

they take necessary actions to defend against possible attacks. This includes ensuring proper controls are in place to defend and protect against potential security risks. (Death 2017, chapter 1.)

Cybercriminals use a multitude of ways to attack, manipulate, and gain access to systems and sensitive information. For years, organizations have been focusing on protecting their information technology, implementing the latest virus protection software, configuring firewalls, and securing their networks. Technology has been the main vector to defend against cybercriminals, and it has been highly successful. As technology has become more and more secure, cybercriminals have been forced to find new ways of attacking. They no longer try to gain access through firewalls but try to find ways to go around them by utilizing humans. (Gardner & Thomas 2014, chapter 2.)

Today, one of the most common types of cyber threats is social engineering, which involves manipulating people. Social engineering is a form of hacking where criminals try to access systems or physical locations without having to break into systems. They gain access to wanted systems and information through people, by using various tactics, such as manipulation. Social engineering involves deceiving and manipulating people into either giving sensitive information or access to it. (Speed 2011, 99-100.)

A mature organization has an established department working solely with Information Technology security threats to secure systems and protect the organization from attacks. An information security department is no longer an isolated function, but one that works in collaboration with others to enable businesses to serve their customers and reach their targets by ensuring security threats are adequately dealt with. Security Awareness experts often work in Information Technology or Information Security organizations, and in many cases are assigned to work on security awareness as one task among others. The most mature organizations can have a dedicated team of experts working on security awareness. (Death 2017; SANS Institute 2021.)

To reduce security risks, organizations need to look at their threats and weaknesses and their possible impact. Management needs to understand what weaknesses were identified in the risk assessment; what their impact could be, how likely they are to occur, and what the potential impact is should they arise. Security awareness material should be updated at least on an annual basis to ensure it addresses new and rising threats. (Death 2017, chapter 1.)

Understanding security risks and vulnerabilities is highly important to run a successful security awareness program, but competence in information or cybersecurity is not enough. Clear and concise communication is key for any security awareness program to

be understood and acknowledged. For this reason, Barman (2001, chapter 1) suggests organizations hire an expert communicator with some level of technical knowledge to drive training and communication activities. This will ensure communication is professional and brings credibility to an Information Security department.

2.2.2 Measuring Security Awareness

According to Chaudhary et al (2022), while it is commonly understood that security awareness programs should be adjusted and assessed regularly, a common understanding of what to measure does not exist. Based on their research, past studies on the topic have focused on measuring three areas: audience interest in a security awareness program, the decrease in incidents, and the change in employees' perceptions, knowledge, attitudes, and behaviors. According to Chaudhary et al (2022), the first two do not provide adequate results, as in the first case, it does not measure whether the program has changed behavior, and in the second case, it does not measure whether the possible reduction in incidents is a result of the program. Therefore, they suggest that the third option is the preferred measurement method and should provide the best indication of a program’s success.

Defining a set of measurements that can be applied universally is challenging, as there is no common agreement on the definition of a successful and effective security program. Without this definition, it is difficult to agree on a unified set of predefined metrics. In addition, all organizations have unique needs, which require security awareness programs and metrics to be customized. With this said, Chaudhary et al (2022) have created a set of measures that they claim should provide organizations with a common way to evaluate their security program and be able to benchmark the results between other organizations.

In their research, Chaudhary et al (2022) analyzed 32 research papers to determine what is measured or what is suggested to be measured to evaluate the effectiveness of a security awareness program. The results indicate that the vast majority focused on measuring employees’ behaviors, attitudes, and knowledge. When Chaudhary et al evaluated the various methods used, they found that surveys were the most popular method, as they allowed a large population to be assessed at the same time, and using online surveys was considered easy and cost-efficient. The second most popular method was utilizing passive data, such as reviewing technical logs, the number of security incidents, clicking rates of malicious links, and increases in reported incidents.

The model suggested by Chaudhary et al (2022) includes a combination of a user survey and passive data. Their model is divided into four sections, measuring: employees’ knowledge, attitude, and behavior towards cybersecurity, the direct and indirect value

added to the organization, effectiveness of used awareness resources and delivery channels, and interest and active participation in the program.

According to Solic, Velki, Fosic and Vukovic (2024), five questionnaires have been scientifically validated to measure information security awareness, online behavior, and user knowledge. Two of these questionnaires, the Users' Information Security Awareness Questionnaire (UISAQ) and Behavior Cognitive Information Security Questionnaire (BCISQ), were created by Solic et al, the latter focusing more on psychological aspects. The three other questionnaires are the Security Behavior Intentions Scale (SeBIS), the Four Measurements Scale (FMS), and the Human Aspects of Information Security Questionnaire (HAISQ).

The UISAQ includes a set of 37 items that are divided into four categories: Potentially risky behavior, information security awareness, beliefs about information security, and quality and security of passwords. The questionnaire was conducted on 135 Croatian university students. The revised version of UISAQ was supposed to be published in 2014 to further improve the questionnaire, however, the later and revised version has not been published.

The SeBIS was created by Egelman & Peer (2015) to assess end-user security behaviors. Their questionnaire includes 16 items, which are divided into four categories that measure attitudes towards: choosing passwords, device security, staying up-to-date, and proactive awareness. In this survey, users evaluate their adherence to computer-related security rules. The questionnaire was conducted on 503 Amazon employees who were paid to take part in the study. The challenge with the SeBIS is that it only measures computer-related security behavior, not all aspects of security awareness.

The FMS is designed to measure users' risky behaviors with computers, how cautious users are when using technology, how exposed users are to cybersecurity incidents, and how dangerous users perceive technology to be. FMS thereby focuses on evaluating users' information security awareness and potential risky behavior. The questionnaire was conducted on 39 information security experts and 23 academic personnel in Turkey. The scope of the questions was limited to software and hardware and hence missing other elements of security awareness.

The HAIS-Q includes 63 items that are divided into seven different areas: password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting. Each of the areas is measured separately by knowledge, attitude, and behavior. The questionnaire was conducted on 112 university students and 505 working Australians. Parsons et al (2017) were able to provide evidence that their

questionnaire could show that employees who scored high on their survey scored lower in phishing simulations, demonstrating that employees who had higher knowledge and better attitude and behavior towards security were also better at identifying possible risks. The challenge with this questionnaire is its length, with 63 questions.

The BCISQ questionnaire includes 17 items that are divided into two categories: behavioral elements and cognitive elements. The questionnaire is divided into four sections, two in each category. The first section is a simulation, where the participants' actions or lack of action provide information on their knowledge and behavior. The remaining three sections are self-assessments. The second section evaluates the frequency of behavior, the third is how the participant rates statements in terms of importance, and the fourth asks the participants to evaluate the rate of risk. The questionnaire was conducted with 960 respondents from 41 countries.

According to Fertig & Schutz (2020), the most used tool to measure Information Security Awareness is a questionnaire. Additional and supporting methods include, for example, behavior tests and benchmarking. Many of the questionnaires used focus on measuring knowledge, for example, how many characters a password should be made of.

Based on a literature review conducted by Rohan, Pal, Hautamäki, Funilkul, Chutimaskul, and Thapliyal (2023), multiple models to measure information security awareness have been described in literature. The research of Rohan et al evaluated 24 articles, in which various methods were used to measure different aspects of security awareness. In their research, Rohan et al highlight that the challenge of measuring security awareness is that the concept of information security awareness is very broad, and thus, commonly agreed upon measurements have not been agreed upon. Among the 24 articles that were studied, the scope differed significantly between the studies, from measuring the impact of training programs to measuring much broader areas, such as information security awareness in general or human behavior.

The studies that were conducted in the 24 articles varied in topics, measurements, and target groups. In most of the articles, the study was conducted on one group of people, for example, university students. A few of the articles used by Rohan et al (2023) were no longer available, four referred to earlier mentioned studies (HAIS-Q, SeBIS, FMS, and UISAQ), and some were measuring irrelevant topics.

The remaining seven studies varied in scope: measuring cybersecurity events and training program's impact on cybersecurity awareness (Muhirwe & White 2016), measuring individuals' practices and perceptions regarding cybersecurity (Arpaci & Sevinc 2022), measuring compliance and awareness (Bulgurcu, Cavusoglu & Benbasat 2010),

measuring deviant behavior, specifically misuse and security carelessness (Chu & Chau 2014), measuring organizational information security culture (Nævestad, Meyer & Honerud 2018), measuring internet user cyber hygiene (Vishwanath, Neo, Goh, Lee, Jhader, Ong & Chin 2020), and measuring employee information security behavior (Gangire, Da Veiga & Herselman 2020). The number of questions in the seven surveys ranged from 18 to 75, of which the majority had approximately 27 questions. All the questionnaires used the Likert scale, mostly a five-point scale. An overview of these studies can be found in Appendix 2.

2.2.3 Critical Review of Previous Research

As mentioned earlier, a common understanding of how to measure security awareness does not exist. Several studies have been conducted on various measurement methods, but the vast majority have not been or cannot be applied to a business context.

The presented model created by Chaudhary et al (2022) includes a survey and data metrics. What it lacks is a predefined set of scores or acceptable result levels, which they state is dependent on the organization and its industry. Thus, leaving a potential challenge in accessing sufficient data to benchmark against others. In addition, the model has not yet been scientifically validated.

The questionnaires presented by Solic et al (2024) also have multiple challenges. The sample size in the UISAQ, FMS, and HAIS-Q are relatively small. In addition, two of the models were tested on university students and one on information security professionals and academic personnel. A notable challenge in the three studies and methods is that they have been conducted in either non-business environments or a limited group of employees with a high degree of knowledge in information security. A general model that could be utilized by organizations around the world should be tested in the correct environment, with respondents working for companies, preferably located across multiple countries and industries, and on employees who work for the same company. Models should also be tested on non-technical employees.

The SeBIS questionnaire was tested at a real business, Amazon, and had a high sample size, 503 employees. However, the employees were paid to take part in the study, which could have had an effect on the study results. The questionnaire's scope was also limited to computer-related security behavior. Of the questionnaires, the BCISQ had the highest number of responses (960) and was tested in 41 countries. However, the questions were not business-related, but measured personal security behavior, such as "How long have you been using the Internet?" and "How often do you lend your private debit or credit card(s) and associated PIN(s) to anyone?".

Questions used by Fertig & Schutz (2020) focus on measuring knowledge, such as a good length for a password. It can be argued whether such information could provide accurate and useful feedback, as in most cases the length of a password is limited by default. A question, such as whether employees reuse passwords, would provide better insight into employees' security behaviors and attitudes.

The 24 studies analyzed by Rohan et al (2023) repeated the same trend as in the previous studies, where the number of respondents was very low or the studies were again conducted outside a business environment, for example, on university students. Many of the questionnaires used in the studies included too many questions, for example 75. A survey this long will have an effect on how likely employees are to provide answers.

Therefore, what is missing in the reviewed studies is the application in real-life businesses, across industries and countries, and including a sufficient sample size. A study should be designed for businesses and conducted across several international organizations to provide sufficient results and the possibility to benchmark against others.

2.3 Culture

According to Bashforth (2019), culture is a combination of what we think, how we relate with each other, and how we act; it is built around human behavior. Culture is often linked to how a particular group of people sees the world, including what they believe in and how those beliefs influence the way the group lives. Cultures exist on various levels and ways, for example, residing within a geographical area, belonging to the same ethnicity, or among people practicing the same religion. It may also be experienced within families or even organizations, and it is the core of why people behave in the way they do. (Bashforth 2019, 1-2; Hayden 2015, chapter 2.)

Ferraro and Briody (2023, chapter 1) define culture as everything that people have, think, and do. Their definition has three major structural components: 1. Something people have: material objects, 2. Something people think: Ideas, values, and attitudes, and 3. Something people do: Patterns of behavior. They also suggest that culture is not instinctive or inherited but learned through interaction with others and through cultural content, such as ideas, values, and behavior patterns. The referred-to behavior is a result of learning and interacting with other members of the same culture.

According to Schein and Schein (2016, chapter 1), a certain culture is often difficult to define as there are multiple areas to observe, including the way people speak, behave, or how they identify themselves. The sum of culture is all aspects the community has learned during its process of growing and developing. These learnings are the beliefs, values, and

behavioral norms of the community, and they manifest as culture once they become basic assumptions and, in time, are no longer a part of general awareness.

Culture is, therefore, a shared product of shared learning that defines who the community is and what their shared purpose is. This can be seen as the community's identity: How the community presents itself externally and how it perceives itself to be. This identity is the core of a culture. Schein & Schein (2016, chapter 1) refer to this identity as a community's "cultural DNA" and explain that, being the heart and soul of a culture, culture-change programs can only succeed if they are aligned with the community's cultural DNA. This is particularly important when addressing organizational culture, where culture-change programs are most often executed.

2.3.1 Organizational Culture

All organizations, big and small, create a distinctive culture that evolves over time. The culture reflects the insight the employees have learned and how they have adapted and endured. It is a shared belief of how things are done and encompasses a common behavior and way to function that is understood by all. (Denison, Hooijberg, Lane and Lief 2012, chapter 1.)

An organization's culture is important, as according to research, it has a direct impact on its performance. According to Denison et al (2012, chapter 1), research shows that there are four main ways culture can affect an organization's performance: It creates a common sense of purpose - a mission and direction, adaptability and flexibility, engagement and involves employees, and stability that is built on the organization's core values. An organization where all employees strive towards the same goal will work together to achieve results. They will be able to adapt to change more quickly and will engage with each other more often. All these attributes combined will ensure an organization is stable and ready to deliver high results. (Denison et al 2012, chapter 1.)

Business strategy and culture are two of the top tools for senior leaders to improve performance and guarantee a stable organization, yet most leaders choose to spend most of their time only on strategy and operations. Culture goes beyond strategy, processes and policies, and includes, for example, how employees communicate, their general habits and norms, and how decisions are made by individual employees. Hence, it makes sense to also utilize this vast possibility of leveraging culture and the people who live it day by day. (Bashforth 2019, 10-12.)

Unfortunately, senior leaders often see culture as somewhat vague. Culture can be seen as too difficult or too intangible. But as senior leaders spend time on strategy and

operations, their employees are left without a sense of belonging and feeling of what the organization stands for. As explained by Bashforth (2019), the best-performing organizations are ones where employees' behavior and work methods are aligned and connected to a common purpose and demonstrate shared values. In such organizations, employees are clear on how things are to be done and what their priorities are. Employees do not need lengthy and detailed instructions; they need common core values and principles that matter. (Bashforth 2019, 39-43.)

What is also important to understand is that all cultures are unique, and they cannot be replicated as they are a result of learning over time and the unique people who together create common beliefs, values, and behaviors. This is why it is impossible to reproduce another organization’s culture. No two cultures are or can be identical, just as no two people can. According to Denison et al (2012, chapter 1), the starting point for any organization in creating a culture is to first define its strengths and challenges, which should be used to define values, behavior, and policies that support them. When analyzing organizations' culture Denison et al (2012, chapter 1) use a sixty-item survey that measures four cultural traits: mission, adaptability, involvement, and consistency. The survey results outline the strengths and weaknesses of the organization’s culture and help identify the impact it may be having on the organization's overall performance. (Denison et al 2016, chapter 2.)

As mentioned by Denison et al (2012, chapter 1) the culture organizations have is highly important and can significantly affect an organization’s performance; culture is often heightened when there is a consensus that an organization has a good and generally accepted culture that contributes to the organization’s success. However, culture is also often called upon when something has gone wrong. When organizations have faced catastrophes, culture is often used as the culprit. Media, shareholders, and the board of directors may easily demand that, together with leadership, the organization’s culture must be examined. Culture is often pinpointed as the reason for poor decision-making, the reason employees and leaders fail to understand risks. (Kartchner, Bowen and Johnson 2023, chapter 1.)

While culture can be a binding force, gathering like-minded people together, it can also blind the common group or community. Communities that have shared values and beliefs tend to draw on actions that they see as acceptable and within the values of their community. They can easily fall prey to doing things the same way they have always been doing, and this can lead to problems. This is why addressing culture is vital. (Kartchner et al 2023, chapter 1.)

2.3.2 Culture Change

The need to change something is the result of dissatisfaction and disappointment, for example, negative results, a decrease in sales, or employees unexpectedly leaving an organization. This often sparks the need to change. To get employees to take part in change, they need to be motivated to do so. They need to understand the problem and why change is needed, but this alone is not enough. When change occurs, employees often feel fear or anxiety about the unknown and how they will cope. This naturally leads to resistance to change. (Schein & Schein 2016, chapter 2.)

The challenge of managing and transforming culture is that there are countless ways of doing it. A “one size fits all” method does not exist, since all organizations have their own culture, created and molded by the various and unique people within the organization. Culture can be altered in multiple ways, but there are a few key methods that should be utilized to gain results. First, top-down one-dimensional communication from senior management to employees no longer works and will not result in successful cultural change. Since an organization’s culture is created and transmitted by all employees, everyone must be involved and engaged. (Hayden 2015, chapter 2.)

Once an organization has succeeded in getting employees engaged, it needs to find a level of consensus on the needed change. Without common agreement on the direction and transformation, employees might end up working against each other. In the information security area, this is particularly challenging as security is seen as a blocker for business instead of an enabler and ally. With the constant rise in security incidents, this view should be changed and a consensus found. (Hayden 2015, chapter 2.)

Cultural transformation programs often fail due to a lack of proper follow-up and measurement. Too often, organizations run a transformation program and assume it has been successful simply by completing all the activities, such as communication with employees. However, no organization should invest in culture transformation without seeking better business outcomes. (Hayden 2015, chapter 2.)

According to research, organizations with good cultures outperform others. For this reason, it is critical to measure culture change: Is culture improving performance, and what is the link between culture and performance? In other words, how much does changing culture change performance? If there is no relationship between the two, there is no point in trying to change the culture in the first place. Finally, while culture change fails when senior management dictates it, they do have a critical role in setting the direction and ensuring that the change and communication are done in the right way. (Hayden 2015, chapter 3.)

2.4 Security Culture

The term “security culture” is being used in organizations more often, however, organizations struggle with understanding what it means, and more so, how to accomplish it. Roer (2015, chapter 1) defines security culture as “The ideas, customs and social behaviors of a particular people or group that helps them be free from threat and danger.” Like Roer, Laycock, Petrič & Roer (2019) define security culture as “The ideas, customs and social behaviors of a group that influences its security” and the Information Security Forum (2024) as “For organizations, the sum of its behaviors”. Dhillon (1997) defines it as “the totality of human attributes such as behaviors, attitudes and values that contribute to the protection of all kinds of information in a given organization”.

These definitions strongly suggest that human characteristics are key attributes in security culture. Martins and Eloff (2002) also emphasize the role employees play in protecting data by describing security culture as an “assumption about perceptions and attitudes that are accepted in order to incorporate information security characteristics as the way in which things are done in an organization, with the aim of protecting information assets”.

In a study conducted by Longitude and Financial Times in 2020, researchers discovered that 54% of respondents to their survey admitted to bypassing their organization’s security policies within the past year. This strongly indicates that employees knowingly expose their organizations to vulnerabilities. The study also revealed that nearly 40% of employees said cybersecurity had nothing to do with them, which suggests that a significant number of employees do not understand their role in protecting their organization. The study concluded that a strong cybersecurity culture will reduce an organization’s human vulnerabilities if it is done in a way that promotes behavior change by motivating employees to think and act differently. A strong security culture is not about strict policies and rules, but about empowering employees to be aware of risks and to be proactive in tackling them. (Fujitsu 2020.)

With the increase in data breaches and their associated high cost, organizations are progressively looking at their employees to create an extra layer of defense. This is achieved by focusing on security awareness and, more so, the security culture of an organization. Developing and fostering a strong security culture is an effective way for an organization to minimize security risks and ensure employees take action to protect the organization. According to Hayden (2015, chapter 3), culture is the most unused and important resource for enhancing information security.

In a study conducted by Uchendu, Nurse, Bada and Furnell (2021), they analyzed 58 research articles on security culture and how security culture is defined. Most of these

definitions referred to values, the attitudes of employees, and their assumptions. Security culture was also defined as a subset of organizational culture, and having a strong link to security awareness.

According to Hayden (2015), security culture is most often a subset of an organization's overall culture, as in large organizations, multiple security cultures can exist, for example, within different countries, business areas, or teams. Often, the security organization has different values and opinions on what to protect or prioritize than other parts of the organization, such as Human Resources or Sales. In some organizations, these beliefs and cultures can coexist, however, they can also clash, resulting in overall prioritization of resources or budget, and thus affecting the information security across the organization. (Hayden 2015, chapter 3.

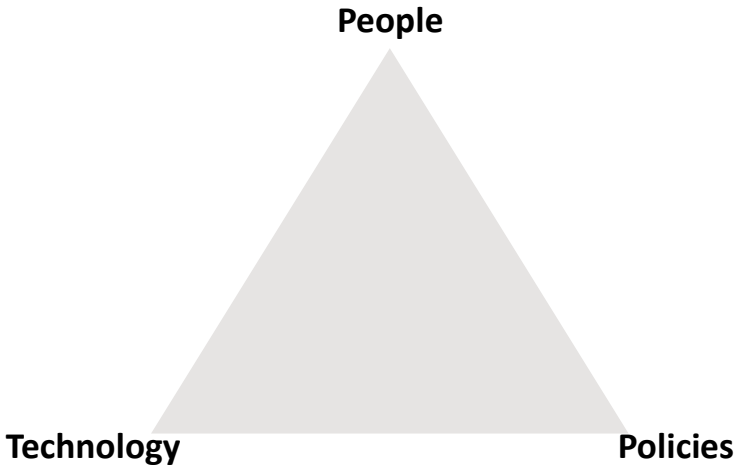

Figure 4. Key Elements of Security Culture (adapted from Roer 2015, chapter 2)

According to Roer (2015, chapter 1), all social behaviors impact an organization's security culture, and vice versa; security culture influences social behaviors. By creating awareness around security topics, an organization can influence its employees' security behaviors, which ultimately results in changing the organization's security culture.

According to Roer (2015, chapter 2), the key elements that create a security culture are people, policies, and technology. All three elements are interconnected, hence should one element be changed, so will the others. Therefore, it is important to always consider the effects of all three elements when conducting change. In this context, Roer defines policies as generally recognized and known rules that regulate ideas, norms, and social manners. He defines technology as any tool that is used in a defined way, and people as the ones who use technology and who follow or disobey policies.

According to Roer (2015, chapter 2), the society we are raised in defines the policies we live by and the tools we choose to use. This shapes our social behavior, and by understanding how they are linked, we can use them to shape and retain security culture.

Hayden (2015, chapter 5) has created a model, the Competing Security Cultures Framework, to measure security culture. Hayden's model has been adapted from well-known organizational culture literature but focuses on describing and interpreting how security is understood and practiced within an organization. Specifically, the model focuses on identifying where competitive principles and values arise to highlight where the greatest risks to an organization's security goals and objectives are. The Competing Security Cultures Framework is built on the Competing Values Framework by Quinn and Rohrnaugh (1983) but from a security perspective.

The Competing Values Framework by Quinn & Rohrbaugh (1983) seeks to understand what characteristics and organizational qualities could be linked with a company's performance. Based on their research, Quinn & Rohrbaugh were able to group organizational traits into core values that created certain cultures within organizations. They discovered, for example, that some organizations were more successful when they had strong hierarchies and bureaucracy to accentuate control and solidity, while other organizations thrived when they were flexible and adaptive. These arousing patterns were divided into four groups of organizational values and their cultures. (Hayden 2015, chapter 5.)

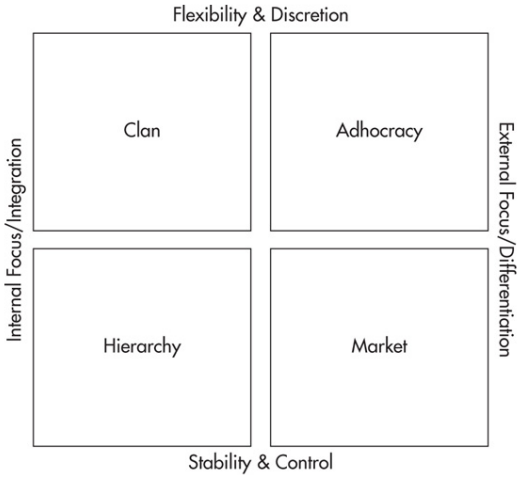

Figure 5. The Competing Values Framework (Hayden 2015, chapter 5)

The clan culture in Figure 7 is one of four organizational behaviors and refers to organizations with a culture of community, where employees value inclusion and a sense of belonging. These organizations emphasize flexibility, personal development, and

responsibility, and are more internally focused, wanting all employees to contribute to the organization's performance. (Hayden 2015, chapter 5.)

Organizations with an adhocracy culture work well with an ad hoc approach. They are flexible by nature, valuing agility and innovation. These organizations are often startups or organizations creating highly innovative solutions and working in a space of unpredictability caused by external factors. Such organizations need to adapt to change quickly to succeed and perform well. (Hayden 2015, chapter 5.)

Market cultures prioritize customers and key relationships, such as relations with partners and regulators; performance is seen as possible through excellent relations with others. While focusing on their stakeholders, they keep a tight grip internally within the organization. (Hayden 2015, chapter 5.)

Organizations with hierarchies emphasize high control, are internally motivated, and focus on being stable. The organization has strict rules and processes, and roles and responsibilities are clearly defined. The culture is formal, highly organized, and hierarchical, where stability overrules adaptability. (Hayden 2015, chapter 5.)

Hayden has used the Competing Values Framework as a basis for his model, as it helps to explain the conflicts and opposing priorities that frequently lead to security risk and failure. Hayden's Competing Security Cultures Framework is adapted to the information security area and focuses on specific characteristics that either improve or hinder security performance in distinct industries or certain circumstances. The model also aims to capture the people-centric approach to security culture. (Hayden 2015, chapter 5.)

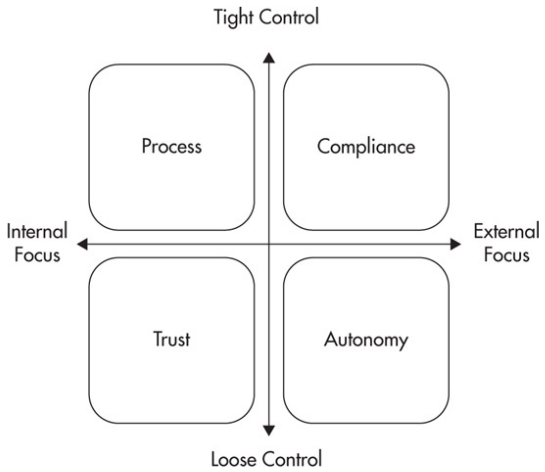

Figure 6. The Competing Security Cultures Framework (Hayden 2015, chapter 5)

As can be seen from Figure 8, the Competing Security Cultures Framework mimics the Competing Values Framework with a similar two-axis diagram, however, it focuses on highlighting and applying this to information security. The diagonal axis corresponds to how much an organization values security control, whereas the horizontal axis corresponds to how much an organization focuses on internal versus external environments. (Hayden 2015, chapter 5.)

In the Competing Security Cultures Framework, the diagonal axis represents the spectrum of control an organization has over security. On one end of the spectrum is losing control, and on the other, tight control. This represents organizations that have lost control, where the level of security can fluctuate across the organization, and organizations that have tight control, where security is built on standards and focuses on ultimate stability. These two examples are complete opposites, and most organizations lie somewhere in between, perhaps leaning towards one or the other. The axis reflects the values an organization must have to make security more effective, but in two opposite ways: by promoting a strict and orderly environment or encouraging a flexible and situation-based approach. (Hayden 2015, chapter 5.)

Control is often enforced by assigning authority, hierarchy, and setting in place documented processes and procedures that define appropriate behaviors. Depending on the organization, control over security is implied by many factors, such as the size of a security team or function, support from senior management, or the magnitude of the mandate given. In Hayden’s model, control has been moved to the top of the diagram, versus in the original Competing Values Framework. This has been done to emphasize that security cultures with tighter control are exemplified in the two top quadrants (Process and Compliance), and to highlight that security culture is most often a control-focused culture. (Hayden 2015, chapter 5.)

The horizontal axis on the Competing Security Cultures Framework shows whether an organization is concerned with understanding and managing security internally within its organization or externally towards stakeholders. In an organization that focuses on internal programs, security is seen as efficient when it is aligned across functions, and the result is a consistent organization-wide program that protects the organization's information assets. On the other spectrum of the axis are externally focused security programs, which are considered successful when they result in good relations between the organization and outside stakeholders. This creates a need to meet contractual and regulatory obligations, protect data, and avoid security failures that could result in reputational loss or the inability to execute business. To support this model, organizations

may need to spread responsibility for security to various teams or units to ensure the different needs of the numerous external parties are fully met. (Hayden 2015, chapter 5.)

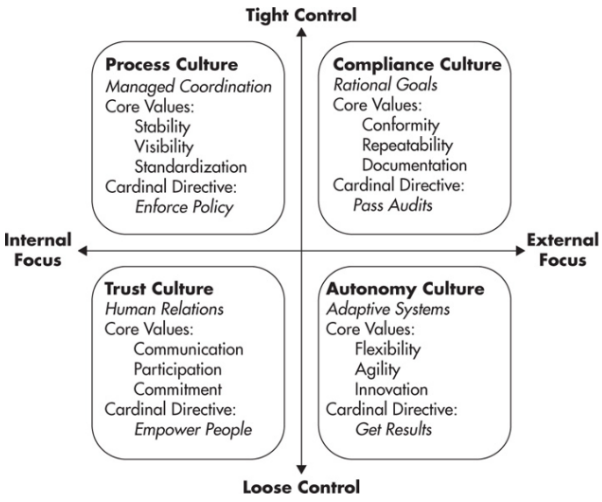

Figure 7. The Competing Security Cultures Framework with expanded details (Hayden 2015, chapter 5)

The different quadrants of the Competing Security Cultures Framework show in more detail the values and components of each security type. Each of the quadrants includes a group of values, assumptions, and priorities that impact how security decisions are made and activities run within an organization. Ultimately, all organizations are a mix of cultures, and hence, most organizations can identify themselves in a mix of the quadrants. Nevertheless, understanding this framework and where an organization fits in provides input on what to possibly shape and how to communicate within an organization about its security culture. (Hayden 2015, chapter 5.)

To measure where an organization is placed on the Competing Security Cultures Framework, Hayden has created a diagnostic tool with ten questions. The Security Culture Diagnostic Survey is presented in Appendix 5. (Hayden 2015, chapter 6.)

2.4.1 Changing Security Culture

Hayden (2015, chapter 1) highlights that a key distinguishing feature of culture is that it is. for the most part, invisible, something that occurs in our subconscious mind. In his opinion. security culture is not about technology or controls, it is about changing what an organization thinks and believes, and what security means to an organization. Policies, processes, and technology are in place to support employees, but people are the ones who define what they are, do, and protect, ultimately being responsible for the security and how it is implemented.

The seven dimensions of security culture, as described by Carpenter and Roer (2022, chapter 6), are codependent, observable, and measurable. They are key in understanding security culture and how to intentionally influence and develop it. The seven dimensions that capture the phenomenon of security culture include: attitudes, behaviors, cognition, communication, compliance, norms, and responsibilities.

Figure 8. Visualizing the seven dimensions of security culture (Carpenter & Roer 2022, chapter 6)

Figure 8 visualizes how the seven dimensions are connected. Attitudes focus on what employees feel: to what extent they care about security and whether their attitude is positive, neutral, or negative. Employees' overall attitude towards security is a critical factor, as studies have shown that the best predictor of an employee's behavior is not their acquired knowledge, but their attitude towards security. (Carpenter & Roer 2022, chapter 6.)

The second of the seven dimensions (behavior) defines what is considered acceptable actions and how employees perceive other employees' actions. Employees are likely to assume the behaviors they observe from others, and over time, these will become common ways of behaving. (Carpenter & Roer 2022, chapter 6.)

Cognition focuses on what employees know, how they learn, and how they apply their learned knowledge. The knowledge employees acquire can affect their behavior; however, this knowledge does not necessarily mean they will act in a preferred way. Thus, while training employees is an important part of security awareness programs, it is only one dimension. It should be supported with strong messaging from senior management that clearly explains why security is crucial for their organizations and their success. Furthermore, activities such as providing rewards and reinforcement can have a positive influence. (Carpenter & Roer 2022, chapter 6.)

Communication refers to how security is communicated across an organization, to what degree their leadership is involved, and whether security is deemed a core value. Carpenter and Roer (2022) highlight the role of senior management in communicating their vision and repeating the organization's values regularly, as this will ensure employees understand what is expected from them and the behaviors they should show. (Carpenter & Roer 2022, chapter 6.)

Compliance refers to how well employees adhere to policies and procedures. All organizations need rules that address what is allowed and what is not. Regardless, in many organizations, employees do not act correctly. This may be because employees are simply not aware of the existing rules, or they are too difficult to follow. A security awareness program should therefore address how to communicate these rules and ultimately how to ensure compliance. (Carpenter & Roer 2022, chapter 6.)

Norms refer to what employees see and to what extent security beliefs, behaviors, and values are rooted in the norms and unwritten rules of an organization. Norms comprise of informal rules, rules that are not official and written down. Research shows that employees are more likely to adhere to norms than official rules, as these are seen as a “normal way” for employees to act. A solid security awareness program addresses the difference between norms and policies and seeks to influence employees' behavior to align norms with the organization's policies. (Carpenter & Roer 2022, chapter 6.)

The last of the seven dimensions (responsibilities) refers to what extent employees feel they are empowered to make security decisions and to what extent they will help ensure that other employees follow the organization's security rules. Communicating employees' responsibilities should be done by focusing on positive change and by making them understand that even small changes and actions can make a big difference. (Carpenter & Roer 2022, chapter 6.)

Roer’s Security Culture Framework was created to address the lack of focus on the human aspect of security. This framework was created due to the overall lack of an existing model that took into consideration the human element. Security awareness programs tended to rely heavily on employee training, which was often information-focused and pinpointing mistakes employees made. Roer’s framework, therefore, incorporates the human element and focuses on using employees as an extra asset. (Roer 2015, chapter 7.)

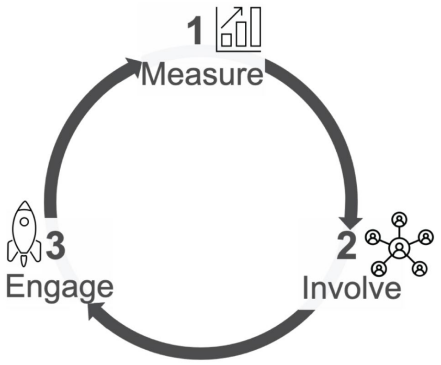

Figure 9. The Security Culture Framework at a glance (Carpenter & Roer 2022, chapter 8)

Roer's Security Culture Framework reflects a continuous cycle that should be completed in succession, starting from the measure, continuing to involve, followed by engagement. All three steps create specific output that is transferred to the next step. Completing a full cycle should result in the ability to document change, and most significantly, the improvements that have been made to the security culture. The Security Culture Framework is designed as a continuous cycle that is repeated regularly, for , on an annual basis. (Roer 2015, chapter 7.)

The first step of the framework (measure) includes identifying differences between an organization's existing culture and the preferred state, including setting concrete goals for the organization's security culture. Carpenter and Roer (2022, chapter 8) suggest that there are multiple ways of measuring culture, but regardless of the chosen measurement, the most important aspect is to ensure that the measurement can be repeated. The measure phase consists of three different actions: defining a baseline (as-is state), deciding where the organization wants to be in terms of its security culture (to-be state), and finding the gap between the baseline and the to-be culture.

In the initial stage of defining the as-is state, it is important to choose metrics that can be repeated and are likely to be relevant during the next five to ten years. The as-is state is measured in the beginning, but it is also revisited regularly to analyze if the security culture has improved. By choosing metrics that measure the same phenomena with the same methods, organizations can ensure their results are comparable throughout the years. Defining a to-be state ensures the organization has a clear understanding of what it wants its security culture to look like and how to reach it, as this stage defines the actions and focus areas of the security awareness program.

Carpenter and Roer (2022, chapter 8) suggest setting three different goals for the to-be state: a long-term goal of three to five years, an intermediary goal of one to two years, and a per-iteration goal. Long-term goals should be strategic and support the organization's

overall business goals. Iterative goals should include smaller, bite-sized goals that help achieve the longer-term goals. Once the as-is stage and the to-be state have been defined, organizations should compare them to understand how far they are toward the goal. This stage will also assist in understanding if the goals are realistic or whether they should be more reasonable and attainable.

The next step in the Security Culture Framework is involve, which focuses on creating support with important stakeholders and understanding target audiences. During this step, organizations often seek to identify employees who can help promote the organization's security culture towards other employees by acting as so-called security ambassadors or champions. These individuals engage with other employees, act as role models, and help drive positive culture change. (Carpenter & Roer 2022, chapter 8.)

To gain traction for a security awareness program, it is important to ensure support and alignment with key stakeholders. This includes, for example, senior management and relevant departments, such as Cyber Security, Human Resources, and Marketing. Key stakeholders can help outline the organization's top security risks and unwanted behavior from employees, which can be utilized to create target audiences for security awareness activities. The earlier chosen security culture goals should also be used to assist in choosing target groups. An organization can choose to focus on a specific goal or choose multiple ones. (Carpenter & Roer 2022, chapter 8.)

The final step of the Security Culture Framework (engage) includes the activities and content that will be directed toward the target group(s) and used to reach the earlier defined goals. In this step, organizations match the goals set in the measure-step with the target groups defined in the involve-step, to decide what activities and topics to include in the security awareness program. Activities can include, for example, e-learning, videos, games, posters, newsletters, and reminders. Once all three steps of the Security Culture Framework have been completed, the steps are repeated. (Carpenter & Roer 2022, chapter 8.)

The Security Culture Framework has been designed to be simple enough to be used by organizations of all sizes, and it is highly adaptable. Using a documented framework is also important as it can serve as documentation of the process and steps taken should an organization be hit with an incident or breach. This documentation can be used to prove that the organization has taken necessary steps to address the human layer in their security and that action has been taken to reduce risks and improve security. (Carpenter & Roer 2022, chapter 8.)

Since an organization’s security culture is shaped by the daily choices, relations, and attitudes of its people, changing its security culture is a lengthy and difficult process, as it requires changing the way people think, not just how they act. Like the SANS Institute Security Awareness Maturity and Carpenter’s Security Culture Shaping models, Hayden (2015, chapter 1) also highlights the importance of taking a people-centric approach to security culture. This means putting employees at the center of an organization's security challenge and stressing their central role in solving them, in contrast to emphasizing how employees contribute to security challenges.

Both SANS Institute (2021) and Carpenter (2019, chapter 1) state that most organizations take the easier route of designing a compliance-driven security awareness program. Hayden (2015, chapter 1) also highlights the challenges from a security culture perspective: Regulation often aims at ensuring organizations take security more seriously while forcing organizations to make important improvements. The challenge, however, is that compliance does not necessarily mean something is more secure. This can be seen in various cases where IT systems have been signed off by auditors yet have ended up being compromised by a cyber-attack. The challenge lies in the fact that compliance often looks at things from a singular point of view, forgetting the bigger picture, resulting in the idea that if auditors are satisfied, the organization itself must be secure and protected. This, unfortunately, is not the case, and where security culture steps in. A solid security culture ensures employees take a more people-centric and broader view; by nature, they question and raise issues from a wider security perspective and see the overall risks, not just what ensures the organization is compliant. (Hayden 2015, chapter 2.)

A people-centric security culture focuses on employees - individuals, and how they have a central role in solving security problems. While all employees are needed and can contribute, according to Hayden (2015, chapter 5), four groups of employees have the greatest chance of changing an organization’s security culture: senior management, security awareness teams, security researchers, and security practitioners.

Senior management has the greatest possibility to influence an organization through their decisions and actions. They can dictate the rules by which the organization is to live, but if they do it in the wrong way, the results will not change the security culture for the positive. Hence, management’s most important role is to live and breathe their culture; to serve as role models, and to show employees what their security culture should be. In addition to management buy-in, organizations focusing on security awareness should have an employee or employees and/or a team dedicated to running security awareness activities. This also includes acting as “cultural change agents”. Due to their work, these individuals

already understand the need for a people-centric security culture and are the key people to drive it within their organization. (Hayden 2015, chapter 2.)

The third group of people who can influence an organization's security culture is what Hayden (2015, chapter 2) calls Security Researchers. These are the individuals who think in different ways, always seeking new ways of doing things (good and bad) in the information security space. These individuals not only bring attention to challenges but also new solutions and innovative ways of thinking. The final employee group that can influence security culture is security practitioners, the people who ensure that the daily work around information security functions properly. Hayden (2015) argues that you cannot change the security culture without them, as they live in the security culture each day. Security practitioners have two key roles: they provide knowledge and insight on how the security culture functions – where it works and where it does not, and take an active role in changing what they can towards a better security culture.

While Hayden (2015, chapter 2) identifies the above-mentioned four employee groups with the greatest effect on changing an organization's security culture, he also highlights that the core of a people-centric security culture is engaging with the people outside the security area. To be successful, an organization must adopt the values and priorities of the larger organization and its people and understand what the world looks like from their perspective. This means that communication must not be purely pushed by the security function towards the organization, but rather a collective way of engaging and interacting. (Hayden 2015, chapter 2.)

According to Martins & Eloff (2002), creating an information security culture is a challenging task that requires multiple years to achieve and is affected by numerous aspects. Culture reflects how things are done and, therefore, derived from employee behavior or through a group of people from organizational behavior. Martins & Eloff (2002) define organizational behavior as focusing on three separate levels: individual, group, and organization. All three levels need to be addressed when implementing a security culture within an organization. From an individual point of view, employees should be encouraged to instill the correct security behavior. From a group-level perspective, management’s attention and support are needed to enable success, and from an organizational level, processes and structures must be applied to ensure employees know how to behave.

On an organizational level, policies and processes should exist to ensure employees are aware of them and they are educated to understand and apply them. With time, this behavior should evolve to be part of the organization’s information security culture. This also applies to the other identified elements, such as analyzing risks, benchmarking

against other organizations, and having a sufficient budget. They all play an important role in creating an information security culture. (Martins & Eloff 2002.)

Management must show support and create an environment of trust. Mutual trust between management and employees ensures new processes and procedures are easier to implement and supports employees in changing their behavior. Each employee contributes to an organization's information security culture by adhering to the correct behavior, but this requires that the organization is successful in communicating what behavior is needed from employees and why. (Martins & Eloff 2002.)

Organizations are constantly faced with change, for example, digitalization, competition, and world economics. These are all issues that organizations need to tackle at all levels of an organization, and they all affect an organization's information security culture. By overcoming them in the right way, an organization can create a solid information security culture that contributes to satisfied customers and productivity. (Martins & Eloff 2002.)

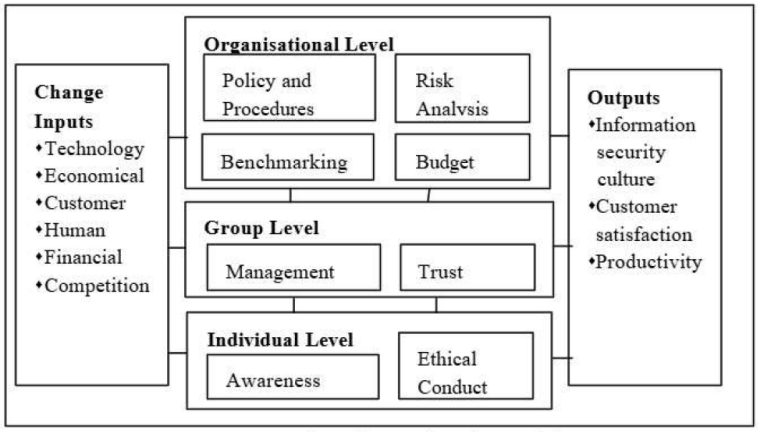

Figure 10. Information security culture model (Martins & Eloff 2022)

An organization's security culture is ultimately the sum of its common values and beliefs. By focusing on their security culture - their values and beliefs, organizations can succeed in reducing their information security risks, increasing their value, and avoiding security incidents. To understand what an organization's values and beliefs are and where they stand, they need to begin by defining their baseline: What does the organization's security culture look like, and how can it be measured? (Hayden 2015, chapter 5; ISF 2024.)

2.4.2 Measuring Security Culture

Changing or managing an organization's security culture requires understanding what security culture is, how it manifests, and how it can be measured. In other words, how it is defined, observed, and assessed. Assessing security culture can be done by using both qualitative and quantitative measurements, both of which should be used to understand

what is happening below the surface. Combining qualitative and quantitative data enables organizations to measure the link between culture and action. Quantitative data provides real numbers, while qualitative data provides insights, such as why something happened or tends to happen. (Hayden 2015, chapter 5.)

To demonstrate the value of a security awareness program and why investing in creating a solid security culture is important, security teams must also provide proof that their actions are creating behavior change and thus contribute to decreasing security risks. This requires developing metrics and key indicators to measure change and return on investment. (ISF 2024.)

According to Orehek and Petrič (2021), measuring security culture reliably and validly is challenging, but not impossible. By measuring security culture, an organization can gain feedback on employee behavior, how important they and their colleagues perceive security to be, as well as their knowledge of information security. This information should enable an organization to understand its weakest links and thereby enable it to address these weaknesses to improve its culture.

According to ENISA (2021), commonly shared and approved methods to measure cybersecurity culture do not exist, which leads to fragmented ways of working and measuring. When organizations do not know what measurements to use, they often do not collect them at all. ENISA suggests that analysis should focus on measuring perceptions, attitudes, and knowledge, which should provide input on what measures to take to protect one’s digital environment. ENISA also suggests using quantitative methods to gather information about people's behavioral patterns and thinking around cybersecurity, which should be combined with statistics on cyber incidents to identify patterns and trends, and to determine what mitigation actions to implement.

Orehek & Petrič (2021) also claim that employees answers to surveys should be compared and validated with evidence. If employees report to be complying with security rules, this should be evident in data, such as a low level of security incidents. Therefore, there should be a correlation between answers and actual employee behavior. If such a correlation cannot be seen, it is suitable to assume that employees have answered questions with bias, such as social desirability bias. This can occur when a survey is conducted in an organizational setting, where employees might feel obligated to answer questions in a certain way or feel they are being observed. This can lead to employees providing answers that mimic security rules rather than reality. This sensitivity to answering security-related behaviors honestly is problematic in effectively measuring security culture.

According to Da Veiga (2018), the first step in improving an organization's security culture is to begin by assessing the organization's existing culture. It is imperative to understand the current situation before taking action to change it. Assessing the current situation creates an understanding of where to start and what employee behaviors need to be monitored and changed. This will define the objectives for an annual security awareness program, which should be assessed on an annual basis and adjusted accordingly.

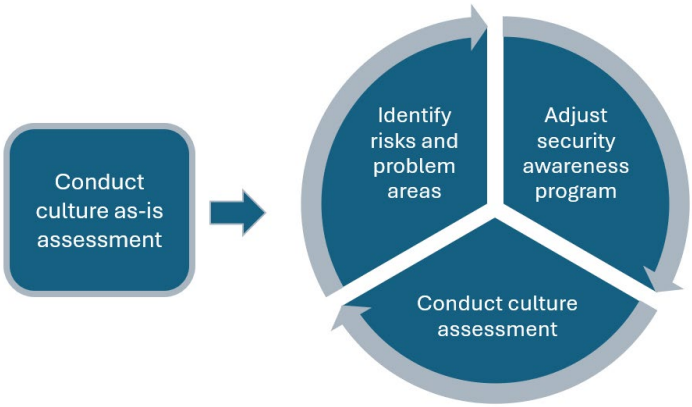

Figure 11. Steps used to improve security culture (adapted from Da Veiga 2018)

Hayden (2015, chapter 5) suggests that both qualitative and quantitative measures can be used to measure culture. His method, the Competing Security Cultures Framework, is designed to measure security culture and has been adapted from well-known organization culture literature, but focuses on describing and interpreting how security, in particular, is understood and practiced within an organization.

According to ISF (2024), each organization should create measurements which apply to them. Organizations need to understand their security culture: What is the security culture of the organization, and particularly what are its strengths and weaknesses. By understanding the as-is situation, an organization is better equipped to take appropriate action. When measuring and assessing the progress of a security awareness plan, thereby the security culture of an organization, it is important to evaluate how successfully results and processes have been achieved and whether there are any residual risks or gaps. This will help steer what actions to take once the culture has been measured. (ISF 2024.)

ISF (2024) suggests using methods such as employee surveys to measure behavior change, track demand to participate in security exercises, measure the number of human-related incidents, and preferably correlate this with the number of training and activities provided, and track how many security concerns or incidents have been raised by employees.

In 2015, Roer and Petrič created the Security Culture Survey to create a scientifically accurate way to measure security culture. The Security Culture Survey has seven dimensions to measure security culture: attitudes, behaviors, cognition, communication, compliance, norms, and responsibilities. The survey results provide a comprehensive overview of each dimension and how the organization is performing in each area. The survey has been created in a way that should provide honest answers and avoid employees answering what they think they should answer. This is achieved by asking questions on how they see other employees behaving and what they generally see as acceptable values and behaviors within their organization. (Carpenter & Roer 2022.)

According to Carpenter & Roer (2022), security culture can be measured most accurately from a group perspective, not by focusing on what employees do or know as individuals, but by focusing on their observations and perceptions of the organization. Culture can be measured in multiple ways, such as observation, experimentation, and interrogation (surveys and interviews). An organization's security culture can be observed by identifying patterns and behaviors, for example, observing whether employees lock their laptops when not in use, adhering to the clean desk policy, or watching out for tailgating. All these activities can be observed and should give an indication of the general security culture; however, it might be difficult to compare results over time as situations can differ. Experimentations are often used to understand behavior, and a common cybersecurity experiment is to conduct phishing simulations, where employees are sent emails disguised as phishing emails to test if employees can recognize high-risk emails and whether they take appropriate action and report them. Finally, surveys and interviews are excellent methods to gather information on employee behaviors and attitudes. (Carpenter & Roer 2022.)

In the earlier introduced SANS Institute Security Awareness Maturity Model (Figure 3), the final step is the Strategic Metrics Framework, which is for organizations that have implemented the most advanced security awareness programs, the focus is not only on culture change but also on how to measure impact. The most mature security awareness programs are aligned with the organization's goals and have metrics in place to measure tangible impact, including employees' behaviors, attitudes, and perceptions. Metrics are measured continuously and over a longer period to demonstrate long-term impact and to expose trends that may not be evident via short-term data.

The SANS Institute's (2021) approach to measuring culture change focuses on clear metrics that measure outcomes and concrete behavior. Instead of only observing employees or asking them questions, SANS Institute also relies on data, such as how many employees fail phishing simulations or the number of employees using secure

passwords. As these results improve, so does behavior and thus an organization’s security culture.

Setting clear metrics enables organizations to manage and improve their security culture in a more structured way. They can be used to answer questions, such as “what is the organization currently doing right”, “how can they improve”, and “what needs to be changed or focused further on”. In addition, metrics enable organizations to communicate the impact and value that their security awareness program is delivering to the organization's security culture. (SANS Institute 2021.)

Regardless of the measurement method, it is important to ensure that employees do not experience in any way that the honest answers they provide will have any repercussions or impact on their job or status within their organization. If this cannot be achieved, it can be assumed that the answers provided by employees will be influenced by social desirability bias. (Orehek & Petrič 2021.)

2.4.3 Measurement Options

Wilson and Hash (2003) have defined three security metrics to measure: execution of security policy, security service delivery, and consequences of security events. They suggest using measurement techniques such as interviews, reports, surveys, focus groups, benchmarking, evaluation forms, and independent observations. ENISA (2021) finds that used measures should be based on the maturity of an organization and, more so, focus on employee behavior, utilizing behavioral measurement theories. This includes utilizing survey-based questions with possible interviews and interactive methods to gather data.

Quantitative research provides insight based on numerical data, whereas qualitative research is based on non-numerical data, such as words, emotions, and experiences. Interviews are qualitative because they consist of the interviewee’s opinions and experiences. There are multiple different kinds of interview methods, such as structured and semi-structured interviews, theme interviews, in-depth interviews, and focus groups. The biggest differences are how open and closed the interview questions are and the flexibility of the interviewer when interviewing. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

A structured interview is used when collecting facts and when using the same questions to interview a larger group of people. After interviews have been conducted, they are transcribed and analyzed. In a structured interview, questions have been created in a specific order that must be used during the interview, but in a semi-structured interview,

the order has been pre-defined, however, the interviewee can change them on the go as well as the questions themselves. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

In an in-depth interview, the discussion between the interviewee and interviewer is confidential to encourage the interviewee to share their views. In an open-ended interview, a certain theme is discussed openly between the interviewer and interviewee. This method is used, for example, when investigating the importance of a phenomenon, when background work must be done before quantitative research, when quantitative research has been completed, or to validate a measurement instrument. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

Focus group interviews are usually organized for six to twelve people. This method allows a deeper discussion within a group. The discussion is run by one or two interviewers who provide a topic and ensure that the discussion is kept on track. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

An interview will include a set of questions, but the answers, both in terms of content and length, vary depending on the interviewee. The results should be analyzed and interpreted, and can be coded for patterns. As open-ended interviews can create a vast amount of data, depending on the length of the answers and the number of respondents, it is worthwhile narrowing down the questions to be rather specific. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

As suggested by Carpenter & Roer (2022), security culture can also be measured in other interactive ways, such as observing and experimenting. Such activities can include, for example, phishing simulations, red teaming activities or simply observing employees' behavior in specific situations. Red teaming activities are ones in which security professionals simulate real-life security situations to gain access to an organization's systems, data, or premises. Such activities could include, for example, trying to access premises by pretending to be someone else or pretending to have access to confidential systems. As alternative measurement methods, SANS Institute (2021) suggests using methods such as Net Promoter Score, focus groups, or interviews.

In addition to the above-mentioned options, organizations should also look at quantitative measurement methods and utilize concrete data, such as the number of incident reports, lost or stolen devices, and policy breaches. Quantitative methods include, for example, surveys, and are used to test hypotheses. Quantitative methods will provide statistical data that should validate employees' behavior and provide insight into what security risks the organization should focus on mitigating. By monitoring statistics regularly, organizations can also detect possible trends or increases/decreases in behavior.

Finally, based on the reviewed literature and research, surveys are the most recommended and preferred tools to measure security culture. Chaudhary et al (2022) suggest that measuring knowledge, attitudes, and behaviors is best done by conducting surveys. Surveys are an excellent method to study employee behavior, attitudes, and opinions on information security. They are easy and cost-efficient to distribute, and user-friendly as they offer predefined questions and a set of answers to choose from. Analyzing and documenting interview results can be time-consuming, whereas survey results are easy to gather and analyze, and the data can be used to identify correlations.

2.4.4 Surveys and Questionnaires

Veiga and Eloff (2010) created the Information Security Culture Framework (ISCF) to help organizations implement activities that encourage employees to protect the organization's information assets. The framework can be used as a strategic plan for creating a successful information security culture, but it was also designed to be used to assess security culture. The notion of the framework is that by focusing on information security components, an organization can influence employees' security behavior and thereby cultivate their security culture.

According to SANS Institute (2021), surveys are a preferred method of measuring security culture. Surveys provide insight into employees' attitudes, beliefs, perceptions, and norms, and are therefore one of the most used tools to measure culture. To get the most out of surveys, organizations should ensure they carefully consider the questions they ask and how the questions are asked.

Orehek and Petrič (2021) highlight that surveys should be multidimensional, meaning that they should measure various aspects. A survey should not be limited to measuring employees' security knowledge or behavior, but should also include their attitudes. As an example, Orehek and Petrič (2021) explain that if survey results show that employee's attitude towards security is becoming more negative, yet their knowledge level remains the same, this should imply that the organization's security culture program should focus on improving attitudes towards security, not increasing employee's knowledge level. The challenge, however, lies in the fact that surveys that are designed to measure various aspects can become lengthy. This can result in less willingness from employees to take the time to answer such surveys and increase the cost of conducting surveys.

When conducting a survey, it is highly important to consider the sample size. First and foremost, it should be statistically large enough to provide valid results. In addition, the results should capture the true view of the entire organization. Orehek & Petrič (2021) suggest that the optimal way would be to survey the entire organization, however,

understandably, this might not be approved or manageable. By ensuring that the results capture the full organizational picture, and the sample size is sufficient for also subunits, the results may provide important indications of sub-cultures that could pose heightened risks to the organization. (Orehek & Petrič 2021.)

When creating questions, it is important to first decide what one wants to know and what behaviors one is interested in, thereafter, the questions should be designed in a way that provides answers to address those needs. Surveys should not be too long, hence, questions must be prioritized and limited to what is truly needed. In addition, questions need to be written in a way that ensures they do not influence the answers. For example, it is recommended to avoid asking security questions that can make the respondent answer them in a certain way to avoid getting in trouble. Instead of asking “have you ever shared your password”, questions should be asked in a non-biased way “how likely is it a coworker has shared their password”. (SANS Institute 2021.)

In terms of answer options and scales, SANS Institute (2021) recommends using the Likert Scale, which was developed by an American social scientist Rensis Likert. The Likert Scale is seen as one of the most reliable ways to measure opinions, perceptions, and behaviors. It does not include yes, no, or open-ended questions, but provides a range of responses. Likert is a psychometric scale that allows respondents more freedom in their answers as it provides multiple options from expressing agreement and disagreement to neutrality. These scales are often used in psychology and sociology as answers are easy to quantify once data has been collected. (SANS Institute 2021.)

The Likert Scale uses a set of predefined options, which can be numeric or verbal, and are always used to answer closed-ended questions. The most commonly used number of alternative answers ranges from four to seven. For example, a question can be designed to understand how important something is to respondents. The first alternative would be “very unimportant” and the last alternative “very important”. Additional options in between would be, for example, unimportant, somewhat unimportant, somewhat important, and important. (SANS Institute 2021.)

2.4.5 Statistical Data and Analysis

According to Freund and Jones (2014), the only role of metrics is to inform decisions, thus meaning that metrics that are not being used for decision-making provide no added value and are therefore considered unnecessary. Freund & Jones recommend using the Goal, Question, Metric (GQM) method in developing metrics. Decision-making is derived from goals, which the organization is trying to achieve. Therefore, each metric should be created by first considering what the goal is for the organization, what question the metric

is answering, and then defining the actual measurement. For example, goal: Reduce the number of employees incorrectly classifying information, question: How much information is classified incorrectly?, metric: Volume of incorrectly classified information.

Metrics are also an important tool in making comparisons, for example, comparing the current station with the desired situation. They can also be used to prioritize activities, create mitigating actions, and evaluate the effectiveness of past decision-making and the actions that were taken. Regardless of what they are used for, it is good to evaluate the metrics regularly and consider whether the data is correct and serves its purpose. (Freund & Jones 2014.)

ENISA (2021) recommends using quantitative methods to measure security culture but highlights a few challenges with using security-related statistical data, such as it is often difficult to interpret. For example, the number of tickets related to security rose towards IT. An increase in tickets raised can be seen as employees not acting according to company rules, which refers to poorer employee behavior, or vice versa; increased security awareness among employees and thus users detecting and reporting more incidents. Another metric that is often used is the number of employees trained or completing specific training. This, however, does not mean that employees have learned or changed their behavior, especially if the training can be completed online and simply clicked through without absorbing knowledge.

SANS Institute (2021) also recommends using metrics but suggests keeping them simple. This means only focusing on metrics that provide value to an organization. When measuring culture, both quantitative and qualitative methods should be used to provide a clear and comprehensive overview. SANS Institute also highlights that because measuring security culture involves measuring humans, multiple ways to capture impact need to be used. Ultimately, the key is using the measurement options that work best for each organization, since one method does not work for all.

ISF (2020) provides example statistics that can be used, such as:

- Percentage of completed training
- Training exam pass/fail rate
- Training evaluation scores
- Number of employees that bypass security controls
- Average time to perform good behavior (e.g. reporting phishing)
- Number of security champions
- Number of employee interactions with security champions
- Number of employees using security controls (e.g. wearing ID badges, lockable storage)
- Number of incidents reported
- Number of employees that ignore password rules

Freund & Jones (2014) suggest the following examples:

- Percentage of personnel who have had generic security awareness training
- Percentage of personnel in specific roles who have received awareness training pertaining to their specific responsibilities
- Number of personnel who were rewarded or commended for their security decisions and actions
- Number of personnel who were reprimanded or fired for their security decisions or actions

SANS Institute (2021) recommends considering which behaviors are important to an organization and then creating the applicable measurement methods to measure them. In general, SANS Institute suggests measuring what employees think and what they know, but also what they do, for example, measuring:

- Number of security bugs in code
- Percentage of people failing phishing simulations
- Number of lost devices
- Number of data access violations

One of the most often used and debated metrics in security awareness are the results of phishing simulations. There are two metrics organizations tend to focus on: how many employees clicked a link (click rate) and how many reported the email as phishing. There is much debate about what constitutes a good result from a phishing simulation, and whether this is the click rate. This, however, depends on the simulation: how difficult it was, was it highly targeted or generic? The challenge is in comparing simulations and their results with each other.

An option is to classify the simulations in terms of difficulty and try to compare the same-level simulations against each other. As the time of day and day of the week can affect the results it would be optimal to ensure the emails are sent out on the same day of the week and at the same time to ensure the best comparability. In addition, organizations can look at creating tier groups, such as sending specific simulations to specific employees based on their roles or how long they have been in the company. Whichever statistic an organization chooses, it is important to understand that when evaluating culture, the value a metric provides is not from a single moment, but the trend that can be seen over time. (SANS Institute 2021.)

2.4.6 Measurement Examples

Based on research and academic principles, Carpenter & Roer (2022) claim that the best way to measure security culture is by sending a survey to all employees. The Security Culture Survey is a survey created by Roer for a security company called KnowBe4, which offers services, such as measuring an organization's security culture and benchmarking results against other organizations. The survey includes 31 questions and measures security culture across the seven dimensions of the Security Culture Framework (Roer 2015, chapter 7). Each of the seven dimensions has three to six questions. The survey questions are unfortunately not publicly accessible; however, Roer has published an outline of each dimension and suggestions around questions. This list can be found in Appendix 3.

Da Veiga & Eloff (2010) created what they refer to as an Information Security Culture Framework, which was designed to assess whether an organization's security culture improves the protection and security of its information assets. The survey is divided into seven categories: leadership and governance, security management and operations, security policies, security program management, user security management, technology protection and operations, and change. The survey includes questions (statements) for all seven dimensions, resulting in a total of 85 statements and using a five-point Likert scale (Strongly disagree to strongly agree). Questions include, for example:

- Q1. I believe it is necessary to protect information to achieve the business strategy of [company]
- Q2. I believe [company] pays adequate attention to an information security strategy to protect information
- Q3. Information security controls are adequately deployed in [company) to protect information (Da Veida & Eloff 2010)

According to Sas, Hardyns, van Nunen, Reniers and Ponnet (2021), a unified and validated tool that can be applied across sectors and organizations does not exist, nor does an underlying agreement on the components or constructs that comprise a security culture. Thus, it is not surprising that a limited amount of research has been conducted on the topic, and only a few have resulted in actual measuring tools. Sas et al (2021) reviewed 16 tools that were created to measure security culture and analyzed six of them in detail. The research concluded that a standardized tool to measure security culture should be created.

Of the six tools analyzed by Sas et al (2021), only four focused on measuring information security culture. The two remaining ones measured physical security culture. Four of the

models measured security culture and provided improvement suggestions, while two focused solely on measuring culture. All six tools used questionnaires for measurement, in addition, two of the tools also used interviews, document analysis, and observations as additional measurement methods. This was seen as a strength, especially combining qualitative methods to gather a more comprehensive picture and views. All six methods measured employee behavior, and half also technological aspects. A complete comparison of the six tools can be found in Appendix 4.

Schlienger & Teufel (2003) created a questionnaire that was designed to measure the security perceptions and attitudes of employees. Each question is designed to have three parts that measure a) individual attitudes, b) perceptions of the company's attitudes, and c) the best solution. The questionnaire includes a total of 10 questions, and five questions on demographics and the questionnaire itself. In addition to sending out the questionnaire to employees, Schlienger & Teufel conducted unstructured interviews with security employees. The questionnaire was created and tested on a global company. The answer options in the questionnaire were based on a three-point Likert scale (True, False and I don't know), and example questions included:

- Q1. The computer and electronic communications systems should be used for Orange's [company] business activities only
    a) Personally I think this is
    b) Orange [company] regards this as
    c) If I were responsible, I would regard this as
- Q2. Every employee should be trained in the information security controls he/she is supposed to use in his/her work.
    a) Personally I think this is
    b) Orange [company] regards this as
    c) If I were responsible, I would regard this as

Martins and Eloff (2002) developed a questionnaire to measure information security culture on three different levels: individual, group, and organizational. Their questionnaire includes 45 statements that address nine specific areas: policies and procedures, risk analysis, benchmarking, budget, management, trust, awareness, ethical conduct, and change. The answer options were based on a five-point Likert scale (strongly disagree – strongly agree and the questionnaire was designed and conducted on an IT consultancy company. Example questions include for example:

- Q1. I know what the term information security implies.
- Q2. I think it is important to implement information security in the organization.

Alnatheer et al (2012) have created a questionnaire with 19 statements that are divided into the following categories: Top management involvement in information security, information security policy enforcement, information security training, information security awareness, and information security ownership. The answer options were on a five-point Likert scale (strongly disagree – strongly agree). The study was conducted in Saudi Arabia on multiple companies. Example questions include:

- Q1. Senior management gives strong and consistent support to the security program
- Q2. Information security policy is communicated well

AlHogail & Mirza (2015) propose using the information security culture framework created by AlHogail (2015), which uses a questionnaire to assess information security culture. The questionnaire assesses employees' knowledge, behavior, perceptions, and beliefs, and is divided into five topics: strategy, technology, organization, people, and environment. Depending on the question, the answer options are either on a two- or five-point Likert scale. The study was conducted at three organizations in Saudi Arabia. The questionnaire includes questions, such as:

- Q1. I have received training on using information security hardware and software
- Q2. Information security strategy element clearly state what is expected from me

In their research, Sas et al (2021) conclude that organizations should use a multi-method approach to measure security culture by using both a questionnaire and conducting interviews. They also recommend that employees across an organization and from all levels should be included in the surveys and interviews to get a comprehensive view of opinions. The questions used should address both internal and external threats and focus on the most experienced threats. Ultimately, the results of the survey should highlight the strengths and weaknesses of an organization’s security culture, thereby indicating recommendations on future focus areas, and finally, the measurements should be carried out regularly.

2.4.7 Critical Review of Previous Research

Hayden’s (2015) Competing Security Cultures Framework was created based on the Competing Values Framework by Quinn & Rohrnaugh (1983), with the difference that it is specially adapted to the security area. Quinn & Rohrnaugh’s model was created to measure organizational culture and, in particular, the opposing priorities and values that

affect employees' decisions and actions. According to Hayden, his model allows an organization to understand how security is seen and practiced by its employees, and identifies competitive principles and values that can pose risk to the organization's security goals and objectives. The main idea was to measure and analyze specific traits that either increased or hindered information security performance.

The challenge with Hayden's model is how it portrays the relationship between tight and loose control. This axis represents the level of control an organization has over its security and suggests that organizations with a trust or autonomy culture have loose control over their security. This indicates that organizations that value communication, participation, and commitment, and where employees are empowered, have loose control of their security. In addition, this applies to organizations with autonomy culture where flexibility, innovation, and performance are valued. One could argue that in organizations that have open communication, employees are included and empowered have strong cultures due to a common sense of belonging and coexistence. This togetherness would most likely portray the contrary and a common will to do the right thing and act securely. According to Hayden, control also refers to the extent to which organizations restrict employees' behavior. Research, however, shows that while rules and laws are implemented, it does not necessarily mean that people will obey. In an organization that promotes security openly and by explaining the reasoning is much more successful than when rules and policies are dictated.

In addition, the value that the Competing Values Framework provides can be argued. The model is very limited as it describes only four main types of security cultures, and at a very high level. Based on the survey they have designed, they can place an organization on the axis, but this does not provide enough information on an organization's security culture, nor does it measure it sufficiently. For an organization that wants to understand its security culture, this model simply does not provide enough value-adding information to take concrete actions or to draw conclusions about employees' true behaviors.

The seven dimensions of security culture, created by Carpenter and Roer (2022), are extensive and capture employees' behaviors from multiple perspectives. Roer's Security Culture Framework (2015) focuses on the human aspect of security and runs in a continuous cycle, in which a full circle should demonstrate change and the improvements to security culture. The model is simple, yet includes relevant steps, and focuses on continuously improving the culture over a longer period. The framework is adaptable, however, both models by Carpenter & Roer and Roer do not provide any measurements or metrics. Therefore, they can be difficult to utilize or expensive to acquire.

Orehek & Petrič (2021) claim that security culture should be measured with employee surveys and validated with evidence, such as data. The answers employees provide should correlate with available data. ISF (2024) suggests the same, however, they also suggest tracking how much training is provided or how often awareness activities are held. The challenge is that it does not matter how many training sessions employees need to take, if they do not commit to changing their behavior. Hence, while an organization can host numerous security-related training courses a year, it does not mean that employees have paid attention or learned anything of value. Thus, the number of activities or trainings courses attended should not be used to measure security culture.

According to Carpenter & Roer (2022), security culture should be measured from a group perspective, not from an individual viewpoint. While it is understandable to assume that employees' observations can be seen as a good measurement, the challenge is that situations vary and interpretations can affect the results.

The Information Security Culture Framework (ISCF), created by Veiga and Eloff (2010), focuses on measuring information security culture. The questionnaire includes 45 questions and is answered on a five-point Likert scale. The questions seem difficult for employees to answer, as they are vague or require a high degree of understanding of the organization's strategy and governance model, which most regular employees would not have. Questions include, such as: The information security controls implemented by ABC support the business strategy, or I understand how information security is managed in ABC to protect information.

Numerous sources, such as Freund & Jones (2014), SANS Institute (2021), ENISA (2021), and ISF (2020), recommend using metrics to measure security culture. ENISA highlights the challenges with metrics, such as the difficulty interpreting them and their reliability. Many of the suggested metrics can be questioned, for example, the percentage of completed training and phishing simulations. As mentioned before, employees can complete security training without changing their behavior. In addition, there is much controversy around using phishing simulations are metrics. Should they be used, they at least need to be used in a way that enables the results to be comparable over time.

Of the measurement tools analyzed by Sas et al (2021), the questionnaire created by Schlienger & Teufel (2003) includes ten questions that measure the persons' individual opinion, their perception of the company's attitude, and their opinion if they were in charge. Since the questions were created in 2003, they use terms that are no longer used, but the length and way the questions have been created seem to add value, and therefore this questionnaire could be used as a basis to create a similar survey.

Martins & Eloff's (2002) questionnaire is more extensive than Schlienger & Teufel's (2003), however, it focuses on areas of less importance when measuring security culture, such as budget. Questions, such as: I know what the term information security implies, and I think it is important to implement information security in the organization, focus either on knowledge or opinion, not behavior. The questionnaires created by Alnatheer et al (2012) and AlHogail & Mirza (2015) have good elements, but they too fall short with questions that are difficult for regular employees to answer.

2.5 Summary

This chapter has included a literature review of key research, definitions, models, and frameworks around information and cybersecurity, security awareness, culture, and security culture. The following summarizes the most important areas.

The past few decades have seen a surge in the development and implementation of digital solutions. While this has enabled industries around the world to advance and take big leaps in productivity, it has also opened the door to new risks. As the world becomes more digitally connected, new emerging risks arise that are increasingly being exploited by cybercriminals. New technology, such as artificial intelligence, brings unimaginable opportunities, but also unprecedented risks that cybercriminals are all too eager to exploit. Artificial intelligence is not used only for good, as it has become a significant tool for criminals, enabling them to develop more advanced attacks and exploit vulnerabilities, and at a high cost for organizations, when the average cost of a data breach is 4.88 million US dollars. It is therefore no wonder that information and cybersecurity have become a top risk for organizations around the world. (World Economic Forum 2025; Rizal & Setiawan 2023.)

Information security is the act of protecting information in all formats, whereas cybersecurity is the digital protection of data, systems, and assets. Access to information and digital systems, and assets is highly desired by cybercriminals because it is their bread and butter. Cybercriminals try to steal information that they can use and sell and turn it into cash. In its simplicity, cybercrime is pure business, and information is the commodity. Organizations are trying their best to defend against these attacks by adapting the latest protective technology. This has forced cybercriminals to find new ways of penetrating organizations, particularly by utilizing employees to gain access. This can be done in multiple ways, for example, social engineering. (Death 2023, chapter 1.)

In 2024, cybercrime increased both in frequency and sophistication. 72% of organizations reported an increase in cyber risks, and 42% reported an increase in phishing and social engineering attacks. These attacks are specifically targeting employees and relying on

them to make mistakes, opening the door for attackers to gain access to systems and data. This is why it is increasingly critical to ensure that an organization has a collective mindset to defend against threats where employees are knowledgeable and willing to take action. To achieve this, organizations need to ensure they foster a sound security culture, where employees are motivated to think and behave securely. (World Economic Forum 2025.)

People are often referred to as the weakest link in security, which can be argued to be true, as statistically, most security incidents have a human component. It is, however, important to understand that while employees can make mistakes, they can also be used as an extra layer of defense when they know how to behave. Implementing an organization-wide security awareness program trains employees to understand and identify relevant security threats and risks, and equips them with the knowledge to prevent attacks and breaches (Hayden 2015, chapter 5; Gardner & Thomas 2014, chapter 1.)

Organizations that have a security awareness program are often compliance-driven, as many industries have a regulatory requirement to run annual security training. But compliance does not equal a secure organization, it can result in considerable gaps and a lack of behavior change among employees. Organizations can also choose to focus on a program that focuses on information sharing, but knowing about security instructions does not necessarily mean an employee changes their behavior. Focusing on behavior change alone can influence how employees act but concentrating on an awareness program dedicated to security culture shaping goes beyond the actions employees take and works to change an organization’s culture: its values, beliefs, and attitudes toward security. (Carpenter 2019, chapter 2.)

Organizations with the most mature security awareness programs focus on not just building a solid security culture but also applying strategic metrics to measure change. Successful security awareness programs inspire employees to demonstrate specific beliefs and behaviors, which are derived from a desire to change and do something meaningful. Measuring the effectiveness of a security awareness program often focuses on the same as measuring security culture: employees' behaviors, attitudes, and knowledge. (SANS Institute 2024; Carpenter 2019, chapter 2; Chaudhary et al 2022.)

An organization's culture is learned by interacting with others and through sharing ideas, values, and behavior. As an organization grows, these beliefs, values, and behavioral norms become basic assumptions and will translate into unconscious actions. All organizations have their own culture, which develops with time and becomes a way to function that is commonly understood and acted upon. Culture has a key role in an

organization, and based on research, organizations with a common culture perform better and even outperform others. (Ferraro & Briody 2023, chapter 1; Schein & Schein 2016, chapter 2; Denison et al 2012, chapter 2.)

Studies confirm that employees bypass organizations' security processes and policies, which is a clear sign that employees are willing to expose their organizations to vulnerabilities and potential attacks. While this is done intentionally, for example, to complete a task in less time, employees are most likely simply not aware of the danger they are inflicting or the potential repercussions. This is a result of employees not understanding what they should do, and more so, why they should do so. Ensuring an organization has a strong security culture will result in a reduction of human vulnerabilities as employees are motivated to think and act differently. (Fujitsu 2020.)

Various frameworks and methods that define security culture have been created, and they enable organizations to conclude on their cultural characteristics. In addition, Carpenter and Roer (2022) define seven dimensions of security culture that have been created to help organizations understand security culture and how to influence and develop it. To understand one's culture, an organization should measure the existing culture. Next, they should define concrete goals for the future culture and measure them regularly. Metrics to measure security culture should be repeatable and relevant for the next five to ten years. In this way, the results can be compared throughout the years, which should show a change in the culture.

By measuring security culture, an organization can learn about employee behavior, their opinions towards security, and their level of knowledge. Research can be done by utilizing both quantitative and qualitative methods, and using both enables organizations to measure the link between culture and action. Quantitative data provides concrete data by numbers, whereas qualitative data provides insights into what has happened or tends to happen. A common measurement method used by all does not exist, hence, it is recommended to use various methods, such as surveys, interviews, and data. As all organizations are different, it is recommended to adjust metrics based on the organization in question. The main measurement method recommended in literature and academic research is an employee survey. (Hayden 2015, chapter 5; ISF 2024.)

3 Methodology

The previous chapter provided an overview of previous research, definitions, models, and frameworks related to this thesis. In this chapter, the focus will be on how this research was designed, how data were collected and analyzed, and how reliability and validity were considered.

3.1 Research Design

The purpose of this research was to investigate how an organization-specific framework to measure security culture could be designed and validated for Organization X. This required both understanding the organization in question, their needs and desires for this research, as well as studying relevant academic and business literature on the topic and interviewing experts that could provide additional input and recommendations.

This thesis was conducted as action research. The approach was selected to research a topic in-depth while creating a solution to change it. The study subject was seen as a challenge at Organization X, and a solution was needed to address it.

During this research, the researcher took an active part in overseeing as well as participating in group work and interviews. By managing the project and actively participating, the researcher gained extensive knowledge of the research topic and how the research question could be solved. By taking an active role, the researcher was able to suggest improvements and assess and adjust the changes throughout the research cycles.

In this research, the researcher took part in each stage and ensured timely progress. A significant amount of time was allocated to gathering information and reviewing related literature to understand the available options. In addition, numerous iterations were conducted along the way, which included multiple workshops and brainstorming sessions.

Action research is a method used to create a deeper understanding of a situation or the practical consequences to improve a situation. According to Seale, Gobo, Gubrium and Silverman (2004, 478-489), the process of action research is highly important and involves working with people as a part of the research. Action research includes both gaining understanding of theories, but also knowledge from encounters with other people and by doing things in practice. This also includes co-operative inquiry, in which research is done collectively within a group that generate ideas and draws conclusions from experience. Research is done in collaboration with people, not on people.

Action research was chosen as the approach for this thesis to conduct in-depth research on the topic of measuring security culture and to simultaneously create new ways of measuring security culture at Organization X. This was done by working alongside a team of security awareness experts and conducting research during three individual cycles, where measurements and metrics were designed specifically for Organization X.

The work involved qualitative research methods, as the purpose was to acquire information to understand the phenomenon of measuring security culture. Methods used included conducting interviews, workshops, and brainstorming. Interviews are often used to gather information in development work and serve as a good tool to suggest ideas or input. Interviews serve as a tool to create clarity on a certain topic or provide knowledge. Interviews were conducted as open-ended interviews, where high-level questions had been created in advance, but their order and wording were decided upon during the interview. New questions were also created during the interviews, based on the discussions and input provided. The interviews were informal by nature and included discussing a certain theme or challenge, and both parties took part in the discussion. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

Collaborative methods were also used to generate ideas to create measurement tools and metrics to measure security culture at Organization X. Collaborative methods are often used in research, where the intention is to develop new ideas or solutions. This requires ensuring an open and positive atmosphere, where each participant’s input is welcomed. Collaborative methods include creative problem solving, which is a process that includes being aware of a problem or a chance for improvement. It includes generating, evaluating, choosing, and implementing ideas. (Moilanen, Ojasalo & Ritalahti 2022, chapter 4.)

In this research, creative problem solving was conducted during workshops and brainstorming sessions, where the main questions revolved around “how” measurements and metrics could be created. Three longer workshops and ad hoc brainstorming sessions were held to address questions and to come up with or test ideas to move forward with the research.

Research was divided into three parts, which included conducting a current state analysis, reviewing existing, models and action research.

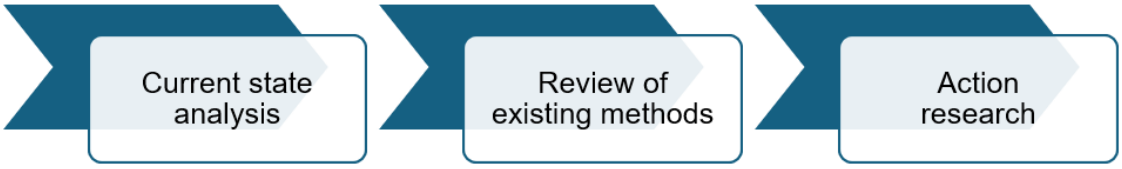

Figure 12. Overview of the empirical part of this research.

3.2 Population and Sample

During the research, four main interviews were conducted. This included three employees from the commissioning organization and one external expert.

The first interview was with a senior manager at Organization X, who was previously responsible for security awareness activities. In addition to previous experience in security awareness, he has also worked in the information security area for more than 20 years and thus has extensive experience in the area. He was also the responsible contact person at Organization X for this thesis.

The senior manager's interview was conducted during the first action research cycle and as part of the planning phase. He provided his views and ideas on what the commissioning organization was interested in gaining from this research and helped define the scope and research questions for this thesis.

The second interview was also held during the first cycle of action research with a world industry leading security awareness expert who teaches courses on security culture and security awareness. He was chosen due to his vast experience in the area and due to his continuous work and research with organizations around the world. He provided knowledge and examples on measurement options and input based on previous experience with other organizations.

The third interview was held after the project team had created the first draft of the security culture survey for Organization X. This was shared with a colleague who was simultaneously working on a survey to measure the risk culture of the commissioning organization. The draft created by the project team was shared with the colleague, who also shared his survey, and the methods and questions were discussed.

During the three action research cycles, multiple meetings were held with key stakeholders, and a final meeting was held with the Chief Security Officer, who had the chance to ask questions and provide input to the final measurement tools and metrics, which he approved in the meeting.

3.3 Data Collection

A mix of methods and methodologies can be used to conduct research, for example, gathering quantitative and/or qualitative data. Quantitative research is objective and empirical and seeks to answer “what” and “do/does”, whereas qualitative research is subjective and inductive. Qualitative research seeks to understand, examine, and discover, and to answer “why”, “how”, and “what”. (Ayton et al 2023.)

Qualitative research is often used when a researcher knows little about the phenomenon or concept that is being investigated or when they are unable to clearly define the scope. To qualify means to assign a quality or to describe something. Thus, qualitative research is used to understand a phenomenon from the viewpoints of the people experiencing it. Qualitative research uses methods such as interviews, focus groups, and observations, which seek to gain insight into how people perceive situations, which are often reflected by their motivations and feelings. (Ayton et al 2023.)

This research used the following qualitative methods: Interviews, workshops, and brainstorming sessions. Interviews were conducted with experts, colleagues, and stakeholders throughout the research, who provided important expertise, knowledge, and support. The other methods used were conducting work in multiple workshops and during brainstorming sessions.

To create an organization-specific framework for measuring security culture, an extensive literature review was conducted to understand what measurements had been studied and created. This included analyzing academic research and literature to understand what frameworks already existed and whether they could be applied to Organization X. In addition to the literature review, interviews were conducted with employees from Organization X, peers, and industry experts, including experts in Security Awareness and measuring culture.

3.4 Data Analysis

The recommended way of analyzing qualitative data is to do it along with data collection. This ensures that the researcher is aware of the amount of data collected and the content, which should help limit the number of people who are interviewed, as topics and information gathered become repetitive. (Merriam and Tisdell 2016.)

Data analysis refers to the process of understanding and interpreting data. This can be done in multiple ways, such as coding, in which the researcher analyses a transcript and highlights the information that is relevant to answering the research question. Once data

has been assigned a code, it can be categorized by grouping the comments and notes that correspond. (Merriam & Tisdell 2016.)

The interviews and discussions during workshops and brainstorming sessions during this research were accounts of employees' experiences, opinions, and ideas. These were all documented in transcripts and notes, which were organized to ensure data could be easily retrieved. As this research was conducted for a specific organization, the data was treated as a case study, where all information is gathered in one resource package. The data was organized in chronological order and based on the three action research cycles. The data gathered and the steps taken during the research are presented and described in Chapter 4.

3.5 Reliability and Validity

One of the most important actions for a researcher is to ensure a study is reliable and valid. This includes ensuring that the measurements assess what it is designed to measure and thereby confirm that the method will provide reliable and valid results throughout time. Validity refers to whether a data collection method measures precisely what it is designed to measure, and reliability refers to whether a data collection method and analysis can produce consistent findings. (Saunders 2017.)

In this research, it was important to first carefully review academic and business literature to understand the topic and only then move to measure the research topic. Metsämuuronen (2005) highlights the importance of ensuring the conducted literature review is done using reliable sources, which are, for example, academic journals and their references. Academic journals are peer reviewed and go through a rigorous analysis before being approved, which ensures a higher level of validity and reliability. Academic and business literature includes basic theories that can be applied and used in research, but in particular, business literature should be reviewed critically.

To ensure the quality of this thesis, a comprehensive examination of available literature was done, and sources were chosen based on their quality. However, the availability of reliable literature on the topic was a concern since finding academic books and articles on measuring security culture was somewhat challenging. To ensure the use of reliable resources the following actions were taken: the list of references was reviewed and checked, the number of times articles had been cited was reviewed, and the qualifications of the authors were analyzed. When reviewing existing academic articles, the reliability and validity of the research were outlined and checked, and the articles often used and referred to the same references, which helped with the analysis.

The terms “reliability” and “validity” were originally used in traditional quantitative research. Therefore, according to Costello (2003), it has been debated whether they are applicable in the context of qualitative and action research. For qualitative research to be valid, it must be accurate, correct, or true, which can be challenging to verify with certainty. Therefore, Costello suggests focusing on the credibility and trustworthiness of the research. A solution is, for example, an audit trail that provides evidence of the researcher being careful and systematic, using multiple sources to collect data, and continuously testing assumptions. (Costello 2003.)

This thesis used interviews, workshops, and brainstorming sessions to collect data. Utilizing three action research cycles ensured that data could be collected multiple times, for example, conducting interviews and workshops during all three cycles.

Since the topic of the research was to find a way to measure security culture at Organization X, the research was closely executed with the help of people working at Organization X. This included interviews with carefully chosen employees that could provide suggestions, ideas and input to the work, while understanding the organization and its nature. In this research, it was important that the organization, its structure, and ways of working was understood by the interviewees. In addition, an interview was conducted with one of the leading experts in security culture to validate the findings from the literature review and provide additional suggestions.

To ensure the data was captured correctly, detailed notes were taken during each interview as well as during the workshops and brainstorming sessions. This ensured that the data was documented and could be referred to at a later stage.

Costello (2003) also highlights that action research is predominantly qualitative and thus sensitive to the researcher’s bias. This is often the case due to the researcher engaging in the study. Costello therefore suggests that results should not be generalized, validity should be addressed by questioning whether the findings are truly about what they appear to be and whether they measure or describe what they are designed for, and reliability whether a another study would yield the same results.

The threat of researcher bias was acknowledged and considered throughout the research, and objectivity was a priority. The challenge with qualitative data is that it is difficult to replicate. In this research, data was collected in interviews, workshops, and brainstorming sessions, which by nature contain variables that cannot be replicated as they are unique events and based on personal knowledge, views, or opinions. For this reason, interviews and workshops were carefully planned, and interviews, workshops, and brainstorming sessions were documented and archived.

Because this research was organization-specific, the data collection methods used could be utilized by another company, but the results would not be due to the specificity of the study subject.

4 Results

The previous chapter explained the methodology used to conduct this research, what data was collected, how it was collected, and analyzed. This chapter will focus on explaining the results of the research by explaining how the research was conducted and how action research was applied as the research method. In this chapter, the theory of action research is first introduced, and the research results are outlined and explained through the applied action research process and its three cycles.

4.1 Action research

Action research is a form where research is done most often on the researcher themself or, for example, a group or organization, and concerning their own work or the context or situation they are in. Action research is self-reflective and used to improve and understand practices and the circumstances these practices are carried out. It can also be described as gathering information to create change. (Carr & Kemmis 1986, 162.)

The different stages in qualitative research are planning, data collection, and analysis. Action research, however, includes an additional action stage, where an analysis of the results will be provided or a solution to the research question will be offered. (Kananen 2011, 149.)

Action research aims at increasing understanding of a study subject, for example, a particular problem or phenomenon, and to create change. Thus, action research aims to understand context and to improve it through either change or action. Action research is practical, focused on solving problems and finding solutions to change them, and often undergoes stages. These stages seek to understand the problem, plan a solution, implement a solution, and reflect and evaluate the solution. These stages are carried out cyclically and iteratively. (McNiff 2013.)

“Action” refers to what the researcher does, while “research” how the researcher learns about what they do. Action research is used to analyze what is being done and requires self-observation, critical analysis, and reflection. It is most often researcher-driven, where a problem or problems are identified with the aim of understanding and improving them, and the researcher takes an active part and frequently participates in the activities they are studying. (McNiff 2013.)

Action research includes various steps that are performed in sequence. Once all steps have been performed, the cycle is begun again and the work is adjusted based on learnings from the previous cycle. An action research project has multiple cycles, each

dependent upon the results and reflections of the previous cycle. Literature describes various variations of these steps. (McNiff 2013.)

According to Mertler (2013), action research begins by identifying a problem, after which it continues to follow a cycle that includes four steps: plan, act, observe, and reflect. As in many cases, proper planning is key to success. This also applies to action research, where once the research topic has been defined, the next step is to develop an action plan. This plan should guide the research process by identifying and limiting the topic, gathering information, reviewing related literature, and developing a research plan. These activities are done before beginning to implement the project. Stage two (act) includes implementing the plan and collecting data, as well as analyzing the data. In stage three (observe), the researcher can revise, change, or make improvements as well as develop future actions, also known as an action plan. In the final stage of the process (reflect), the results of the research are summarized, and a plan for sharing the results is created. In addition, the researcher reflects on the research process.

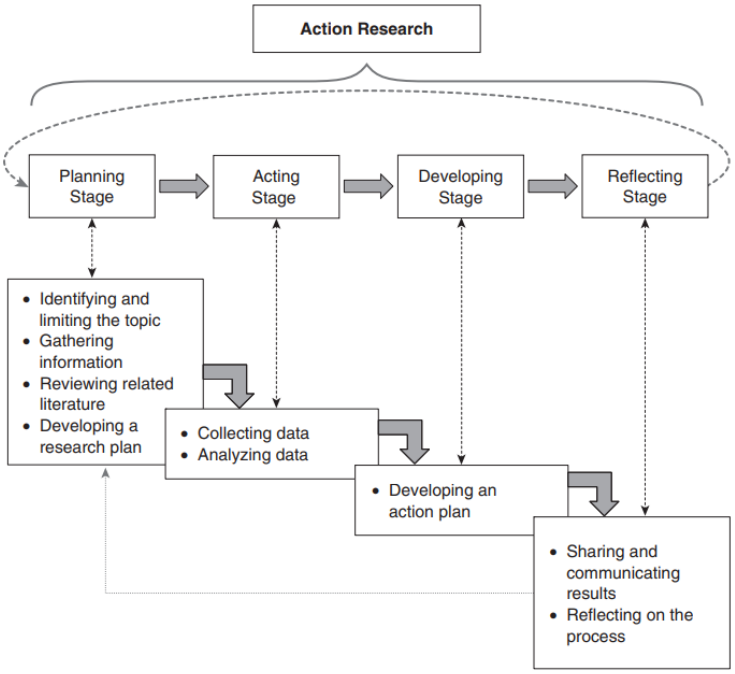

Figure 13. The step-by-step process of action research (Mertler 2013)

According to Willis and Edwards (2014, 12-13), action research includes seven iterative steps, which form a circle. An action research circle can have multiple cycles, each running independently and drawing from the learnings from the previous cycle. In the first of the seven steps (identify a general or initial idea), an idea or plan is created. In the second step (reconnaissance), the idea or plan is studied, followed by the third step (plan and implement), where an action plan is created and implemented. In the fourth step

(evaluate), the results of the action plan are assessed, which leads to the fifth step (revise action plan), where the action plan is revised based on results. In the final step (begin recursive action research cycle again), a new cycle is begun based on lessons learned.

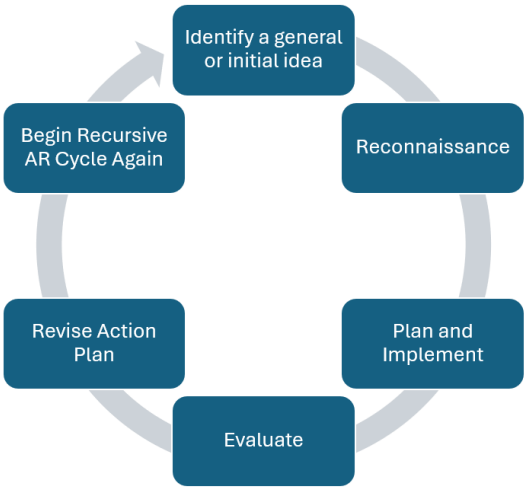

Figure 14. Action research model (adapted from Willis & Edwards 2014, 13)

Moilanen, Ojasalo & Ritalahti (2022, chapter 3.) present a similar, but more simplified overview of the various stages in action research: plan, act, observe, and evaluate. These four steps are carried out as a cycle that is repeated. Moilanen et al explain that the goal of the research is first defined, and the objectives are thereafter set accordingly. This is followed by a literature review to investigate whether the topic to be researched has previously occurred or been studied. Once the researcher has familiarized themselves with the topic, a project plan that outlines the target for development and its goals is created. The concrete work begins by studying and experimenting with ways to reach the research goals. Once this has been done, the results are analyzed, and the plan is adjusted (goals, schedule, and experiments). The action research project continues by using each step (plan, act, observe, and act) in cycles.

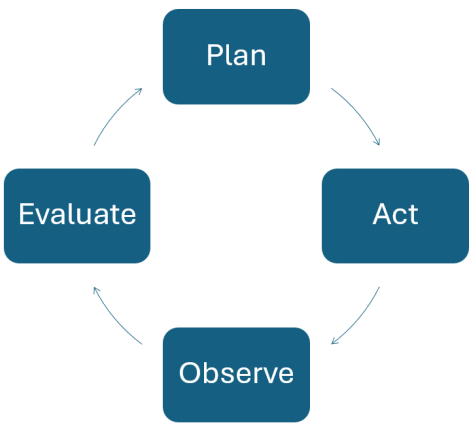

Figure 15. The four stages of action research (adapted from Moilanen et al 2022, chapter 3)

As action research is not a linear process, but cyclical by nature, multiple rounds can be done. This means that action research has a clear starting point, but it does not have a specifically identified ending point. This is due to the nature of creating change. (Mertler 2013.)

In this thesis, action research was conducted based on the model created by Moilanen et al (2022) and by utilizing the model's four stages (plan, act, observe, and evaluate). The research had a total of three cycles, during which each one included the four stages.

4.2 Current State Analysis

Organizations with a security awareness program should continuously evaluate their program's effectiveness with defined metrics. These metrics should provide senior management with insight into how security impacts the organization's business and what actions should be taken to further enhance it. A key component of the security awareness program is the organization's security culture: the beliefs, attitudes, and behaviors of all employees, as this is the backbone of how employees behave and adhere to security policies and procedures. (SANS Institute 2021.)

Organization X has a well-established security awareness program, which includes various training programs addressing different target audiences, a multitude of awareness activities, and regular phishing simulations. The activities are developed and executed by a dedicated Security Awareness team with defined goals: to create awareness about security instructions and procedures, to reduce human risk by changing employee behavior, and to achieve regulatory compliance.

In 2023, the Security Awareness team evaluated themselves against the SANS Institute Security Awareness Maturity Model and, based on measurements outlined in the model, concluded that they were moving from the second to last phase (Long-term Sustainment and Culture Change) to the last phase (Metrics Framework). Based on data and feedback from employees and senior management, the team had already succeeded in changing employee behavior for the better, however, they wanted to measure the organization's security culture and to quantify how good the culture was (or potentially was not).

Measuring the security culture would allow the team to: 1. set a baseline for the existing culture, 2. evaluate the security culture on an annual and monthly basis, and to see if they had succeeded in changing employees' security-related attitudes and behaviors, and 3. pinpoint possible improvement areas.

The SANS Institute Security Awareness Maturity Model's final stage requires organizations to have a thorough metrics framework that can demonstrate the value it brings to the organization (SANS Institute 2021). To move forward in the SANS Institute Security Awareness Maturity Model, the Security Awareness team at Organization X decided to begin measuring security culture.

4.2.1 Used Metrics

A key part of the security awareness program at Organization X was their training plan, which included multiple annual mandatory courses for existing and new employees. In addition, the organization had implemented short security training sessions that were sent to all employees every three weeks, but completion was set as voluntary. The Security Awareness team used completion rates as a metric for all training. For mandatory training, this measured compliance, and for voluntary training, it provided insight into how important security was seen and prioritized.

In addition to training, the Security Awareness team conducted monthly phishing simulations that targeted the entire organization. The results were a key metric used to evaluate how easily employees could fall for phishing attacks and to measure how well the organization was learning from previous simulations, thereby changing their behavior. The results were shown based on business area, where lower-performing organizations were contacted to take action to correct employee behavior.

Throughout the year, the Security Awareness team ran awareness activities, such as campaigns, events, newsletters, polls, articles, etc. Feedback, as well as the number of attendees and readers, were used as metrics to see to what extent employees had been exposed to security awareness activities and how they rated the activities.

4.2.2 Used Methods

The security culture at Organization X had never been evaluated previously. The Risk organization ran a one-off Risk Culture survey to selected employees, however, it did not focus on specific areas, such as security. The survey was designed to measure risk and control, for example, how well employees utilized and complied with the internal instructions on risk management.

User feedback on provided training and online sessions was gathered by sending out short questionnaires asking to rate the training/session and recommend improvements. All other statistics were gathered directly from systems, such as click rates in simulations, training completion numbers, number of readers for newsletters and articles, and attendees to arranged sessions. In addition, the team was able to access statistics on

reported incidents, such as the number of lost or stolen devices or other acts that constituted breaching internal rules. However, these statistics were only utilized to see if they showed areas that would benefit from raised awareness or training activities.

4.3 Planning for Measuring Security Culture

It was evident for the Security Awareness team that to develop further and achieve their goal of creating sustainable behavior change, they needed to get a clear understanding of the Organization's existing security culture. It was therefore decided that the team would research how security culture could be measured and what metrics should be agreed upon to continuously monitor employee-related security risks (risky behavior).

In December 2023, a project team was established with employees from the Security Awareness team to create a plan on how to measure security culture. This included researching and evaluating existing methods of measuring security culture, measuring employees' perceptions, investigating suitable metrics, and validating the findings.

The work was carried out in multiple cycles, as per the action research model, and carried out together with the project team. Each cycle included creating a new suggested metric model, which was adjusted in the following cycles.

4.3.1 Preparing a Plan

In December 2023, a project plan was created. This included discussing and agreeing on the goals and objectives of the project. The main goal was defined as: To create a framework for measuring security culture at Organization X. The objectives were defined as:

- Creating a way to measure security culture, initially the as-is situation to define the existing security culture, and running the measurement each year to see whether the culture is changing or improving
- Creating a set of defined monthly or quarterly metrics that should portray employees' security behavior and attitudes

The project timeline and working methods, as well as assigned roles and responsibilities, were outlined and included.

4.3.2 Project Plan and Timeline

The project team approved the project plan and suggested a timeline, which would be adjusted based on the number of cycles needed. The initial plan included three cycles. In the planning stage, a current state analysis was conducted, literature reviewed, and benchmarked. In the acting phase, a draft for measurement methods was created. In the

observing phase, feedback was gathered from stakeholders, and in the final reflecting phase, the feedback received was analyzed and the plan revised.

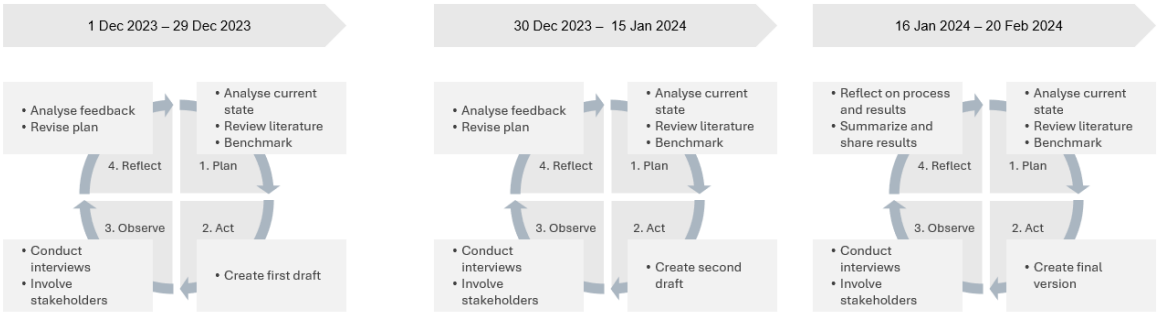

Figure 16. Agreed project timeline and cycles

4.3.3 Benchmarking

A part of the preparation work was to discuss with other security or security awareness professionals what measurements and frameworks they had used or were aware of. This also included looking into available material and literature. The review and discussions indicated that while various methods have been used to measure security culture, a common industry-leading method does not exist, as all organizations are unique.

In addition, measurement methods that had previously been applied at Organization X were reviewed. This included a survey on risk culture and questions related to training. Finally, multiple meetings were held with stakeholders to gather input on what surveys and methods they had previously used and whether there were any dependencies on other teams' or units' plans.

4.4 Creating the First Draft

This section presents how known security culture frameworks were used to create security culture measurements for Organization X. The results utilize theory as well as internal discussions and observations. In December 2023, the team started working on the first draft for measuring security culture. This included reviewing literature and academic research, and multiple brainstorming sessions to create an initial draft.

Based on research, the project team concluded that surveys are a common and proven method to measure culture but require solid planning to ensure the information gathered serves the initial need. In addition, creating additional metrics that supplement the survey would require additional research and analysis.

4.4.1 Plan

The plan phase began with an interview with a senior manager at Organization X, who was also the responsible contact person at Organization X for this thesis. He provided his views and ideas on what the commissioning organization was interested in gaining from this research and helped define the scope and research questions for this thesis.

The research was conducted as an informal interview, and the following questions were asked:

- What does Organization X want to achieve, or find out?
- Have similar activities been tried or done before?
- Are there any preconditions or limitations?

During the interview, the senior manager explained that while the organization looked at incident data, no specific measurements or metrics had been created to specifically measure the organization's employees' attitudes or behaviors in relation to security. For this reason, Organization X wanted to create a method to measure security culture on a monthly and annual basis.

Measurements and metrics had previously been discussed at Organization X, and with peers and other organizations, yet a universal and suitable model had not been identified. The organization's Key Risk Indicators included metrics, such as lost or stolen devices, links clicked in phishing emails, and training completion rates, but specific metrics to measure security culture and which were regularly monitored were preferred.

The requirements for the measurements were to ensure they were comparable across years, to see the trends, and for the metrics to be used monthly. In addition, there should be a correlation between them to see if the monthly metrics validate the annual results.

The project team did not have a clear picture of the options that could be used to measure security culture, hence, the work began by reviewing related literature to understand and clearly define security culture. This was discussed within the project team, and a common definition was agreed upon. Several definitions were reviewed, but in the end, the team concluded by using Roer's definition: "The ideas, customs and social behaviors of a particular people or group that helps them be free from threat and danger.". This definition was chosen as it includes behaviors (our key focus area) of a certain group (in this case, employees) and the security perspective (being free from threat and danger). (Roer 2015, chapter 1.)

Once the literature review was completed and a ready-made framework was deemed not to exist or be available, an interview was held with an industry-leading security awareness

expert to verify the conclusions and get recommendations. The interview included the following questions:

- Does a common framework to measure security culture exist?
- Are you able to recommend a specific one?
- Do you have any views on questionnaires, such as the UISAQ (Users' Information Security Awareness Questionnaire), the SeBIS (Security Behavior Intentions Scale), FMS (Four Measures Scales), HAISQ (Human Aspects of Information Security) and the BCISQ (Behavior Cognitive Information Security Questionnaire)?
- Do you know anyone who is using them?

The expert confirmed that a commonly used and validated framework did not exist. He did, however, share a version of metrics that had been created by his organization with the help of other security awareness experts. This included five categories that measured employee behavior, culture, strategy, compliance, and a potential ambassador program. In addition, he provided a sample questionnaire that included 15 questions, divided into perceptions, attitudes, and beliefs of five categories: the security team, security policies, security training, cybersecurity in general, and security behaviors.

When discussing the models that were referred to in the questions, he concluded that he had not used them. He reminded of two key issues to consider: What do we want to measure and why do we want to measure it. According to him, three things can be measured: Culture (what people think), knowledge (what people know), and behavior (what people do). All of these are important, but also different. Therefore, it is important to determine what is being measured, and why it is being measured. A strong recommendation was to decide on the reason for measuring something and what the results would be used for. This was emphasized from the viewpoint that organizations often take the time to measure something, but if nothing is done with the results, it is a waste of time.

Roer's book "Build a Security Culture" and Carpenter's and Roer's "The Security Culture Playbook" were used as references to understand how security culture relates to a security awareness program, the critical concepts and elements of security culture, and how it can be measured. In addition, other literature and academic research were reviewed to understand the main measurement methods. Most recommend using a combination of data and statistics, for example, security incidents, and using a survey to gather user input on behavior and attitudes. In addition, user interviews were recommended to validate the survey and data results.

The project team chose to use all four options for measuring security culture: using a survey, conducting interviews, using data and statistics, and conducting red teaming

exercises. A workshop was held to define the need and set of requirements for a security culture survey. The agenda of the workshop included:

- Defining the goals for the survey
- Discussing ideas and setting requirements
- Defining and addressing restrictions
- Agreeing on suitable methods and frameworks
- Defining reliability and validity

During the workshop, the project team agreed that the main intention of the survey was to measure the security culture of Organization X, enabling the project team to quantify employees' common customs and behaviors towards security. Understanding employees' attitudes and behaviors around security was deemed highly important to ensure the team could address these behaviors and thereby reduce the risk and the impact of possible security incidents and breaches.

To ensure continuous review of the security culture, the survey questions had to be designed in a way that guaranteed they were applicable for the next 5-10 years, allowing the team to execute the survey on an annual basis and compare results across the years.

The objectives for the security culture metrics were agreed as follows:

- To identify weak areas that most likely pose the greatest risk to the company
- To understand why employees are behaving the way they are
- To identify activities or initiatives that have the greatest impact and are therefore worth continuing
- To identify activities or initiatives that have the lease impact and therefore need to be changed, discontinued or improved
- To be applicable for the next 5-10 years

Next, Quinn and Rohrbaugh's (1983) Competing Values Framework was studied to understand how they measure culture, and thereon Hayden's (2015, chapter 5) Competing Security Cultures Framework on how it uses the Competing Values Framework, but from a security context.

Hayden's Competing Security Cultures Framework includes a Security Culture Diagnostic Survey (SCDS), which has a predefined set of ten questions that seek to define an organization's unique traits and cultural and behavioral norms. The full questions can be found in Appendix 5. The results of the survey indicate what characteristics, values, and behaviors an organization exhibits based on four different security cultures outlined in the framework. (Hayden 2015, chapter 5)

4.4.2 Act

The project team analyzed all survey questions in the SCDS and agreed that the answers to the questions were very long and therefore decided to break them down into shorter sentences to get a better understanding of their core meaning. These can be seen in Table 1.

Table 1. Security Culture Diagnostic Survey questions and proposed shorter versions (Hayden 2015, chapter 5)

SCDS survey question	SCDS answers	Project team's shorter version
1. What's valued most?	Stability and reliability are valued most by the organization. It is critical that everyone knows the rules and follows them. The organization cannot succeed if people are all doing things different ways without centralized visibility.	I value following rules and guidelines.
	Successfully meeting external requirements is valued most by the organization. The organization is under a lot of scrutiny. It cannot succeed if people fail audits or do not live up to the expectations of those watching.	I value meeting external requirements.
	Adapting quickly and competing aggressively are valued most by the organization. Results are what matters. The organization cannot succeed if bureaucracy and red tape impair people's ability to be agile.	I value agility and the ability to adapt to changes quickly.
	People and a sense of community are valued most by the organization. Everyone is in it together. The organization cannot succeed unless people are given the opportunities and skills to succeed on their own.	I value the sense of community.

The original answers to the SCDS questions were written objectively and in the third person. The team was concerned that presenting the answer alternatives in this way would be perceived by employees as too vague, and employees might find it challenging to answer questions as they are asked to evaluate from a wider organizational perspective, not from a personal perspective.

After analyzing the SCDC questions, the project team concluded that the questions were difficult to answer by regular employees, as they required knowledge of how the organization, for example, managed its technology or operations. In addition, when discussing the Competing Security Cultures Framework, it was rather clear where Organization X would sit on the graph, and hence the results would not provide much insight into the actual security behaviors or attitudes of employees. For this reason, the project team decided to investigate other survey alternatives.

The project team then decided to study Roer's (2015, chapter 7) Security Culture Framework and its seven dimensions used to measure security culture. In this model, each dimension is individually measured and placed on a scale from low risk to high risk. Research on the Security Culture Survey concluded that the survey was not available to the public but had to be purchased as part of a security awareness program offered and sold by a private company. While the actual survey questions were not available, Roer has published the seven dimensions as well as an outline for each dimension with a set of broad-level example questions. This overview was evaluated, and the project team concluded that even though they could not directly use the Security Culture Survey or its ready-made questions and framework, they could utilize the available dimensions and outlines. An overview of Roer's Security Culture Survey (Roer 2015, chapter 7) can be found in Appendix 3.

After concluding that the questions in the Security Culture Survey could not be accessed and therefore directly used, the project team reviewed example questions created by SANS Institute (2021). While the example questions were seen as good, the project team agreed that many were not necessarily applicable to Organization X or did not provide answers to the questions the team was seeking. The project team, therefore, decided that while a ready-made solution would be easy to implement, the team needed to create a survey of their own that specifically addressed their needs.

By using questions from multiple sources, adjusting them based on the specific needs of Organization X, and grouping them with the seven dimensions of the Security Culture

Survey, the project team was able to create the first version of their security culture survey. This can be found in Appendix 6.

Next, monthly data and statistics were considered. Chaudhary et al (2022) define the criteria for good metrics to be:

- Consistent measure (i.e., no subjective criteria)
- Cheap or economical to gather (i.e., preferably automated)
- Expressed as a cardinal number of percentages
- Expressed using at least one unit of measure
- Contextually specific (i.e., relevant to decision-makers so they can act)

SANS Institute (2021) has created a set of human risk metrics, which they have divided into the following groups: compliance metrics, behavior metrics, culture metrics, ambassador program metrics, and strategic metrics. The model includes a set of 41 metrics divided into the above groups. Eight of those questions form a human risk score that can be used by management to see the current state of an organization's human risk. When evaluating the metrics, it was evident that not all of them could be applied to Organization X, and in some cases, the data gathered could not be validated. For example, password sharing with others was measured via a security culture survey, and thus the accuracy of the results could be questioned. From the 41 suggested metrics, 13 were chosen to be used in the first draft. These are listed in Appendix 7.

4.4.3 Observe

The first drafts of the culture survey and metrics were presented to key stakeholders and discussed. The first draft was seen as a good starting point, but it needed a bit more work in terms of defining the actual questions and their concrete relevance, as well as the actual wording. Using the seven dimensions by Carpenter and Roer (2022) was seen as a good idea as it gave structure and ensured that important areas were addressed.

The 13 metrics were also seen as a good starting point, but based on feedback, not all the data was easily accessible or existed. In addition, the number of metrics could be decreased to provide an even better overview of the most important factors. For this reason, it was decided to reassess the metrics and see how well they measure security culture and whether the data added true value.

4.4.4 Reflect

Regardless of a lengthy and detailed literature review, it was surprising not to find a ready, or nearly ready-made, version of metrics and a survey that could be directly utilized at Organization X. However, it was evident that researchers had come to the same

conclusion that a ready-made solution is not available, since the survey questions and metrics depend on the organization in question.

During this cycle, the project team succeeded in completing a thorough literature review and created a first draft for measuring security culture. Key learnings during this cycle include that investing sufficient time in planning, preparing, and reviewing literature is highly important and a key success factor.

4.5 Creating the Second Draft

The second research cycle began at the end of December 2023 and focused on improving the first versions of the survey and metrics, as well as deciding on interview questions.

4.5.1 Plan

During the first action research cycle, the project team was able to create the first draft of the security culture survey for Organization X. This was shared with a colleague at the beginning of the second cycle with a colleague who was simultaneously working on a survey to measure the risk culture at the commissioning organization. The draft created by the project team was shared with the colleague, who also shared his survey. It was concluded that there was very minimal overlapping with the two surveys, however, it was agreed to share the results to cross-reference and find potential correlations. A timeline for distributing the surveys was also agreed to ensure that both surveys were not sent out at the same time.

Alignment meetings were also held with communication and management support departments to provide transparency on the work that was being conducted and to gather input.

When designing the second version of the security culture survey, the project team had to take into consideration several issues, such as the length of the survey, how the questions were written, and how they would be answered. During a workshop in January 2024, these alternatives were discussed from multiple angles.

Roer’s (2019) Security Culture Survey consisted of 31 questions, however, the team concluded that this was too many questions. To ensure employees take the time to complete the survey, it was clear it could not be too long and time-consuming, yet it had to include enough questions to address and provide answers to the survey goals. The project team agreed on no more than a total of 20 questions.

It was also important to include demographic questions on the respondents, such as age, country, and business area, to see whether there were any correlations between demographics and behaviors and opinions. Including demographic questions would naturally extend the questionnaire and thus possibly decrease the number of questions addressing security behaviors and perceptions, but they were deemed as important information to draw conclusions and find possible correlations.

During the workshop, various alternatives for demographic questions were considered, such as including gender, but the team concluded that most likely, there would not be significant gender-related differences in the answers. In addition, going forward, security awareness activities could not be directed to employees based on gender. Age, on the other hand, was seen as an important factor to understand if there were differences between younger generations versus older ones. We were interested in seeing if younger, more technologically experienced employees, took security more seriously or found it more relevant to them. Therefore, we decided to ask employees to choose the age group they belonged to. Employees were also given the option of choosing “prefer not to say”.

Since Organization X is a mix of employees who have recently joined, to employees who have spent 40 years in the company, we were interested in finding out whether there were any differences in the behaviors or beliefs based on how long an employee had worked at Organization X. We were particularly interested in finding out if the length of employment at Organization X influenced the respondents’ answers. Therefore, it was agreed to provide options to indicate the length of employment.

As Organization X has operations in multiple countries and locations, we also wanted to investigate whether cultural differences could be seen in the employees' responses. Hence, we wanted to include a question on what country the respondents were located in. As Organization X has offices in various locations, there was a possibility that the results could indicate that employees in certain countries had more negative or positive values or behaviors. If so, this was of interest to the project team as it could potentially identify areas or issues to improve or learn from.

The final demographic question that the team wanted to include was which business area the respondent belonged to. This would naturally allow the team to see if employees’ behaviors or opinions differed based on where they were in the organization. During previous work, the project team had noticed a stronger focus on security by certain senior managers and wanted to see if this could be seen in the survey results and employees’ perceptions.

To ensure the answers provided were as truthful as possible, the team decided that the survey had to be anonymous. This would ensure that the team would be given honest answers, without any fear of repercussions or improper disclosure of information. For the team, this was a concern, as there was a risk of employees being afraid to answer questions that could indicate or prove they had acted against the organization's policies or procedures. Based on internal company rules, the team was obligated to use Microsoft Forms for the survey. Access to the form and results was restricted to only two employees to ensure the highest level of confidentiality.

Most of the team workshop was allocated to discussing the actual survey questions and how they should be adjusted based on feedback received. The format of the questions was discussed. Again, the team turned to various examples and discussed alternatives. Open-ended questions were deemed too time-consuming as their results needed to be manually analyzed and categorized to be comparable. In addition, simple "yes" and "no" questions were seen as too limiting. Hence, the team agreed on using concise statements that would be measured on the Likert Scale.

The Likert Scale is seen as one of the most reliable ways to measure people's attitudes, perceptions, and opinions, and it was used in most literature and examples. It provides the respondent with predefined answer alternatives that are measured on a scale. The most used scale is five alternatives, such as 1 is "Strongly agree" and 5 is "Strongly disagree". Likert-type questions are regularly used to provide the respondents with more options, and they are easier to quantify once the answers are analyzed.

Using the Likert Scale also enables questions to be asked in a way that ensures the answers are normalized. For example, all answers that are equal to 1 = Strongly agree are representative of a strong security culture. And vice versa, answers that equal 5 = Strongly disagree represent a weak security culture. Standardizing all answers in this way makes analyzing the data much easier. (SANS Institute 2021)

While a five-point Likert Scale was chosen, the team agreed that the survey should include one open question at the end to give employees the chance to also express their overall opinions or to address issues. It was decided to write the question so that employees were asked if they had additional comments related to the question topics or the overall security culture at Organization X. This limited the scope of the answers to security culture but also gave the employees the chance to raise any other related topics that the survey possibly had missed. Finally, the team discussed that based on the survey results, the team might have additional questions for respondents, and hence it was agreed to include at the end of the survey a possibility for employees to indicate if they

were willing to be interviewed. This would also allow the team to ask new questions and get more in-depth answers.

To guarantee the reliability and validity of the data collected via the security culture survey, certain steps needed to be addressed. During the workshop, the team discussed the action needed and decided on specific steps. First, the team considered the distribution method for the survey and how to ensure the sampling was random and captured the entire spectrum of employees across Organization X. Random sampling ensures that all employees have an equal probability of being included, which aims at minimizing bias and improving generalization. Multiple distribution methods were considered, including randomly choosing employees to send the survey to. Publishing the survey online on the company intranet or other communication channels could potentially result in unreliable data, since the responses could be biased, for example, attracting employees interested in security or culture. It was therefore decided that the best option would be to choose random employees across all countries and organizations and send the survey via email.

We also calculated how many responses we would need to ensure that the gathered data was statistically reliable. This was done by using an online calculator. Based on the number of existing employees, we concluded that we needed a total of 381 responses. To succeed, we agreed to initially send the survey to a total of 1,500 employees and replicate it with a new list of randomly chosen employees if we were unsuccessful in securing the number of responses needed with the first send-out.

To validate our findings with additional measures, the team agreed to conduct interviews in addition to collecting data via the survey. Employees were asked at the end of the survey to indicate whether they would be willing to take part in an interview. These respondents would also be chosen randomly, and the interviews would be done with pre-made questions.

4.5.2 Act

A cybersecurity-aware person is characterized as being capable of identifying, judging, preventing, or resolving threats in cyberspace (Wang et al 2018). We therefore wanted to create survey questions that measured how well employees could achieve these goals of identifying, understanding, preventing, and/or resolving threats.

Since many of the previously reviewed surveys and frameworks had good elements, it was decided to utilize the parts that applied to our goals. Most importantly, we wanted to create questions that would provide insight that would allow us to draw solid conclusions

on the overall security culture of Organization X and provide concrete input on what issues to address and focus on through the Organization's security awareness program.

Roer's Security Culture Survey was used as a basis for building the survey questions, which were supplemented with other frameworks and available examples. Using Roer's security culture dimensions enabled us to divide the questions into seven different categories: attitudes, behaviors, cognition, communication, compliance, norms, and responsibilities. Using these dimensions ensured we covered all relevant topics and areas and created structure.

Attitudes

According to Roer (2015, chapter 7), employees' attitudes, in other words, feelings and beliefs, towards security protocols and issues, can be measured by asking how much employees overall care about security and whether their attitudes towards security are positive, neutral, or negative.

Based on our survey goals, one of the most important questions to ask employees was whether they a) felt that security was a priority, and b) this was also visible in the organization's core values. Answers to these questions would create the entire basis for the company's security culture and define whether a security culture existed and was felt by employees.

According to Bashforth (2019, 106), a company's values should be implemented top-down by senior management. Top management should live and breathe the organization's values, thereby acting as role models on how to behave. As a company's core values can significantly influence its employees' behaviors and attitudes and have a major effect on the decisions employees make, it is important from a security perspective to understand whether employees see top management and the organization as valuing security. Hence, the first survey question focused on measuring the security attitudes at Organization X.

After lengthy discussions with the project team, we chose to focus on two components: security was seen as a priority at Organization X, and was the company culture supported reporting security incidents. These two questions were addressed with the following statements:

Question 1. I believe that security is a priority and a part of our way of working at Organization X

Question 2. I feel comfortable reporting a security incident even if I have caused it

Behaviors

How employees behave has a significant effect on a company's risk posture, as employees can both be responsible for creating cyber incidents or for taking action to protect against them. In Roer's (2015, chapter 7) Security Culture Survey framework, behaviors are defined as employees' actions and the activities that impact an organization's security. Therefore, it is important to understand what employees consider acceptable behaviors and how employees experience each other's behavior.

To measure key behaviors, the project team discussed which important areas should be included. This was done by taking a risk-based approach and by pinpointing the most likely security risks that can be caused by employee behavior.

Cybercriminals aim to gain access to an organization's systems and data, and this is often done by utilizing the human element and the errors humans make. One example is for employees to intentionally use weak passwords or reuse existing passwords. As this is a common way for cyberattacks to occur, the team felt it was important to ask employees how well they adhered to keeping their passwords safe and the organization's password policy. Instead of creating a statement about their behavior, their perspective was changed by their colleagues. According to SANS Institute (2021), people tend to answer security behavior-related questions more positively as they are afraid of being punished for not acting according to official rules. Hence, SANS Institute recommends asking questions where employees evaluate their colleagues, as this should provide more honest answers.

Question 3. My colleagues would never share their passwords with anyone else

In addition, we chose to measure other key security behaviors, such as willingness to obey security rules and policies, for example, wearing their access card visibly and labeling information. By obeying companywide security policies and instructions, employees ensure they take appropriate action to prevent attacks from occurring. After multiple discussions, the team concluded to include a question focusing on protecting against social engineering attacks from a physical security perspective.

In the cybersecurity area, attention is often paid to technology and protecting against technological risks, yet physical security can be just as important. Social engineering attacks can often start by gaining access to an organization's premises. This is done by manipulating an employee to grant access. At Organization X, one of the most important security rules was to ensure no one was able to gain unauthorized access to its premises. All employees received annual training on the risks associated and the required actions to

be taken. One policy was that each employee had to always wear their access cards visibly. For this reason, it was decided to ask employees whether they behave accordingly. The results for this question were also important as it would provide insight as to whether additional training and action were needed to ensure full compliance.

4. I always wear my access card visibly at Organization X premises

Finally, as Organization X had, within the past few years, launched new training initiatives and significantly increased security training frequency and quality, the team wanted to dedicate a question to finding out if employees felt that the provided security training had changed their behavior. This statement could also provide information on whether training or other activities have affected the company's security culture.

6. I noticed a change in my behavior as a result of security training

Cognition

According to Roer's (2015, chapter 7) Security Culture Framework, cognition refers to how employees understand security issues, what knowledge they have on the topic, and how aware they are. The key question was: Do employees know how to report an incident or a situation they find suspicious? The answer to this question would provide valuable insight into whether employees had the required knowledge and skills to prevent possible attacks.

As reporting a suspicious situation could potentially stop an attack before it advanced to an actual data breach or incident, it was important to measure if employees knew how to act. For this reason, the following statement was included in the survey:

6. I know how to report something suspicious or abnormal

Cyberattack types with a human element, such as business email compromise, phishing, and social engineering, result in the highest losses for organizations. (IBM 2024) For this reason, attacks that utilize the human component pose a greater financial risk and should be continuously monitored and measured. As mentioned earlier, preventing phishing attacks is a top priority at Organization X. While the organization has multiple advanced systems in place to prevent phishing emails from reaching employees' email inboxes, sometimes these emails are advanced enough to bypass all protective measures. For this reason, employees are constantly educated about phishing and how to spot the signs.

Generative AI is used by cybercriminals to create more believable phishing emails, making it easier for employees to fall prey to phishing attacks. As a result, organizations

can expect more complex and realistic phishing attacks to occur. (World Economic Forum 2024) Since phishing is seen as a realistic cyber risk at Organization X, it was important to measure how well employees can recognize the signs. These results would provide valuable information on how much more training and awareness employees need going forward.

Cyber incidents occur in many forms, but to limit the number of survey questions, we chose to focus on the human element and thus to measure employee cognition related to cyberattacks. With the advances in the cyber arena and the likelihood of employees being targeted by phishing and social engineering, we chose to ask employees how they perceived their ability to identify these kinds of attacks and thereby prevent cyberattacks:

7. I know how to recognize phishing

8. I can recognize signs of social engineering (e.g., tailgating)

As part of the behavior-related questions, employees were asked if they labelled information correctly. In the cognition area, the question was taken one step further to understand whether employees not only label information, but they truly understand how it is labeled, and more so, why it is labeled. Because information classification is such an important area at Organization X, it was necessary to ensure that both aspects, behavior (acting) and cognition (understanding), were included.

Information classification is done at Organization X by assigning information to one of four classes. These classes are explained in detail in multiple training courses and should be understood due to their repetitive nature by all employees. The project team discussed whether employees should be asked if they label information correctly, in other words, took the correct action, instead of indicating whether they know or understand how to do it. The challenge was that based on the team's experience, employees were aware of company rules, but we assumed that information classification was not performed due to inadequate knowledge or know-how, but due to a lack of prioritization. Assigning a certain information class results in certain actions, such as limiting the information. This can be seen as time-consuming and can be bypassed by labeling incorrectly.

A key cornerstone of information security is confidentiality, integrity, and availability of information. This includes protecting information, both physical and digital, to ensure it is not available or disclosed without authorization. To prevent this, Organization X has strict policies and instructions on how to handle and classify information. Adhering to these rules ensures information is handled with due care and accessed only by authorized parties. Due to the Organization’s line of business, information classification is of utmost

importance, and correct behavior is ensured with detailed instructions and mandatory training. As this was a highly important area, it was decided to ask employees to indicate their behavior and whether they knew to adhere to the policy by answering the following statement:

9. I understand and follow Organization X's information classification rules

Communication

The fourth dimension in Roer's Security Culture framework is communication. Questions in these areas are designed to measure the quality of communication and how well employees are provided with support on issues and incident reporting. This includes investigating how security is communicated within an organization, and how employees are involved and supported. A security culture where employees feel it is safe to discuss security, and leadership shows openness and acceptance, will help foster a good security culture. (Roer 2015, chapter 7.)

Organizations that have a good security culture ensure that discussing and raising security-related issues is a norm and encouraged. This builds employee commitment and makes it easier for employees to report incidents, even if they cause them. (Roer 2015, chapter 7.)

In larger organizations, it is often difficult to understand who to contact, and hence it was important for us to understand if employees felt like they knew who to contact and had dialogues with about security-related issues. The hypothesis was that if employees knew who to contact, then the security awareness and communication activities our team had been running would have been successful: seen and heard. For this reason, we chose to include the following statement:

10. I know who to contact in case I have questions about security matters

As part of our efforts to bring security closer to the rest of the organization, we created security-related content for team meetings. These were promoted to all leaders, and they were given instructions on how to conduct these short sessions with their employees. The aim was for leaders to act as role models toward employees and to do their part to promote good security behavior. Therefore, the project team wanted to measure to what extent information security was discussed in team meetings. Hence, the following statement was included:

11. We discuss information security in team meetings

Norms

Norms are internal and unwritten rules that represent how things are done in a certain organization. They are unique to organizations and showcases, for example, beliefs, values, and behaviors. Changing an organization's norm is time-consuming and challenging, as it requires changing an entire group's behavior. (Roer 2015, chapter 7.)

In the Security Culture Survey framework, the norm dimension measures how well security-related beliefs, values, and behaviors are rooted in the norms of an organization. From a security culture perspective, the project team wanted to understand how employees saw information security concerning their jobs, and whether they felt it was preventing them from doing their job. The results for this question would show on an overall level how employees saw security – whether it was something they were obliged to, understood and supported, or simply saw it as hindering their work.

12. Information security does not get in the way of doing my job

Norms and organizational culture often represent senior management's values and behaviors. They act as role models and are responsible for acting according to the organization’s culture and values. It is for this reason that it was important to measure whether employees felt and perceived that leadership at Organization X prioritized security. The results would indicate whether there was a need to act and work more with leadership. In addition, the results would help show the team’s challenge to management and the need for improved support.

13. Our leaders lead by example and actively promote security matters

Compliance

Roer’s (2015, chapter 7) compliance dimension measures how well employees adhere to policies and instructions. It can be said that many of the previous statements created for the survey also measure adherence to instructions, but in this dimension, the focus is more on the broader view of whether employees know these instructions exist, and if so, to what extent they follow them.

Organization X has a vast number of policies, guidelines, and instructions, which are often written in very official and difficult language. They include legal and regulatory requirements and can be seen as unrelatable by individual employees. For employees to know how to behave, they must first know where that information can be found, and second, if the instructions provided are clear. To understand how employees experience these two aspects, we decided to ask the following questions:

14. I know where to find security instructions that are relevant to me

15. I believe that security instructions are clear at Organization X

Responsibilities

For employees to take action to prevent cyberattacks, they need to possess the knowledge and skills to act correctly. In addition, they need to feel that their actions have a direct impact on the organization's security. The Security Culture Framework's final dimension measures to what extent employees follow security rules and to what extent employees feel empowered that their actions matter.

Ensuring employees feel they have a responsibility to protect their organization provides them with the needed motivation to step up. Should an incident occur, employees must take action to prevent the consequences and resolve the situation.

16. My actions have a significant impact on protecting Organization X

17. I feel comfortable addressing unusual or suspicious behavior in person

The project team created and concluded the survey questions based on multiple discussions until everyone in the team agreed that all possible viewpoints were considered. Most of the questions were specifically designed from a first-person perspective, as this would create accountability and ensure employees answer the questions from their perspective, not from a collective company or teamwide viewpoint. For two questions, this was not possible as they asked about team and leadership behavior. The final version of the aforementioned statements can be found in Chapter 4. In addition, changes were made to wording, such as changing "organization" to the company's name. The company name was used throughout the survey to create ownership.

The project team did not make any changes to the metrics created in the previous cycle but was eager to get more input from stakeholders on them.

A set of interview questions was created to supplement the survey. It was agreed that the interviews would be conducted informally, where additional questions could be asked if needed. The team agreed that the following questions would be asked at least:

- How much do you know about cybersecurity and cyberattacks? Can you give examples?
- Can you tell us about the security policies and instructions at Organization X? Do you know where to find them?
- How important do you feel security is at Organization X?
- What is your impression of the leadership's approach and commitment to security?

- Do you feel that security incidents are handled adequately?
- Do you discuss security with your colleagues or in team meetings?

4.5.3 Observe

The revised and improved questionnaire was presented to key stakeholders and discussed in detail. In the end, no changes were made, as the reasoning behind the questions was seen as valid and relevant. The interview questions were discussed and adjusted based on feedback from stakeholders.

The metrics that were designed during the first cycle were discussed again, and it was agreed at this stage to remove the average time to detect an incident, the costs related to an incident, downtime related to an incident, and compliance or audit violations. These were removed as the data was not comparable or reliable. In addition, it was agreed to add intentional data leakage, however, these statistics are highly confidential and hence would most likely not be included in the version distributed to most participants.

The organization's Chief Security Officer approved the measurement methods and distribution of the survey.

4.5.4 Reflect

A significantly larger amount of time was put into altering the survey statements during this cycle, which was logical as in the first cycle focus was on analyzing literature and available frameworks. The iterations with key stakeholders and discussions within the working team made a significant difference, as this ensured the statements were considered from multiple angles.

In the end, four metrics were removed from the final list, as it was important to ensure that the data was accurate and provide concrete input. Too many metrics can also be time-consuming to produce and analyze.

A key learning from this cycle was that rewriting and adjusting the survey questions was time-consuming, however, extremely important to ensure the questions would provide the information needed.

4.6 Implementing the Final Version

In mid-January 2024, the project team began working on finalizing the metrics, survey, and interview questions based on the received input. Once the adjustments were made,

the project team began gathering the agreed-upon metrics and preparing to distribute the survey.

During the first action research cycle, the project team was able to create the first draft of the security culture survey for Organization X. This was shared with a colleague who was simultaneously working on a survey to measure the risk culture at the commissioning organization. The draft created by the project team was shared with the colleague, who also shared his survey. It was concluded that there was very minimal overlap with the two surveys, however, it was agreed to share the results with each other to cross-reference and find potential correlations. A timeline for distributing the surveys was also agreed to ensure that both surveys were not sent out at the same time.

Alignment meetings were also held with communication and management support departments to provide transparency on the work that was being conducted and to gather input. This was done twice: once during both the first and second cycle. In the second meeting, the final survey and metrics were presented and approval requested and received. The project team also held meetings with colleagues in other organizations, who were responsible for the data the suggested metrics were built on. Access and the reliability of the data were verified and agreed upon.

4.6.1 Plan

It was agreed that the survey would be sent out at the end of February 2024, which gave the project team approximately four weeks to add the final questions to the survey tool and ensure distribution.

4.6.2 Act

The preferred survey tool at Organization X was Microsoft Forms. Which was used for sending out, as all employees had access to it, it was highly secure, and employees were used to using it. In addition to creating the survey in Microsoft Forms, the survey was sent out to participants via the tool.

The text accompanying the survey was reviewed and edited multiple times to ensure it was not too long and included all relevant information. Since it was the first time that a security culture survey was conducted at Organization X, the project team felt it was important to explain what security culture is, why it is important, and why the survey was being sent out. In addition, a specific page was created on the company intranet to provide additional information and contact details.

The survey was sent out on 20 February 2024 to 1,500 employees across all business areas and countries. The survey was open until 18 March 2024 and received a total of 549 responses. A total of 40 employees indicated they were willing to be interviewed. Respondent interviews were carried out, and results were analyzed by the end of April 2024.

The results of the survey were presented to management and the security organization. In addition, the created metrics were used every month to create a management report.

4.6.3 Observe

The entire process of creating the final metrics and sending out the survey was successful and achieved on time and without any challenges. The number of responses surprised the team, and ultimately, there was no need to send the survey to additional employees, as the response rate was already high. The feedback from interviews was positive, and there seemed to be a genuine interest in security culture at Organization X. With that said, the project team was also able to pinpoint areas that needed further development and attention.

4.6.4 Reflect

The final action research cycle was planned well and executed accordingly. During this cycle, most of the time was allocated to sending out the survey and analyzing the results. The distribution of the survey and the survey tool worked well. It is recommended to use the same method of distribution and survey tool.

The results of the survey were highly interesting, and in general, employees expressed their interest in security and acknowledged its importance. A few comments referred to the questionnaire and its questions, however, most of the comments provided positive or constructive feedback on how various security aspects are run at Organization X. From this perspective the open question in the survey provided valuable insight and additional input.

The employee interviews also allowed the team to dig deeper into employee perceptions and behavior. During the interviews, some employees admitted that they did not know about security instructions or policies, yet in the discussions, they were able to demonstrate understanding and even explain the rules. Therefore, while some employees felt that they did not have adequate knowledge, they were not consciously aware that they did. Several employees highlighted a lack of management focus on security, which affected employees' behavior and perception of the topic's importance. This indicated that

management involvement was needed to ensure security becomes an everyday topic, thereby improving the organization's overall security culture.

Key learnings in this cycle included the importance of proper planning, and given the chance, employees were very willing to participate and engage in the topic.

4.7 Summary of the Action Research Cycles

Utilizing action research as a method was well received and ensured work could be carried out in cycles, each cycle building on top of the previous one. It allowed the team to focus on planning, take time to act, use others to observe and improve, and finally reflect on what went well and what could be improved.

The first action research cycle was structured and included a high level of planning and focused on understanding the topic and reviewing the literature. The initial literature review and analysis of academic research took more time than anticipated, however, it was rewarding and most definitely had a positive effect on the result. It was surprising to see that a common industry-approved method to measure security culture does not yet exist, and therefore, utilizing multiple studies, methods, and frameworks was the right approach.

It was important to take time to agree on a common goal and objectives for the research, as this ensured the team understood what to focus on. Due to the comprehensive literature review, the team was able to decide rather quickly which measurement options to use and which frameworks to apply. The first cycle also included testing different options and concluded with a first draft.

The second action research cycle focused on improving the first draft by having multiple discussion rounds on each question and reasoning. Taking the time to rewrite and adjust the questions ensured that multiple aspects and viewpoints were considered. Investing enough time and precision ensured the questions were thoroughly thought through and should not leave room for interpretation. Utilizing one framework to create the basis of the survey was a good idea and created the necessary structure.

The second cycle resulted in a revised and final set of survey and interview questions, as well as a set of metrics. Again, utilizing literature and frameworks provided guidance and an open atmosphere among the team, and continuous alignment with stakeholders ensured an optimal result was reached. Gathering feedback and suggestions was key to success.

The third action research cycle focused on running the survey, interviews, and gathering metrics based on the work completed in cycles one and two. Teamwork and proper planning ensured that the team was able to deliver according to plan and without challenges.

During the action research cycles, the project team worked together virtually across various countries by utilizing communication channels as well as brainstorming sessions and workshops. Proper project management ensured the team had a plan, timeline, and a clear vision of the result. This ensured the team knew what to deliver and which areas to focus on.

The full suggestion for measuring security culture at Organization X is presented in Chapter 4.

4.8 Final Measurements and Metrics

Using a combination of four methods: surveys, interviews, metrics, and red teaming exercises, Organization X will be able to establish the organization’s security culture level. This will be accomplished on an annual basis with a survey, which should indicate change from the previous years, and with interviews that should provide additional information and explanations about employees' perceptions, behaviors, values, and knowledge. The answers could potentially also raise important issues, recommendations, or new or emerging risks. Finally, the implemented metrics and red teaming exercises should be used to identify key risks, analyze trends, validate results from the survey and interview, and provide continuous feedback and information on employee behavior and the security culture at Organization X.

4.8.1 Security Culture Survey

Based on an extensive literature and academic research review, known security culture frameworks were used to create a security culture survey for Organization X. A ready-made option was not identified, as available surveys were either focusing on different topics, not applicable to Organization X, or deemed too detailed or lengthy. The final survey is a result of utilizing various theories and frameworks as well as multiple iterations based on internal discussions and observations. Questions included in Table 2. were answered with a five-point Likert scale (1 = Strongly disagree, 5 = Strongly agree).

Table 2. Final security culture survey for Organization X

Culture Dimension	Nr.	Statements
Attitudes	**1**	I believe that security is a priority and a part of our ways of working at Organization X
	2	I feel comfortable reporting a security incident even if I have caused it.
Behaviors	**3**	My colleagues would never share their passwords with anyone else
	4	I always wear my access card visibly at Organization X premises
	5	I noticed a change in my behavior as a result of security training
Cognition	**6**	I know how to report something suspicious or abnormal
	7	I know how to recognize phishing
	8	I can recognize signs of social engineering (e.g. tailgating)
	9	I understand and follow Organization X's information classification rules
Communication	**10**	I know who to contact in case I have questions about security matters
	11	We discuss information security in team meetings
Norms	**12**	Information security does not get in the way of doing my job.
	13	Our leaders lead by example and actively promote security matters
Compliance	**14**	I know where to find security instructions that are relevant to me
	15	I believe that security instructions are clear at Organization X
Responsibilities	**16**	My actions have a significant impact on protecting Organization X
	17	I feel comfortable addressing unusual or suspicious behavior in person

The following demographic information was asked: number of years employed by Organization X, business area, location (country), and age group.

At the end of the survey, employees were given the option to provide additional comments about the survey or the overall security culture at Organization X. Of the 549 respondents, 68 provided additional comments. The last question in the survey asked if the respondent was interested in taking part in an interview. Of the respondents, 43 indicated that they would be willing to share their thoughts in more detail.

4.8.2 Security Culture Interviews

The interview questions were reviewed and adjusted after the second cycle. For some questions, the wording was changed, and new questions were added. While the list of questions is rather extensive, they are designed to gather more detailed information on employees' behavior and observations and to provide an understanding of why employees behave or view issues in this way.

The interviews are carried out as semi-structured, where the interviewee can change the order of the questions depending on the interview. In addition, the interviewee has the option to ask additional questions if topics arise in the interview that should be clarified or researched in more detail.

The final interview questions included:

- How much do you know about security and threats to Organization X? Can you give examples?
- Have you witnessed incorrect behavior? If so, what happened and why?
- Have you been in security situations where you do not know how to behave? If so, when?
- Can you tell us about the security policies and instructions at Organization X? Do you know where to find them?
- How do you feel about the security level at Organization X?
- What is your impression of the leadership’s approach and commitment to security?
- Have you discussed security with your colleagues? If so, when and why? If not, why not?
- What do you think are Organization X’s greatest security risks?
- What would you do to improve the security culture at Organization X?

4.8.3 Security Culture Metrics

A thorough literature review was conducted to identify suitable metrics. This included industry reports and methods suggested by organizations such as the Information Security Forum, SANS Institute, and National Institute of Standards and Technology. The final list of chosen metrics includes ones that can be used for regulatory compliance (e.g., percentage of employees having completed annual training), ones to measure employee behavior (e.g., click rate in simulations), and adherence to company rules (e.g., data leakage prevention). In addition, these metrics should also cover the main human risks: human error, social engineering, authentication, detection and reporting, and employee misconduct.

Table 4. Final security culture metrics for Organization X

Metric name	What is measured?	How is it measured?	When is it measured?
Training completion	Percentage of employees that have completed annual training	Learning Management System (LMS)	Annually
Reinforcement training	Percentage of employees completing voluntary training	LMS	Monthly
Phishing click rate in simulations	Percentage of employees falling for simulation	Simulation program	Monthly
Phishing reporting	Percentage of employees reporting the simulation	Simulation program	Monthly
Phishing report offenders	Percentage of employees repeatedly falling victim in simulations	Simulation program	Monthly
Multi-Factor Authentication adoption	Percentage of employees using Multi-Factor Authentication	System admin information	Monthly
Lost/stolen devices	Percentage of devices that were lost or stolen	Asset register	Monthly
Accidental Data Loss	Number of employees sharing sensitive information by accident	Data Leakage Prevention (DLP) system	Monthly
Intentional Data Loss	Number of employees sharing sensitive information intentionally	Data Leakage Prevention (DLP) system	Monthly
Number of incidents	Overall number of incidents	Incident tracking process	Monthly
Policy violations	Number of times employees violate security policies	Incident tracking process	Monthly

4.8.4 Security Culture Red Teaming Exercises

Organization X has conducted regular red teaming exercises, such as ensuring employees are wearing their key cards, trying to access restricted areas, and observing employees' security behaviors in certain pre-defined situations. These activities would be continued, and the results reviewed by comparing them to the results from the survey and interviews, and seeing if they corresponded.

5 Discussion

In the previous chapter, the research results were presented by first describing the detailed action research process and finally the results. This chapter includes answers to the research questions, reflections on validity and reliability, ideas for further development, and lessons learned.

5.1 Key Findings

The objective of this thesis was to research how an organization-specific framework for measuring security culture could be designed and validated for Organization X. The research was conducted as action research, which involved working and gathering data during three cycles. This included searching for and analyzing existing methods, considering which elements could be used for Organization X, and designing prototypes. These prototypes were assessed and edited to create a complete set of measurements and metrics.

The research resulted in a framework designed to measure security culture with a combination of four methods: a survey, interviews, metrics, and red teaming exercises. These were explicitly designed for Organization X and captured the specific needs of the organization. The framework captures both an annual assessment with a survey, combined with interview questions, and monthly metrics based on concrete data. Both are additionally supplemented with red teaming exercises that can be executed when needed, or when resources are available. The framework should provide a comprehensive overview of the security culture at Organization X and its maturity and how it evolves.

The survey was designed to initially define the organization’s existing culture and, therefore, to be used on an annual basis for the next five to ten years to assess changes. The interviews were designed to be used alongside the survey to gather additional information and validate the survey findings. Finally, the metrics were designed to measure the culture on an annual and monthly basis and to also validate that the responses given in the survey, interviews, and seen during red teaming exercises corresponded with true behavior.

Organization X has a well-established security awareness program, which is a result of increased attention and focus on security awareness for the past five years. During this time, new resources have been hired, competencies increased, and a unique team has been established to drive the annual security awareness program. This includes, for example, developing and executing training, running awareness activities, and conducting phishing simulations targeting the entire organization.

The investigative questions for this thesis included:

- What are the key dimensions of security culture as identified in current academic and professional literature?
- Which methods and indicators are most effective in measuring security culture in practice, and how can they be adapted to fit the context of Organization X?
- What are the limitations and potential future developments in measuring and improving security culture in organizations?

The literature review conducted as part of this research examined the key concepts and frameworks of security culture as described in academic and professional literature. This included presenting various definitions of security culture, both by researchers and authorities, and explaining models and key elements of security culture. A few of the most important frameworks and models to measure security culture were presented, such as the Competing Security Cultures Framework by Hayden (2015), the seven dimensions of security culture by Carpenter and Roer (2022), and the Security Culture Framework by Roer (2015).

The comprehensive review was conducted on how academic and professional literature recommend measuring security culture, and concrete examples were studied in depth. While a common universal way to measure security culture does not exist, the most recommended option, and the one researchers have tested the most, was to send out surveys and questionnaires. In a few cases, these were complemented with interviews and metrics. Experiments, or what are referred to in cybersecurity as red teaming exercises, were mentioned in only a few instances. Data and metrics were discussed more often, but concrete metrics were often not suggested.

The literature review provided a good framework for designing a questionnaire, however, the questions were mostly written specifically for Organization X. It was evident in the previously conducted research and became also evident in this research that questions need to be applied to the organization in question, as all organizations are different. To a certain degree, some questions can be applied in general, but the most significant questions need to be designed based on the organization, the culture they want to have, and the risks they see.

This also highlights the challenge that many of the researchers raised: For measurements to be accurate, they would need to be adapted to the organization in question, as a commonly used method to measure security culture does not exist. The limitation will continue, since as long as a commonly agreed upon security culture definition has not been agreed upon, nor can a method to measure it. In addition, as long as organizations are unique, they will need specific metrics. Nonetheless, there is great potential to create a commonly validated and agreed-upon method that has elements that can easily be

adjusted based on the organization. There is also room for a set of predefined metrics that all organizations could use.

5.2 Recommendations

This research aimed at developing ways to measure security culture at Organization X. After a thorough review of the literature and academic research on security culture, one common and generally approved solution to measure security culture could not be found. This is because all organizations are unique, which means that one size does not fit all.

The methods created for this research were implemented at Organization X, and the strong recommendation is that they are executed, as designed, on a monthly and annual basis. This will provide the organization with clear information on the existing culture, but also how it is progressing, and help identify potential high-risk areas that need further attention.

The monthly and annual results should be presented to the senior management of Organization X on a regular basis to ensure they can monitor and take potential action on the results.

5.3 Reliability, Validity and Relevance

The quality of the research remained high due to the carefully chosen experts who were interviewed, the thorough literature review, and the fact that the research was conducted in three cycles. Working iteratively ensured that methods were tested before use, while experts validated that the work that was being done was correct. The research could have included more expert interviews, but this was not possible due to the time limitation of the project.

The project team also included highly experienced experts in the field of information and cybersecurity, which significantly affected the results positively. Their expertise, keen interest in the topic, and willingness to push through were instrumental to the success of the project.

The defined measurement methods for Organization X were executed in 2024, and the results of the survey and interviews surprised the project team. Employees were much more interested in security and behaving in the right way, versus the initial hypothesis. Input provided during interviews was value-adding, and employees were highly engaged. Conducting the survey and interviews was highly relevant as it enabled the organization to understand what most employees thought of security for the first time.

A few areas could have been improved, such as doing an actual test run of the survey with a small sample of employees and getting feedback on what could be improved. This could potentially have made the survey even better and enabled the project team to address issues that could be challenges for some employees, such as interpreting words incorrectly. Such feedback was not given to the project team but could be used to ensure even better quality.

5.4 Further Research

Based on the literature review and discussions with peers and experts, there is a clear need for organizations to measure their security culture in a reliable and common way. This would enable organizations to benchmark their results against other similar organizations, thereby identifying which organizations are doing well and what could be learned from them.

Most of the studies that have been conducted by researchers were only applied to a small number of people, often outside a business environment, which indicates that there is a strong need of doing research on actual organizations and on multiple organizations at a time. This would provide better input on the measurement methods, how to improve them, and whether they could be applied to organizations, at least to some extent.

5.5 Reflection on Learning

This research introduced me to a new way of working: Action research, which was a highly suitable method for this research and a method that I can utilize and apply also in the future. The three cycles ensured continuous improvement and created structure. The need to gather data, document, and analyze it was also interesting and taught me how important thorough and continuous documentation is for any research project. I will remember this also in the future when conducting research or working on a project.

The extensive literature review has significantly increased my knowledge and understanding of security culture, how it can be measured, and what methods can be considered. I now know and understand several of key frameworks, methods and concepts that can be applied and used in future work or studies.

I enjoyed reading academic research and will continue to do so regularly. It was interesting to learn about new studies and how the area of security culture is being developed and tested. I realized how little time I normally have to read and consider advances in our field due to busy workdays, something which has taught me to allocate more time to read and learn.

Most importantly, this research taught me how engaged and interested I am in this topic and that this was only the beginning. I plan is to continue research in this area and hopefully one day succeed in creating a measurement model that can easily be applied to any organization.

References

Alhogail, A. 2015. Design and validation of information security culture framework. Computers in Human Behavior, 49, pp. 567-575.

Alnatheer, M. Chan, T., Nelson, K. 2012. Understanding and measuring information security culture. PACIS 2012. Proceedings 144. Pacific Asia Conference on Information Systems (PACIS).

Ayton, D., Tsindos, T. & Berkovic, D. 2023. Qualitative Research: A practical guide for health and social care researchers and practitioners. Monash University.

Basforth, K. 2019. Culture Shift: A Practical Guide to Managing Organizational Culture. Bloomsbury Publishing.

Barman, S. 2001. Writing Information Security Policies. Sams. E-book. Accessed: 15.3.2025.

Carpenter, P. 2019. Transformational Security Awareness. Wiley. E-book. Accessed: 15.12.2024.

Carpenter, P. & Roer, K. 2022. The Security Culture Playbook. Wiley. E-book. Accessed: 16.12.2024

Chaudhary, S., Gkioulos, V., & Katsikas, S. 2022. Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity, 1.

CISA (The United States of America's Cybersecurity & Infrastructure Security Agency). s.a. URL: https://www.cisa.gov/uscert/ncas/tips/ST04-001. Accessed: 4.1.2022.

CISA (The United States of America's Cybersecurity & Infrastructure Security Agency). 2023. #StopRansomeware Guide. URL: https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf. Accessed: 4.1.2022.

Committee on National Security Systems. 2010. National Information Assurance (IA) Glossary. CNSS Instruction No. 4009. URL: https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf. Accessed 15.1.2022.

Costello, P. 2003. Action Research. Bloombury Publishing. E-book. Accessed: 1.5.2025.

Da Veiga, A. 2018. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Information and Computer Security, 26, 5.

Da Veiga, A. & Eloff, J. 2010. A framework and assessment instrument for information security culture. Computers & Security, 29, 2, pp. 196-207.

Da Veiga, A., Martins, N. & Eloff, J. s.a. Information security culture – validation of an assessment instrument. South African Business Review, 11, 1.

Death, D. 2023. Information Security Handbook. 2nd ed. Packt Publishing. Birmingham. E-book. Accessed: 14.12.2024.

Denison, D., Hooijberg, R., Lane, N. & Lief, C. 2012. Leading Culture Change in Global Organizations: Aligning Culture and Strategy. Jossey-Bass. San Francisco. E-book. Accessed: 14.12.2024.

Dhillon, G. 1997. Managing Information System Security. Macmillan. E-book. Accessed: 14.12.2024.

Egelman, S. & Peer, E. 2015. Scaling the Security Wall. Developing a Security Behavior Intentions Scale. (SeBIS). CHI 2015, Crossings, Seoul.

ENISA (European Union Agency For Networks and Information Security). 2017. ENISA overview of cybersecurity and related terminology. URL: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf. Accessed 8.8.2024.

ENISA (European Union Agency For Networks and Information Security). 2021. Raising Awareness of Cybersecurity. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Raising%20awareness%20of%20cybersecurity%20as%20a%20key%20element%20of%20NCSS.pdf. Accessed: 20.3.2025.

Eriksen, A-C., Petrič, G., & Roer, K. 2021. Security culture and credential sharing: How improved security culture reduces credential sharing in cybersecurity. https://www.knowbe4.com/hubfs/Security%20Culture%20and%20Credential%20Sharing.pdf. Accessed 7.4.2025.

Ferraro, G. & Briody, E. 2023. The Cultural Dimension of Global Business. 9th ed. Routledge. Oxon. E-book. Accessed: 13.3.2025.

Fertig, T. & Schutz, A. 2020. About the Measuring of Information Security Awareness: A Systematic Literature Review. Proceedings of the Hawaii International Conference on System Sciences, pp. 6518-6527.

Freund, J. & Jones, J. 2014. Measuring and Managing Information Risk. Butterworth-Heinemann. E-book. Accessed: 13.2.2025.

Gardner, B. & Thomas, V. 2014. Building an Information Security Awareness Program. Syngress. Waltham. E-book. Accessed: 13.2.2025.

Grubb, S. 2021. How Cybersecurity Really Works. No Strach Press. San Francisco. E-book. Accessed: 1.11.2024.

Hayden, L. 2015. People-Centric Security: Transforming Your Enterprise Security Culture. McGraw-Hill Education. E-book. Accessed: 3.11.2024.

IBM. 2024. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach. Accessed: 12.2.2024.

ISF (Information Security Forum). 2020. Human-Centred Security: Positively influencing security behaviour. URL: https://www.isflive.org/s/article/Human-Centred-Security-Positively-influencing-security-behaviour. Accessed: 3.3.2024.

ISF (Information Security Forum). 2024. From Promoting Awareness to Embedding Behaviours: Secure by choice, not by chance. URL: https://www.isflive.org/s/article/from-promoting-awareness-to-embedding-behaviours-secure-by-choice-not-by-chance. Accessed: 11.11.2024.

Kartchner, K., Bowen, B., & Johnson, J. 2023. Routledge Handbook of Strategic Culture. Routledge. Oxon. E-book. Accessed: 13.11.2024.

Laycock, A., Petrič, G. & Roer, K. 2019. The seven dimensions of security culture. URL: https://knowbe4.com/hubfs/CLTRe-The7DimensionsSecurityCulture-ResearchPaper.pdf?hsLang=en. Accessed: 3.3.2024.

Longitude., Financial Times. & Fujitsu Global. 2020. Fujitsu Research Study: Building a Cyber Smart Culture. 2020. URL: https://www.fujitsu.com/global/imagesgig5/Cyber_Smart_Culture_Fujitsu_Report.pdf. Accessed: 3.3.2024.

Martins, A. & Elofe, J. 2002. Information Security Culture. IFIP Advances in Information and Communication Technology, 86, pp. 203-214.

McNiff, J. 2013. Action research: principles and practice. 3rd ed. Taylor & Francis Group. Oxon. E-book. Accessed: 14.12.2024.

Merriam, S. & Tisdell, E. 2016. Qualitative Research: A Guide to Design and Implementation. 4th edition. Jossey-Bass. San Francisco. E-Book. Accessed: 4.5.2025.

Mertler, C. 2013. Action Research. Sage Publications. E-book. Accessed: 4.5.2025.

Moilanen, T., Ojasalo, K., & Ritalahti, J. 2022. Methods for Development Work. Books on Demand GmbH. Helsinki. E-book. Accessed: 4.5.2025.

Muhirwe, J. & White, N. 2016. Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. Issues in Information Systems, 17, 11, pp. 183-192.

NCSC (The United Kingdom's National Cyber Security Centre). 2022. What is cybersecurity. URL: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security. Accessed: 4.1.2022.

Orehek, S, Petrič, G. 2021. A systematic review of scales for measuring information security culture. Information and Computer Security, 29, 1.

Petrosyan, A. 2024. Annual number of cyberattacks worldwide from 2016 to 2023, by type (in millions). Statista. Accessed: 13.3.2025.

Quinn, R. & Rohrbaugh, J. 1983. A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. Management Science, 29, pp 363–377.

Rizal, M, & Setiawan, B. 2023. Information Security Awareness Literature Review: Focus Area for Measurement Instructions. 7th Information Systems International Conference.

Roer, K. 2015. Build a Security Culture. IT Governance Publishing. Cambridgeshire. E-book. Accessed: 10.11.2024.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. & Thapliyal, H. 2023. A systematic literature review of cybersecurity scales assessing information security awareness. Computer Science, 9, 3.

SANS Institute. 2024. Embedding a Strong Security Culture: SANS Institute 2024 Security Awareness Report. URL: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt18199203e8608f2f/SANS%20Security%20Awareness%20Report%202024.pdf?is=0f6ebef41e9d4fbe9c8717f2d88eb313d582cae972d5ea0b19eabb35f1adb07c. Accessed: 12.12.2024.

SANS Institute. 2021. Leading Cyber Security Change: Building a Security-Based Culture. Course material.

Sas, M., Hardyns, W., van Nunen, K., Reniers, G & Ponnet, K. 2020. Measuring the security culture in organizations a systematic overview of existing tools. Security Journal, 34, pp. 340-357.

Saunders, M. 2017. Doing research in business and management. Person Education. E-book. Accessed: 12.11.2024.

Schein, E. & Schein, P. 2016. Organizational Culture and Leadership. 5th ed. Wiley. E-book. Accessed: 13.11.2024.

Schlienger, T. & Teufel, S. 2003. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. 14th International Workshop on Database and Expert Systems Applications, Prague.

Schlienger, T. & Teufel, S. 2003. Tools supported management of information security culture. IFIP International Security Conference, Athens.

Schroeder, J. 2017. Advanced Persistent Training. Apress. Edinburgh. E-book. Accessed: 15.12.2024.

Seale, C. & Gobo, G., Gubrium, J. & Silverman, D. 2004. Qualitative Research Practice. Sage Publications. E-book. Accessed: 3.5.2025.

Siponen, M. 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8, 1.

Speed, T. 2011. Asset Protection through Security Awareness. Auerbach Publications. Parkway. E-book. Accessed: 15.12.2024.

Taylor, A., Alexander, D., Finch, A., & Sutton, D. 2013. Information Security Management Principles. 2nd ed. BCS Learning & Development Ltd. E-book. Accessed: 15.12.2024.

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

Vacca, J. 2013. Managing information security. 2nd edition. Syngress. Waltham. E-book. Accessed: 16.12.2024.

von Solms, R. & van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38, pp. 97-102.

Wang, Y., Qi, B., Zou, H., & Li, J. 2018. Framework of Raising Cyber Security Awareness. 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, pp. 865-869.

Willis, J. Edwards, C. 2014. Action Research: Models, Methods, and Examples. Emerald Publishing. E-book. Accessed: 5.5.2025.

Wilson, M. & Hash J. 2003. NIST (National Institute of Standards and Technology). Building an Information Technology Security Awareness and Training Program. URL: NIST SP 800-50, Building an Information Technology Security Awareness and Traini https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. Accessed: 12.11.2024.

World Economic Forum. 2024. Global Risks Report. Geneva. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Accessed: 13.3.2025.

World Economic Forum. 2025. Global Cybersecurity Outlook 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. Accessed: 4.5.2025.

Appendices

Appendix 1. Security Awareness Maturity Model levels (adapted from SANS Institute 2011)

Maturity level	**Non-existent**	**Compliance-focused**	**Promoting awareness and behavior change**	**Long-term sustainment and culture change**	**Strategic metrics framework**
Characteristics	• Security Awareness Program does not exist • Employees do not discuss or exhibit secure behaviors • Employees do not know or follow the organization's policies • Employees do not understand their impact on the security of the organization • Employees easily fall victim to attacks	• Program is designed to meet compliance or audit requirements • Training is limited to annual or ad hoc basis • Employees are unsure of the organization's policies • Employees are unsure about their role in protecting the organization's assets	• Program identifies the top human risks to the organization and behaviors that manage those risks • Training is continuous throughout the year and based on specific roles, departments or regions • Awareness material is communicated in a way that promotes positive behavior change • Employees understand their role in protecting the organization and follow policies	• The program has processes and resources in place • The program is (at a minimum) annually reviewed and updated • The program is an established part of the organizations culture • Employees have shared attitudes, perceptions and belief • Measures and reports on changes in behavior and culture	• The program has a robust metrics framework aligned with the organization's mission and business goals • Measures how behavior change is reducing risk and supporting the organizations strategic goals
Average of team size	• 1.14	• 1.49	• 1.81	• 2.62	• 4.18

Appendix 2. Overview of seven models to measure information security awareness (adapted from Rohan et al 2023)

Authors(s)	Objective	Nr of items	Scale
Muhirwe & White 2016	Measure cybersecurity events/ training programs impact cybersecurity awareness	27	5 point Likert scale
Arpaci & Sevinc 2022	Measure individuals' practices and perceptions regarding cybersecurity	25	5 point Likert scale
Bulgurcu, Cavusoglu & Benbasat 2010	Measure compliance and awareness	45	Mixed, including Likert scale
Chu & Chau 2014	Measure deviant behavior, specifically resource misuse and security carelessness	32	7 point Likert scale
Nævestad, Meyer & Honerud 2018	Measure organizational information security culture	24	5 point Likert scale
Vishwanath, Neo, Goh, Lee, Jhader, Ong & Chin 2020	Measure internet user cyber hygiene	18	5 point Likert scale
Gangire, Da Veiga & Herselman 2020	Measure employee information security behavior	75	5 point Likert scale

Appendix 3. Overview of Security Culture Survey (adapted from Roer 2015)

Nr	Dimension	Outline	Questions to ask
1	**Attitudes**	**The feelings and beliefs that employees have toward the security protocols and issues**	To what extent do employees care about security? Are they positive, neutral, or negative?
2	**Behaviors**	**The actions and activities of employees that have direct or indirect impact on the security of the organization.**	What are considered acceptable behaviors? What do employees see others doing?
3	**Cognition**	**Employees' understanding, knowledge and awareness of security issues and activities.**	What do employees know? How do they learn? How do they apply that knowledge?
4	**Communication**	**The quality of communication channels to discuss security related topics, promote a sense of belonging and provide support for security issues and incident reporting.**	How is security communicated throughout the organization? To what extent is the leadership involved? Is security considered a core value?
5	**Compliance**	**The knowledge of written security policies and the extent that employees follow them.**	How well do employees adhere to policies and procedures?
6	**Norms**	**The knowledge of and adherence to unwritten rules of conduct in the organization.**	To what extent are security-related beliefs, behaviors, and values embedded in the norms and unwritten rules of the organization?
7	**Responsibilities**	**How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.**	To what extent do employees feel empowered? To what extent will they help ensure that other employees follow the rules?

Appendix 4. Comparison of the six measurement tools adapted from Sas et al (2021)

	Analyzing Information Security Culture (Schlienger & Teufel, 2003)	**Self-assessment of nuclear security culture in facilities and activities (International Atomic Energy Agency, 2017)**	**A WINS international best practice guide for nuclear security culture (World Institute for Nuclear Security, 2011)**	**Information Security Culture (Martins and Eloff, 2002)**	**Understanding and measuring information security culture (Alnatheer et al, 2012)**	**Organizational Information Security Culture Assessment (AlHogail & Mirza, 2015)**
Domain	Information security	Physical security	Physical security	Information security	Information security	Information security
Key indicators	– Artifacts (e.g., behavior, technology, security handbooks) – Official values (i.e., the perception of the company on security) – True values (i.e., the individual attitude towards security)	– Beliefs and attitudes – Principles for guiding decisions and behavior – Leadership behavior – Management systems (e.g., processes, procedures, programs) – Personnel behavior	– Beliefs, principles and values – Characteristics (e.g., leadership, accountability, competency) – Documented expectations (e.g., security policy, responsibilities) and behaviors	– Organizational level: policy, benchmarking, risk analysis and budget – Group level: management and trust – Individual level: awareness and ethical – Change	– Top management involvement in information security – Information security policy enforcements – Information security training – Information security awareness – Information security ownerships	– Strategy (S) (e.g., policies, guidelines, best practices) – Technology (T) (e.g., hardware, software, services) – Organization (O) (e.g., beliefs, values, norms) – People (P) (e.g., behavior of employees) – Environment (E) (e.g., national culture, ethical conduct, legal systems)
Measurement approach	Questionnaire, interviews, document analysis, observations	Questionnaire, interviews, document analysis, observations	Questionnaire	Questionnaire	Questionnaire	Questionnaire

Type of questionnaire	Self-assessment	Self-assessment	Self-assessment	Self-assessment	Self-assessment	Self-assessment
Number of questions	42	25-35	52	45	19	79
Type of answers	Three options : true, false, I don't know	Likert scale: strongly disagree – strongly agree	Likert scale: strongly disagree – strongly agree	Likert scale: strongly disagree – strongly agree	Likert scale: strongly disagree – strongly agree	Likert scale: strongly disagree – strongly agree

Appendix 5. The Security Culture Diagnostic Survey (Hayden 2015, chapter 6)

Question	Answer options
1. What's valued most?	a) Stability and reliability are valued most by the organization. It is critical that everyone knows the rules and follows them. The organization cannot succeed if people are all doing things different ways without centralized visibility. b) Successfully meeting external requirements is valued most by the organization. The organization is under a lot of scrutiny. It cannot succeed if people fail audits or do not live up to the expectations of those watching. c) Adapting quickly and competing aggressively are valued most by the organization. Results are what matters. The organization cannot succeed if bureaucracy and red tape impair people's ability to be agile. d) People and a sense of community are valued most by the organization. Everyone is in it together. The organization cannot succeed unless people are given the opportunities and skills to succeed on their own.
2. How does the organization work?	a) The organization works on authority, policy, and standard ways of doing things. Organizational charts are formal and important. The organization is designed to ensure control and efficiency. b) The organization works on outside requirements and regular reviews. Audits are a central feature of life. The organization is designed to ensure everyone meets their obligations. c) The organization works on independent action and giving people decision authority. There's no one right way to do things. The organization is designed to ensure that the right things get done in the right situations. d) The organization works on teamwork and cooperation. It is a community. The organization is designed to ensure everyone is constantly learning, growing, and supporting one another.
3. What does security mean?	a) Security means policies, procedures, and standards, automated wherever possible using technology. When people talk about security they are talking about the infrastructures in place to protect the organization's information assets. b) Security means showing evidence of visibility and control, particularly to external parties. When people talk about security they are talking about passing an audit or meeting a regulatory requirement. c) Security means enabling the organization to adapt and compete, not hindering it or saying "no" to everything. When people talk about security they are talking about balancing risks and rewards. d) Security means awareness and shared responsibility. When people talk about security they are talking about the need for everyone to be an active participant in protecting the organization.

4. How is information managed and controlled?	a) Information is seen as a direct source of business value, accounted for, managed, and controlled like any other business asset. Formal rules and policies govern information use and control. b) Information is seen as a sensitive and protected resource, entrusted to the organization by others and subject to review and audit. Information use and control must always be documented and verified. c) Information is seen as a flexible tool that is the key to agility and adaptability in the organization's environment. Information must be available where and when it is needed by the business, with a minimum of restrictive control. d) Information is seen as the key to people's productivity, collaboration, and success. Information must be a shared resource, minimally restricted, and available throughout the community to empower people and make them more successful.
5. How are operations managed?	a) Operations are controlled and predictable, managed according to the same standards throughout the organization. b) Operations are visible and verifiable, managed and documented in order to support audits and outside reviews. c) Operations are agile and adaptable, managed with minimal bureaucracy and capable of fast adaptation and flexible execution to respond to changes in the environment. d) Operations are inclusive and supportive, allowing people to master new skills and responsibilities and to grow within the organization.
6. How is technology managed?	a) Technology is centrally managed. Standards and formal policies exist to ensure uniform performance internally. b) Technology is regularly reviewed. Audits and evaluations exist to ensure the organization meets its obligations to others. c) Technology is locally managed. Freedom exists to ensure innovation, adaptation, and results. d) Technology is accessible to everyone. Training and support exists to empower users and maximize productivity.
7. How are people managed?	a) People must conform to the needs of the organization. They must adhere to policies and standards of behavior. The success of the organization is built on everyone following the rules. b) People must demonstrate that they are doing things correctly. They must ensure the organization meets its obligations. The success of the

	organization is built on everyone regularly proving that they are doing things properly. c) People must take risks and make quick decisions. They must not wait for someone else to tell them what's best. The success of the organization is built on everyone experimenting and innovating in the face of change. d) People must work as a team and support one other. They must know that everyone is doing their part. The success of the organization is built on everyone learning and growing together.
8. How is risk managed?	a) Risk is best managed by getting rid of deviations in the way things are done. Increased visibility and control reduce uncertainty and negative outcomes. The point is to create a reliable standard. b) Risk is best managed by documentation and regular review. Frameworks and evaluations reduce uncertainty and negative outcomes. The point is to keep everyone on their toes. c) Risk is best managed by decentralizing authority. Negative outcomes are always balanced by potential opportunities. The point is to let those closest to the decision make the call. d) Risk is best managed by sharing information and knowledge. Education and support reduce uncertainty and negative outcomes. The point is to foster a sense of shared responsibility.
9. How is accountability achieved?	a) Accountability is stable and formalized. People know what to expect and what is expected of them. The same rewards and consequences are found throughout the organization. b) Accountability is enabled through review and audit. People know that they will be asked to justify their actions. Rewards and consequences are contingent upon external expectations and judgments. c) Accountability is results-driven. People know there are no excuses for failing. Rewards and consequences are a product of successful execution on the organization's business. d) Accountability is shared among the group. People know there are no rock stars or scapegoats. Rewards and consequences apply to everyone because everyone is a stakeholder in the organization.
10. How is performance evaluated?	a) Performance is evaluated against formal strategies and goals. Success criteria are unambiguous. b) Performance is evaluated against the organization's ability to meet external requirements. Audits define success.

	c) Performance is evaluated on the basis of specific decisions and outcomes. Business success is the primary criteria. d) Performance is evaluated by the organizational community. Success is defined through shared values, commitment, and mutual respect.

Appendix 6. First draft of the security culture survey for Organization X

Culture Dimension	Statements
Attitudes	I believe that security is a priority and a core value at Organization X I care about security and report security incidents even if I have caused it
Behaviors	I always wear my access card visibly in Organization X premises My colleagues would never share their passwords with anyone else
Cognition	Security related training at Organization X is relevant and helpful to me I know how to recognize a phishing attack I know the consequences a ransomware attack can cause Organization X I know how to report suspicious or abnormal security matters
Communication	We discuss information security in team meetings Our leaders lead by example and actively promote security matters
Norms	Security rules are helpful for the work that I do I seek for help when I have questions about security matters
Compliance	I know where to find security instructions that are relevant to me I believe that security instructions are clear at Organization X I understand and follow Organization X's information classification rules
Responsibilities	My individual behavior is important to secure and protect Organization X I am comfortable to address inadequate security behaviors

Appendix 7. First draft of security culture metrics

Metric name	What is measured?	How is it measured?	When is it measured?
Training completion	Percentage of employees that have completed annual training	Learning Management System (LMS)	Annually
Reinforcement training	Percentage of employees completing voluntary training	LMS	Monthly
Phishing click rate in simulations	Percentage of employees falling for simulation	Simulation program	Monthly
Phishing reporting	Percentage of employees reporting the simulation	Simulation program	Monthly
Phishing report offenders	Percentage of employees repeatedly falling victim in simulations	Simulation program	Monthly
MFA adoption	Percentage of employee using Multi Factor Authentication	System admin information	Monthly
Lost/stolen devices	Percentage of devices that were lost or stolen	Asset register	Monthly
Accidental Data Loss	Number of employees sharing sensitive information by accident	Data Leakage Prevention (DLP) system	Monthly
Time to detect an incident	Average time to detect an incident	Incident tracking process	Monthly
Number of incidents	Overall number of incidents	Incident tracking process	Monthly
Costs related to incidents	Overall costs	Incident tracking process	Monthly
Downtime related to incidents	Overall downtime or unavailability	Incident tracking process	Monthly
Compliance or audit violations	Number of violations or fines	Audit or compliance reports	Annually
Policy violations	Number of times employees violate security policies	Incident tracking process	Monthly