Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Marte Marjorie Søgnen

# Delay Discounting and its Impact on Information Security Decision-Making

Master's thesis in Information Security
Supervisor: Einar Arthur Snekkenes
Co-supervisor: Adam Szekeres

June 2023

NTNU
Norwegian University of
Science and Technology

Marte Marjorie Søgnen

# Delay Discounting and its Impact on Information Security Decision-Making

Master's thesis in Information Security
Supervisor: Einar Arthur Snekkenes
Co-supervisor: Adam Szekeres
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

# Abstract

The influence of information technology on organizations is steadily growing. Digitization has brought about enhanced business prospects and efficiency. However, with these advancements come ever-evolving risks, and organizations must protect themselves. Information security, a specialized field within information technology, focuses on mitigating risks and ensuring protection. Nevertheless, employees can seriously compromise information security unintentionally or intentionally. Delay discounting is the trade-off between immediate benefits and future rewards in human decision-making, with a preference for smaller immediate rewards over larger delayed rewards. This master's thesis investigates the gap between delay discounting and information security decision-making.

A mixed-methods research was used in order to address the research problem. First, a traditional literature review was conducted to investigate previous research, revealing that the area is highly unexplored. A questionnaire (N=135) was conducted in order to close the identified gap between information security and delay discounting. Finally, the collected data were combined to address the research questions fully.

The study uncovered an unexplored field where delay discounting and information security decision-making intersect. Findings indicate that framing security decisions as a potential loss of productivity or workflow could be advantageous. Surprisingly, the high discounting score challenges previous research and assumptions that people tend to postpone implementing security measures. The findings suggest that delay discounting is essential when investigating information security decision-making. However, attitudes are revealed to be the better predictor for actual security behavior.

By applying an exploratory sequential design, the thesis presents two modified questionnaires to measure delay discounting in an information security context and an instrument to measure security behavior. This field remains relatively unexplored, highlighting the significance of investigating the cognitive mechanisms that drive decision-making and real-world choices. The study makes a valuable contribution to advancing our understanding in this area.

# Sammendrag

Påvirkningen informasjonsteknologi har på organisasjoner er i stadig vekst. Digitalisering har ført til nye forretningsmuligheter og effektivitet. Imidlertid følger det med disse fremskrittene stadig skiftende risikoer som må beskyttes mot. Informasjonssikkerhet, som et spesialisert felt innenfor informasjonsteknologi, fokuserer på å redusere slike risikoer og sikre beskyttelse.

Ansatte kan utilsiktet eller med hensikt utgjøre en alvorlig trussel mot informasjonssikkerheten. Delay discounting er avveiningen mellom umiddelbare fordeler og fremtidige belønninger i menneskers beslutningsprosess, med en preferanse for mindre umiddelbare belønninger fremfor større forsinkede belønninger. Denne masteroppgaven har som mål å undersøke gapet mellom delay discounting og beslutninger innenfor informasjonssikkerhet.

En forskningsmetode bestående av et tradisjonelt litteraturstudie avdekket at området er lite utforsket. Samtidig besto forskningsmetoden av en spørreskjemaundersøkelse (N=135) som ble gjennomført for å tette det identifiserte gapet mellom informasjonssikkerhet og delay discounting. De innsamlede dataene ble kombinert for å besvare alle forskningsspørsmålene.

Studien avdekket et uutforsket område der delay discounting og beslutninger inngenfor informasjonssikkerhet overlapper hverandre. Resultatene antyder at det kan være gunstig å fremstille sikkerhetsbeslutninger som potensiell tap av produktivitet eller arbeidsflyt. Overraskende nok, utfordrer resultatene tidligere forskning og antagelser om at mennesker ofte utsetter implementeringen av sikkerhetstiltak. Resultatene antyder at delay discounting er en viktig faktor å undersøke når en studerer beslutninger innenfor informasjonssikkerhet. Imidlertid viser det seg at holdninger er en bedre prediktor for faktisk sikkerhetsadferd.

Oppgaven to nyutviklede spørreskjemaer for å måle delay discounting i en informasjonssikkerhetskontekst, i tillegg til et instrument for å måle sikkerhetsadferd. Det uutforskede feltet understreker betydningen av å undersøke de kognitive mekanismene som driver beslutningsprosesser og valg i den virkelige verden. Studien gir et verdifull bidrag til å utvide forståelse på dette området.

# Acknowledgements

I would like to thank my supervisor, Einar Arthur Snekkenes, for providing guidance, feedback, and support throughout my research. A special thank you to my co-supervisor, Adam Szekeres, for his continuous encouragement and always pushing me to accomplish my goals. I would also like to give a thank you to Espen Ringdal, Head of the computer security incident response team (CSIRT) in the Norwegian Customs, for expert knowledge and guidance during the survey design process.

I am extremely grateful to all participants who contributed to my research project. Thank you for taking your valuable time to answer my questionnaire.

Finally, I would like to give a special thank you to my closest friends and family for always believing in me.

# Contents

# Figures

# Tables

# Acronyms

**AIC** Akaike Information Criterion.

**LDG** Larger Delayed Gain.

**LDL** Larger Delayed Loss.

**LDR** Larger Delayed Reward.

**MCQ** 21-Item Monetary Choice Questionnaire.

**MCQ-G** 21-Item Monetary Choice Questionnaire Gain.

**MCQ-L** 21-Item Monetary Choice Questionnaire Loss.

**RQs** Research Questions.

**SA-6** Self-Report Measure of End-User Security Attitudes.

**SeBIS** Security Behavior Intentions Scale.

**SEG** Smaller Earlier Gain.

**SEL** Smaller Earlier Loss.

**SIR** Smaller Immediate Reward.

**TLR** Traditional Literature Review.

# Chapter 1

# Introduction

*The chapter presents an introduction to the master's thesis. The chapter presents the topic covered, relevant keywords, and the problem description. In addition, the chapter describes the research's justification, motivation, and benefits. Based on the problem description, the chapter introduces the Research Questions (RQs), followed by the planned contributions and the thesis structure.*

## 1.1 Topic covered by the project

Information technology has an increasing impact on organizations. Digitization has increased business opportunities and effectiveness; however, there are constantly new risks, and organizations must protect themselves. Information security is a field within information technology that aims to protect against such risks. Concerning information security, organizations tend to focus on technical measures rather than human aspects [1]. However, employees are the most vulnerable link when discussing organizational information security. The technological components of information technology systems can be secure at an acceptable level. However, if the people using the systems do not comply, the organizations are still vulnerable [2–4]. Employees in an organization use information technology systems every day. Therefore, the need for information security compliance is increasing as technology evolves. Several known factors contribute to decision-making. Attitudes, information technology knowledge, values, and personality are examples of such factors [5]. Delay discounting is directly linked to the human decision-making process and is the trade-off between immediate benefits and benefits in the future. When making decisions, humans tend to prefer smaller immediate rewards rather than larger delayed rewards [6]. Research shows that a possible future reward loses its value, even though the reward itself is larger [7–9].

## 1.2 Keywords

Information Security, Human-Computer Interaction, Human Factors, Security Management, Delay Discounting

## 1.3 Problem description

Employees are the greatest threat to information security, whether due to lack of knowledge or intentionally [10]. The fact that humans are a significant risk is well known, but why do humans struggle to comply with security measures and information technology systems? The information security focus is mainly on information technology [1]. Cyber threats are increasing in terms of sophistication and impact on organizations. Therefore, employees must implement security controls to protect organizational assets against cyber attacks. Employees are governed by measures such as policies, frameworks, and guidelines in order to protect against cyber attacks. The problem this thesis aims to answer is based on two assumptions regarding employees and information security. (1) Employees postpone implementing information security measures, and (2) employees do not fully comply with information security measures. The assumptions hold even though the employees know that the measures reduce the risk [11]. Delay discounting has implications for everyday decision-making because such decisions are complex [12]. To what extent does the concept of delay discounting affect decision-making regarding information security within Norwegian organizations, and how valuable is it to examine its influence on security-related choices in this context? The thesis aims to investigate and measure the impact of delay discounting on information security decision-making, specifically regarding information security compliance activities such as security controls.

## 1.4 Justification, motivation, and benefits

Organizations, governments, and other businesses collect, process, and store large amounts of information and data. In addition, the number of cyber attacks is increasing, and the methods are getting more sophisticated. Therefore, delay discounting is an important aspect when making decisions. A significant amount of research exists on delay discounting within economics and areas such as addiction, abuse, and gambling. However, more research must be done on delay discounting in an information security context.

In May 2019, the Health Services Executive in Ireland was subjected to a severe cyber attack using Conti ransomware. The attack resulted in losing access to IT and financial systems, severely disrupting healthcare services. The incident's root cause was an employee opening a malicious Microsoft Excel file [13]. In March 2020, SolarWinds was subjected to a cyber attack. SolarWinds is developing IT monitoring and management tools for more than 300.000 customers. The hack resulted in SolarWinds sending out an update with malicious code, which affected many customers [14, 15]. The exact method used has yet to be confirmed; however, it was discovered that several SolarWinds servers were protected with the password 'solarwinds123'. In addition, it was possible to gain unencrypted access to the SolarWinds update server as it was published online [16, 17].

Humans are the weakest link regarding information security and are often the cause of an incident[2–4, 10]. World Economic Forum states in its Global Risk Report that 95% of cyber security issues are due to human error [18]. In addition, Deloitte Malaysia published a press release stating that 91% of all cyber attacks begin with a phishing email [19]. Therefore, it is crucial to understand the individuals within an organization to ensure information security at an acceptable level. The research can provide several possible benefits to the field of information security. Understanding the individuals within the organization is essential in information security work, and the thesis can provide relevant information regarding employee behavior and the impact of delay discounting.

## 1.5 Research questions

Several factors influence human decision-making, and delay discounting is such a factor. When making decisions, humans need to make a trade-off between present and future benefits [7]. The following RQs is developed to answer the research problem:

**RQ1** What is the current state of research on delay discounting in information security, and what are the key findings based on the literature?

**RQ2** How well can a survey measuring delay discounting be modified to fit an information security context with similar qualities?

**RQ3** How does delay discounting impact individual decision-making in the context of information security in Norwegian organizations?

**RQ4** How useful is it to discuss delay discounting on how it affects security-related decisions in Norwegian organizations?

The information gathered from the questions in this section is useful when conducting the research problem in section 1.5. First, RQ1 aims to provide and examine previous information and research on delay discounting related to information security. Secondly, RQ2 aims to develop a new instrument to measure delay discounting in information security. The reason for developing a new measure is to tighten the gap between delay discounting and its relevance to information security. Finally, RQ3 and RQ4 aim to combine previous research with new findings to establish how delay discounting impacts information security decision-making and how useful it is to discuss the concept within the field.

## 1.6 Planned contributions

The contribution of this master's thesis is increased knowledge of information security decision-making on an individual level in terms of delay discounting. Additionally, the thesis contributes to the current research gap in the field. The results are based on qualitative data from a traditional literature review and quantitative data from a questionnaire. The thesis presents two modified versions of the 21-Item Monetary Choice Questionnaire by Kirby & Maraković [20] aiming to measure delay discounting better in an information security context. In addition, the thesis presents a questionnaire aiming to measure actual security behavior. The field is quite an unexplored area, and exploring the cognitive mechanisms underlying decision-making and real-world choices is essential; this study contributes in this direction.

## 1.7 Thesis structure

The thesis is structured as follows:

**Chapter 2** presents the general theoretical background to why the research is relevant.
**Chapter 3** defines the previous research and the results from the literature review needed to answer the research questions.
**Chapter 4** describes and justifies the research methodology needed to conduct the research.
**Chapter 5** presents the survey design process.
**Chapter 6** presents the results and data analysis methods.
**Chapter 7** discusses the results in a greater context and answers the research questions.
**Chapter 8** presents suggestions for future work.
**Chapter 9** summarizes the conducted research.

# Chapter 2

# Background

*This chapter provides a general overview of the problem description, explaining the challenges regarding information security decision-making. The chapter shows how delay discounting is related to information security, and it is divided into three sections: information security decision-making, the adaption of security measures, and delay discounting.*

## 2.1 Information security decision-making

Because of the increasing cyber threats in today's society, organizations need to protect their information assets. Today, policies and standards highly mandate protection mechanisms, and employees must comply with the protection mechanisms to ensure a sustainable security level. The information security policies and standards define how employees should act and behave to protect critical information [21]. Employees are a significant threat within an organization, whether unintentionally or intentionally, for example, when an employee innocently opens a malicious file attached to an email. The information security policies and standards are a response to such threats [5]. However, research shows that there is a difference between stated attitude and actual behavior [22–24]. Employees must perform at a satisfying level regarding information security, but even when the measure costs are limited, humans tend to refrain from using them [8]. Research shows that people find information security compliance activities stressful and have experienced difficulties fulfilling their jobs as a result of them, meaning that due to enhanced security requirements, employees reduce their information security compliance [21].

Several factors influence information security decision-making, such as information technology knowledge, personality, values, and attitude. In addition, organizational factors such as policies and standards can influence security decisions. Meaning that the organizational factors themselves are not the only decision-making factor when it comes to the information security compliance activities [5]. Herbert A. Simon [25] introduced the Theory of Bounded Rationality, which states that cognitive limitations, such as knowledge and capacity, influence decisions.

Therefore, employees may try to comply and make the correct decisions, but they need the knowledge or capacity to have acceptable behavior [5]. Another critical cognitive limitation is the ability to forecast the future [25], and individuals face significant uncertainty regarding information security decisions.

Compared to machines, humans could be more predictable. If different machines receive the same input and process the data similarly, the output is the same every time. However, when giving different humans the same input, the output is not the same because of the individual belief system [26]. Parsons et al. [27] state that because the field of information security is complex, the decision-making process concerning individual knowledge, attitude, and behavior is complex. One employee can have an appropriate attitude, but more knowledge regarding information security results in better information security behavior.

## 2.2 The challenges of adapting security measures

As stated in Chapter 1, employees are a significant threat to organizations regarding information security [2–4, 18, 19]. However, despite implementing compliance activities, information security policies and standards, organizations are still troubled by information security policy violations such as password sharing by employees [28]. Because of the rapid evolution of technology, there is a rapid growth of information security threats resulting in a growth of security requirements. Research shows that employees tend to find these requirements constraining, disruptive, and time-consuming [29]. Box & Pottas [30] shows that healthcare workers "*are aware of the importance of being security compliant but do not practice it*". Password sharing amongst healthcare workers was significant, even though they knew the importance of security compliance. These findings reflect that employees potentially find information security compliance activities as an overload when they are to be done in addition to everyday work tasks [28].

Technical security demands are intended to help employees comply with the information security requirements. However, the demands impose several restrictions on the employees using the systems. For example, some technical security demands include Internet access limitations, access control mechanisms, or file encryption. In addition, such security measures require employees to use their time on measures rather than performing their tasks, resulting in reducing employees' work productivity [21].

## 2.3 Delay discounting

Delay discounting is "*the process wherein rewards lose value as a function of their delayed receipt*" [9]. Recently, studies have focused on how much decision-making is influenced by the rate at which rewards are given out. Intertemporal choices initially attracted the attention of economists, and in order to explain these decisions, a theoretical model known as the Discounted Utility Model was developed. The model assumes that the discount rate must be applied to every option; however, the majority of investigations have been unable to produce a reliable measurement [31]. According to Loewenstein [32], delay discounting is the cognitive process that enables a person to assess the values of immediate and delayed consumption of a specific reward. According to the methodology behind delay discounting, subjective values are automatically assigned to both the immediate and delayed value whenever a decision is taken. Therefore, people who minimize the importance of delayed consequences frequently act in a way that prioritizes immediate consequences above larger, delayed ones. Such factors can help explain why people's reasoning does not always support the option that seems to be the most advantageous.

Furthermore, research on decision-making has involved integrations to various fields of knowledge. For example, studies within the domains of psychology and economics explore how gains, losses, and probabilities associated with time are integrated to generate decisions and influence choices. Delay discounting has emphasized the significance of the immediacy of reward release in the decision-making process [8, 11, 31].

# Chapter 3

# Related work

*The chapter presents previous research on delay discounting. The chapter results from the literature review described in Chapter 4, contributing to RQ1. A significant amount of research exists on delay discounting within economics and areas such as addiction, abuse, and gambling. However, few studies address the relationship between delay discounting and information security.*

## 3.1 Delay discounting and information security

Acquisti [22] present delay discounting as a factor that possibly infers with the rational decision choice when humans make privacy decisions. Even when users have all information and knowledge needed to make the correct security decision, individuals are likely to avoid the security step when performing tasks due to the current needs being in the future, which means there is a gap between security attitude and actual security behavior.

Acquisti & Grossklags [23] published a paper in 2005 examining how individuals decide whether to disclose personal information during online purchases. The research specifically examines the role of discounting in these decisions and the impact of privacy concerns on discounting. The authors conducted a series of experiments in which participants got asked whether to provide personal information in exchange for different rewards. The benefits granted, the quantity of personal information asked, and the perceived reliability of the requestor all varied among the tests. Acquisti & Grossklags discovered that participants tended to discount the value of their personal information when making these decisions. As a result, they were willing to share more personal information in exchange for smaller rewards than larger ones. The research showed that participants less concerned about privacy experienced this effect more intensely. However, the authors also found that privacy concerns might outweigh the benefit of discounting. When participants were made aware of potential privacy risks associated with sharing their personal information, they were less likely to do so, even when offered larger rewards. Overall, the results indicate that the perceived value of rewards and privacy concerns influences people's decisions about disclosing personal information.

Grossklags & Barradale [24] observed in their study that efficient privacy and security decision-making typically entails an economic evaluation of choices that could have long-term positive or negative effects. The researchers pointed out that investing in additional security measures now may prevent an attack or protect a person against an intrusion attempt in the future as such an effect. In the paper, they experimented on time preferences that shed light on the issue of whether people from different socioeconomic status categories exhibit the same level of impatience when making decisions. The findings from Grossklags & Barradale contribute toward explaining the gap between information security attitudes and security behaviors. People may be able to express their security concerns, but the likelihood that they will take action to protect themselves may vary depending on their level of impatience.

Mishra and Lalumière [33] published an article in the Journal of Behavioral Decision Making that investigated associations between delay discounting and risk-related behaviors, traits, and attitudes. The research revealed that some individuals have a high level of risk acceptance in some areas but a low level of risk acceptance in other areas. Meaning that the individual delay discounting rate can variate when investigating different contexts. The paper also states that uncertainty is essential when discussing delay discounting. If the future is uncertain, people prefer smaller, immediate rewards. On the other hand, if the present is uncertain, people prefer the future reward. In addition, there are individual differences that impact the delay discounting rate.

Frik et al. [34] identify time's utility in implementing information security controls as a challenge. Implementing measures takes time and results in interruption of workflow in order to protect against a future possible danger. When costs and benefits happen at different times, people tend to procrastinate on the costs and expedite the benefits. The authors performed a study where the participants were to choose between updating a system now or after a preferred delay in terms of time. Several respondents chose to update the system with delay, and the research also showed that one-third of the sample wanted to choose a time where it was more convenient for them. Vaniea & Rashidi [35] found in their research on tales of software updates that humans turned off automatic updates on their systems because the timing of the update was inconvenient. The effect of experience with rare probability events, such as cyber-attacks, on updating decisions was examined in a behavioral economics experiment by Rajivan et al. [36]. The findings demonstrated that after experiencing an attack, people frequently underestimate the risk of future ones, which results in poor security choices. Although updating right away is the best course of action, most experiment participants either delayed or skipped updating.

Based on the previous research, delay discounting strengthens the assumptions provided in section 1.5, and the work is relevant to answer the RQs.

## 3.2 Calculation of delay discounting

Delay discounting measures the degree of decreasing a value as a consequence of a delay to its delivery [37]. The rate of delay discounting $k$ is the slope between immediate and delayed rewards [9]. A greater $k$ indicates greater impulsivity. Traditionally, an exponential function was used to present the value of the delayed reinforcement: $V = Ae^{-kD}$. Where $A$ is the larger, delayed amount, $k$ is the scaling constant of the individual delay discounting, and $D$ is the delay associated with $A$. However, research has shown that a hyperbolic function is more efficient when characterizing the patterns of delay discounting [20, 37]. Mazur [38] presents a hyperbolic equation which is presented in Equation 3.1.

$$V = \frac{A}{1 + kD} \tag{3.1}$$

The function shows that the greater the discounting, the greater the $k$ value. To illustrate $k$, equation 3.1 can be rearranged as follows:

$$V(1 + kD) = A \tag{3.2}$$

$$1 + kD = \frac{A}{V} \tag{3.3}$$

$$kD = \frac{A}{V} - 1 \tag{3.4}$$

$$k = \frac{\frac{A}{V} - 1}{D} \tag{3.5}$$

Equation 3.5 presents the relationship that $k$ have with $A$, $V$, and $D$. Where $A$ is the larger, delayed reward size; V is the smaller, immediate reward size; and $D$ is the delay associated with the larger, delayed reward size $A$ [9, 20]. Research shows that a greater discounting rate is associated with high impulsivity [37].

# Chapter 4

# Methodology

*This chapter presents the thesis methodology. The methodology is the chosen strategy to acquire knowledge regarding the problem description and how to answer the research questions. Firstly, the chapter elaborates on the importance of methodology and types of data collection methods. Secondly, the applied research methodology is presented and justified along with the research design. It is important to determine a suitable research design based on the problem description in order to answer the research questions provided in Section 1.5. In addition, the data collection methods needed are elaborated on in this chapter. Lastly, ethical and legal considerations are presented.*

## 4.1 Considering methods

Figure 4.1 [39] illustrates that the methodology is the strategy used to answer the research problem. The figure also illustrates that the methodology should be based on the research problem and the specific RQs. The research questions presented in Chapter 1 are qualitative, meaning they aim to explore meaningful content in a larger context. However, when exploring delay discounting in an information security context, there is a limited amount of previous research, as shown in Chapter 3.

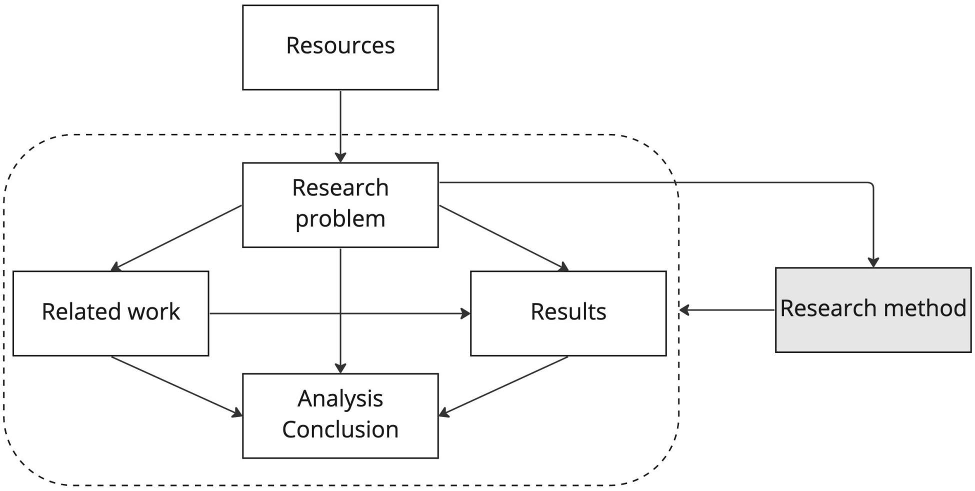


**Figure 4.1:** Methodology as a strategy [39]

The methodology must be based on the RQs. The RQs aims to explore a field with limited previous research, requiring many references when collecting data. Therefore, collecting data using survey research is more appropriate than interviews because of the high number of participants. However, the RQs can not be answered with the survey results alone, which means that the research problem requires both quantitative and qualitative data collection. Mixed-method research is suitable when researching such a problem because it collects, analyzes, and interprets quantitative and qualitative data. In addition, the quantitative and qualitative data collection results are to be integrated and discussed in a context. The most challenging part of mixed-method research is integrating the findings from the two collection methods [40]. However, Bryman [41] and Greene et al. [42] present several positive aspects of using mixed-method research, such as completeness and complimentary. By using both qualitative and quantitative data, the problem can be addressed more thoroughly and completely. In addition, qualitative data can compensate for possible weaknesses in quantitative data and vice versa. Using previous research on delay discounting, in combination with quantitative data done in an information security context, can improve the quality of the quantitative findings.

### 4.1.1 Qualitative and quantitative research

Two categories can be distinguished; primary data and secondary data. Primary data refers to information collected by the researcher, while secondary data is information collected that already exists [1]. Data collection is essential to answer the research questions. The methods one can use when collecting data can be categorized as qualitative or quantitative methods [40]. Data collected that satisfies the qualitative method is text-based, while quantitative data are presented as numbers or statistics. Qualitative data are helpful when the focus is on a complex phenomenon in the world. Qualitative research uses several forms of data to answer a research problem, for instance, observations, interviews, or written documents. When conducting quantitative research, the sense of the phenomena is created through measurements and numbers. The measurements and numbers are summarized using statistical approaches to find meaning in the numerical data. A survey is an example of a quantitative research approach [40]. The research questions require the collection of both qualitative and quantitative data. The qualitative data to be used is the secondary data collected from a literature review aiming to answer RQ1. The quantitative data is the primary data that a questionnaire will collect. The qualitative data will be integrated and discussed with the quantitative data to answer RQ1, RQ3, and RQ4.

### 4.1.2 Choice of methodology

The methodology to be used in order to answer the research questions consist of two approaches for collecting data. Figure 4.2 presents several mixed-methods research designs.

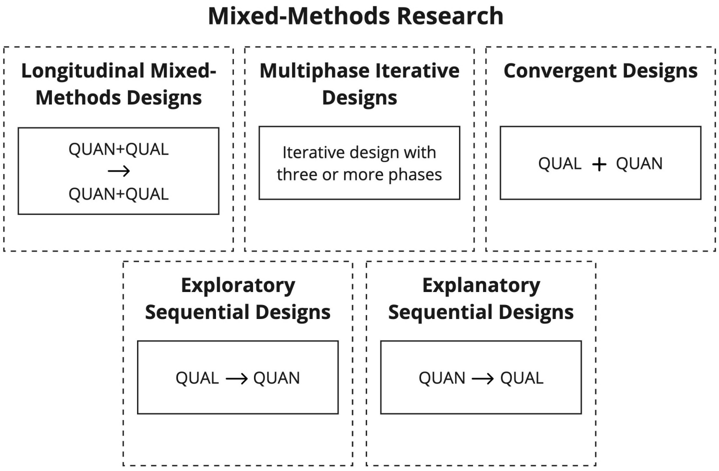

Mixed-Methods Research
Longitudinal Mixed-Methods Designs
QUAN+QUAL → QUAN+QUAL
Multiphase Iterative Designs
Iterative design with three or more phases
Convergent Designs
QUAL + QUAN
Exploratory Sequential Designs
QUAL → QUAN
Explanatory Sequential Designs
QUAN → QUAL

**Figure 4.2:** Mixed-Methods Research Designs according to Leedy & Ormrod [40]

[1] From Oxford Learners Dictionaries

A longitudinal mixed-methods design requires a long period because it collects data from the same sample group on two or more occasions, for example, months or years. Multiphase iterative designs require more than three phases; additionally, qualitative and quantitative data are collected in an iterative process, meaning that the researcher goes back and forth between qualitative and quantitative methods. A convergent design uses both qualitative and quantitative data, but the two methods are equally weighted in such a design. Experimental sequential designs and explanatory sequential designs are similar, and the main difference is which data collection method comes first [40]. The research questions require a qualitative approach before the quantitative data can be collected to gain knowledge regarding the research problem. Therefore, an exploratory sequential design is suitable for mixed-method research. The exploratory sequential design consists of two main phases. In the first phase, a qualitative method is used to achieve general knowledge of the phenomena, and the results contribute towards developing the research questions and the second phase. The second phase consists of the qualitative data collection methods [40].

Figure 4.3 illustrates the data collection process and the exploratory sequential design, which includes a Traditional Literature Review for the qualitative research and survey research for the quantitative research. Lastly, the findings from the first two phases will be integrated to answer RQ3 in the third phase.

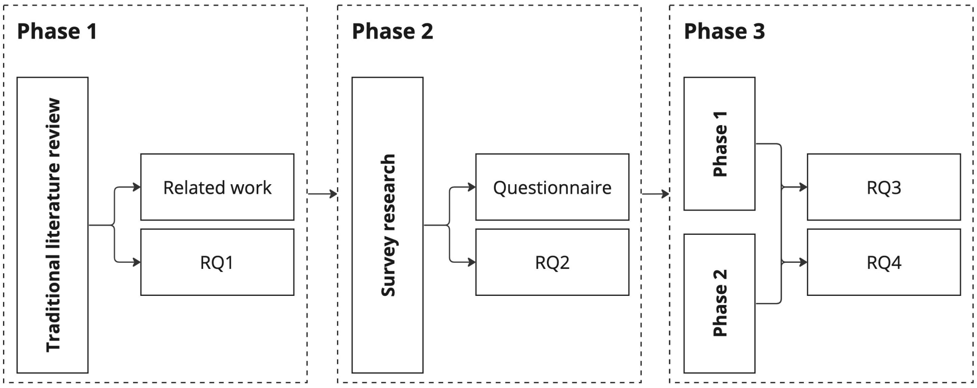


**Figure 4.3:** Data collection process

The findings from the Traditional Literature Review in Phase 1 are presented in Chapter 3 and aims to answer RQ1. The results are used in the survey research to develop the questionnaire, which aims to answer RQ2. The TLR was conducted to gather information and knowledge about the research problem. To develop a satisfying questionnaire in the second phase, gaining in-depth knowledge of the research problem is essential. Lastly, the data collected from the first and second phases are being reviewed together to answer RQ3 and RQ4.

## 4.2 Applied research methodology

This section presents the applied research methodology based on Figure 4.3. In addition, the section presents how the Traditional Literature Review and survey research were executed.

### 4.2.1 Traditional literature review

A Traditional Literature Review (TLR) was conducted to summarize previous research and knowledge on delay discounting and information security aspects. There are several types of TLRs that exist. Jesson et al. [43] present them as (1) a traditional review, (2) a conceptual review, (3) a state-of-the-art review, (4) an expert review, and (5) a scoping review. Because the RQs aims to provide new knowledge on delay discounting in an information security context, a scoping review was selected as the appropriate approach. The small amount of previous research on the topic also contributed to selecting a scoping review.

#### Scoping review

According to Jesson et al. [43], a scoping review aims to review the previous knowledge and information on the topic and identify the gaps. A scoping review is helpful when the field of study is emerging because it helps to refine the RQs and problem description after the gaps are identified [43, 44]. Arksey & O'Malley [45] presents a methodological framework for conducting a scoping review used when performing the scoping review for this thesis. The framework consists of five stages (1) identifying the research question, (2) identifying relevant studies, (3) study selection, (4) charting the data, and (5) collecting, summarizing, and reporting the results.

The research questions were identified based on the researcher's curiosity about why employees often postpone or do not implement information security controls. Delay discounting was introduced because the thesis supervisor and co-supervisor previously had written a paper [7] on the subject. When searching for online sources, several search engines and databases were used, as presented in Table 4.1. The scoping review started in October 2022 during the NTNU course *IMT4205 Research Project Planning* and was carried out until April 2023.

| **Search engines** |
|---|
| ACM Digital Library |
| IEEE Xplore |
| Google Scholar |
| Oria |

**Table 4.1:** Search engines used in the literature review

To identify relevant studies, it was important to determine relevant keywords to scope the results. A Boolean search string was used to identify previous studies containing delay discounting and information security. The keywords could be mentioned throughout the paper, and the search was not excluded to in-title only. Table 4.2 shows the results for each search engine on the Boolean search string "*delay discounting*" *AND* "*information security*".

| **Search engine** | **Results** |
|---|---|
| ACM Digital Library | 0 |
| IEEE Xplore | 0 |
| Google Scholar | 56 |
| Oria | 0 |

**Table 4.2:** Results: "delay discounting" AND "information security"

First, all 56 results were looked at, and a more detailed keyword search in each paper was performed. Most papers only referred to 'delay discounting' or 'information security' in the bibliography, and they got excluded. Papers that only mentioned 'delay discounting' in a brief sentence also got excluded. When screening the papers, the terms *time preference* and *hyperbolic discounting* were identified as synonyms to delay discounting. Due to the small number of papers, *delay*, *discounting*, and *hyperbolic* were used as synonyms when searching for delay discounting in each paper, and the keywords *security*, *cyber*, and *privacy* were used as synonyms for information security.

| | **Initial results** | **Potentially in scope** | **In scope** |
|---|---|---|---|
| Google Scholar | 56 | 3 | 1 |

**Table 4.3:** Relevant papers after screening process from Boolean search string 1

After the screening, three papers were seen as potential literature relevant to the RQs and the problem description. The findings are presented in Table 4.3. All three papers were read, but unfortunately, two of the papers were only available as a preview, resulting in only one paper being in scope after reading. Because the first Boolean search string only resulted in one paper in scope, another search string was created using *hyperbolic discounting*. The results are presented in Table 4.4.

| **Search engine** | **Results** |
|---|---|
| ACM Digital Library | 2 |
| IEEE Xplore | 8 |
| Google Scholar | 446 |
| Oria | 1 |

**Table 4.4:** Results: "hyperbolic discounting" AND "information security"

The same criteria as for the Boolean search string 1 were used in the screening process of the articles. Table 4.5 presents the results, which reveal four in-scope papers.

| | **Initial results** | **Potentially in scope** | **In scope** |
|---|---|---|---|
| ACM Digital Library | 2 | 2 | 1 |
| IEEE Xplore | 8 | 2 | 1 |
| Google Scholar | 446 | 11 | 2 |
| Oria | 1 | 0 | 0 |

**Table 4.5:** Relevant papers after screening process from Boolean search string 2

However, the result from ACM Digital Library and one of the papers from Google Scholar were duplicates and previously found using the Boolean search string 1. Therefore, two papers were relevant as the IEEE Xplore paper also were found in the Google Scholar search. Nevertheless, some potentially in-scope articles were used in Chapter 2.

In addition to the three papers discovered using Boolean search strings, a keyword search using 'delay discounting' was conducted in the Journal of Cybersecurity. The search resulted in one paper relevant to the scope, and two additional papers were identified from the paper's reference list. Lastly, the final paper was found using 'delay discounting' AND 'attitudes' in a Google Scholar search to find general knowledge presented in Chapter 2. All papers were charted and summarized after the papers were studied as part of the third stage from Arksey & O'Malley's [45] framework. The chart is presented in Table 4.6, and the summarizing and the reporting of the results are presented in Chapter 3.

| # | Author(s) | Year of publication | Keyword | Methodology | Important results |
|---|---|---|---|---|---|
| 1. | Acquisti, A | 2004 | ("hyperbolic discounting" AND "information security") | N/A | The paper suggests that delay discounting can impact rational decision-making process when it comes to privacy decisions.<br>Even when individuals have all information necessary, they may avoid taking security steps because their current needs are focused on the present rather than the future. Identifies a gap between human security attitude and behavior. |
| 2. | Acquisti, A; Grossklags, J. | 2005 | ("hyperbolic discounting" AND "information security") | Experimental methodology | The paper aims to identify how people decide whether to disclose personal information during online purchases. The authors conducted experiments and found that individuals tend to value their personal information less when making decisions and that privacy concerns can outweigh the benefit of discounting. People's decisions are influenced by both the perceived value of rewards and their privacy concerns. |
| 3. | Grossklags, J; Barradale, N J. | 2014 | ("hyperbolic discounting" AND "information security") | Experimental methodology | The research found that efficient privacy and security decision-making requires an economic evaluation of choices with long-term effects.<br>They conducted an experiment on time preferences that helps explain why people's security behaviors may not match their preferences.<br>People's level of impatience may influence their likelihood of taking action to protect themselves. |
| 4. | Mishra, S; Lalumière, M L. | 2017 | ("delay discounting" AND "attitudes") | Literature review, meta-analysis | The paper discusses that people's level of risk acceptance can vary depending on the context and that uncertainty plays an important role in delay discounting. The paper also notes that individual differences can impact the delay discounting rate |
| 5. | Frik, A; Egleman, S; Harbach, M; Malkin, N; Peer, E. | 2018 | Found in reference list from paper #7. | Experimental methodology | The research found that implementing information security measures is challenging due to the time required and potential workflow interruption.<br>People tend to procrastinate on costs and prioritize immediate benefits, which can lead to delayed system updates. In their study, participants were given a choice to update a system immediately or with a delay, and some preferred to delay updates until a more convenient time. |
| 6. | Vaniea, K; Rashidi, Y. | 2016 | Found in reference list from paper #7. | Survey research | The researchers identified that humans turned off automatic updates on their systems because the timing of the update was inconvenient. |
| 7. | Rajivan, P; Aharonov-Majar, E; Gonzalez, C. | 2020 | "delay discounting" in Journal of Cybersecurity | Experimental methodology | Studies the impact of rare cyber attacks experience on updating decisions.<br>The researchers found that people often underestimate future attack risks after experiencing one, leading to poor security choices. Despite immediate updating being optimal, most participants in the experiment delayed or skipped it. |

**Table 4.6:** Charting of Traditional Literature Review (Scoping review)

### 4.2.2 Questionnaire

Survey research is the chosen methodology to collect quantitative data. Survey research collects data from a sample of individuals, and the aim is that the sample is representative of a larger population. Survey research is typically approached with either a face-to-face interview, a telephone interview, or a questionnaire. A questionnaire can be distributed to many people, and the approach saves the researcher time compared to face-to-face and telephone interviews. Because the research questions require a large amount of data in a short time, a questionnaire is appropriate to answer the RQs. Another positive effect of using questionnaires is the anonymity aspect. Participants might be more willing to complete the survey when total anonymity is an option. However, there are some negative aspects to consider. Questionnaires often tend to have a low return rate. Meaning the majority of the people that receive the questionnaire by email do not respond. If the number of participants is not large enough, it might not be a satisfying sample to represent a larger population [39, 40].

Sufficient sample size is dependent on the aim of the research project. Increasing the sample size leads to more precise and representative findings, whereas smaller sample sizes can introduce higher levels of variability and uncertainty. Several estimates of sufficient sample sizes are based on the data analysis techniques to be used. For example, techniques such as t-tests require at least 30 responses for each variable. However, for regression analysis, approximately 50 respondents are seen as sufficient. Other researchers suggest using the formula $N > 50 + 8m$ for a multiple regression analysis, where $m$ is the number of independent variables. For example, if five independent variables are to be used, a sample size of 90 is sufficient. If a stepwise regression model is to be used, it is recommended that the sample size is higher[46, 47].

Several measurements exist that aim to calculate and investigate delay discounting, for example, experimental designs where participants are observed or physically asked to choose between two options [31, 48, 49]. However, it was impossible to conduct physical observations or such experiments considering the limited time. Therefore, a questionnaire-based delay discounting measurement, the 21-Item Monetary Choice Questionnaire (MCQ) by Kirby & Maraković, was to be used as a guide when developing the questionnaire for this thesis. Chapter 5 presents the survey design process.

#### Target group and sample size

The questionnaire was sent out to three target organizations and further distributed to other employees working in other organizations using convenience sampling. Convenience sampling is a non-probability sampling method used because it is convenient [40, 50]. However, snowball sampling was also used, which involves asking the recruited participants to distribute the questionnaire to other individuals as well [40]. The development process of the questionnaire is presented in Chapter 5, and the finalized survey can be found in Appendix A and B.

The target audience was aiming to be people working in Norwegian organizations. Therefore, the invitation was standardized, so all target organizations were sent the same email. The critical information provided in the invitation was also included in the introduction part of the questionnaire. The reason for doing this was that people were free to distribute the link to other employees, which required the introduction text to include all necessary information. The survey invitation can be found in Appendix C.

The questionnaire was distributed via email, and approximately 400 employees received the survey invitation, which resulted in a total of $N = 135$ total respondents. The survey software used was Nettskjema because it can easily be accessed with an NTNU account. Additionally, one can set anonymity as a beneficial requirement. Participants can access the questionnaire with a link; it does not require them to sign in or give any personal information. All respondents answered all questions as it was set as a requirement in Nettskjema, meaning that all responses are represented in the results.

### Data analysis tools

The primary data analysis tool used to analyze the data was Rstudio. Additionally, the data set from Nettskjema was downloaded to Microsoft Excel and structured before the data was converted to a CSV file. Additionally, an automatic scoring tool by Kaplan et al. [9] was used to calculate the k-values and consistencies. The scoring tool is a Microsoft Excel sheet that takes the instances of 0s and 1s and outputs calculations such as the overall and geometric k-value, k-values for small, medium, and large rewards, and the consistency score. Each participant's k-value is estimated from their overall response patterns. If there are irregular shifts between the respondents' preference for immediate and delayed rewards, the two questions most proportional to a respondent's responses are chosen. For example, if a participant chooses only delayed or immediate rewards, the k-value equals the endpoints (0.0007 or 0.1310). The scoring tool provides these calculations immediately after inserting the respondents' answers [9].

## 4.3 Ethical and legal considerations

It is essential to consider research's ethical and legal aspects, especially when humans are involved. The ethical considerations to be taken are usually protection from harm, voluntary and informed participation, honesty, and the right to privacy. Researchers must not harm the participants involved, either physically or psychologically. Examples of such harm can be loss of self-esteem or embarrassment. As a researcher, taking care of the participants and showing respect is important.

Regarding voluntary and informed participation, the participants must give informed consent. When conducting a survey, participation should be strictly voluntary. The right to privacy must be obtained, especially when the research involves human beings. The data presented should never reveal information that can be used to reveal a particular participant. Protecting the participant's privacy is crucial when considering the ethical and legal aspects of the research.

In addition, honesty is an important factor when doing research. The researcher must report the findings with honesty and correctness. If it is any form of personal bias, it should be acknowledged. Honesty is also referring to other work. When using secondary data, it is crucial to fully acknowledge the author(s) by citing it properly [40]. Because the questionnaire is entirely anonymous, applying Sikt [51] was unnecessary because no sensitive or personal information was to be collected. The thesis is written with all the ethical and legal considerations presented above. The information collected from the literature review is cited correctly. The survey distributed contains a consent form that fulfills the requirements. In addition, the statistical methods used to present the data comply with complete anonymity to the participants.

# Chapter 5

# Survey design

*This chapter presents the questionnaire development process that was used as a data collection method for answering the research questions. The chapter aims to present the entire process from start to finish, including the choices and challenges faced. The finalized survey is presented in Appendix A and B.*

## 5.1 Modifying the original MCQ

Table 5.1 presents the 21-Item Monetary Choice Questionnaire (MCQ) by Kirby & Maraković [20]. The MCQ consists of 21 choices: a smaller reward tonight or a larger reward in $x$ amount of days. The questionnaire is validated to calculate delay discounting, and in addition, it has a validated scoring tool [9]. In the original paper, Kirby & Maraković [20] distributed the finalized survey to college students. The main limitation of using the MCQ is the value of the rewards and scale. The value used in MCQ is currency (USD); however, for employees that have to implement information security measures, the value is not economical on an individual level. Implementing information security measures has some costs; it takes time and interrupts the workflow. Additionally, a dollar becomes less valuable depending on how much money a person has. If one only has 5 dollars, 40 dollars immediately might be needed. If one has 1000 dollars, getting the immediate reward is not as important, suggesting that the choice is highly subjective. The context is different from information security decisions when looking at the MCQ from this perspective. Therefore, a possible approach was using the MCQ and using previous research to elaborate on the limitations and the gap between the two different contexts. Another possible approach was to modify the MCQ to fit within an information security context.

When deciding the appropriate approach, it was essential to consider the quality of the thesis and the risk of the choices. In addition, the work was to be finished in six months. However, because of the lack of previous research in the field, it was decided to develop a new questionnaire aiming to calculate delay discounting in an information security context based on the 21-Item Monetary Choice Questionnaire by Kirby & Maraković [20].

| Order | Question | Hyperbolic parameter ($k$) |
|---|---|---|
| 4. | Would you prefer $34 tonight, or $35 in 43 days? | 0.0007 |
| 5. | Would you prefer $53 tonight, or $55 in 55 days? | 0.0007 |
| 7. | Would you prefer $83 tonight, or $85 in 35 days? | 0.0007 |
| 12. | Would you prefer $65 tonight, or $75 in 50 days? | 0.0031 |
| 20. | Would you prefer $27 tonight, or $30 in 35 days? | 0.0032 |
| 9. | Would you prefer $48 tonight, or $55 in 45 days? | 0.0032 |
| 16. | Would you prefer $47 tonight, or $60 in 50 days? | 0.0055 |
| 8. | Would you prefer $21 tonight, or $30 in 75 days? | 0.0057 |
| 3. | Would you prefer $67 tonight, or $85 in 35 days? | 0.0077 |
| 14. | Would you prefer $30 tonight, or $35 in 20 days? | 0.0083 |
| 18. | Would you prefer $50 tonight, or $80 in 70 days? | 0.0086 |
| 10. | Would you prefer $40 tonight, or $65 in 70 days? | 0.0089 |
| 2. | Would you prefer $40 tonight, or $55 in 25 days? | 0.0150 |
| 19. | Would you prefer $45 tonight, or $70 in 35 days? | 0.0159 |
| 11. | Would you prefer $25 tonight, or $35 in 25 days? | 0.0160 |
| 21. | Would you prefer $16 tonight, or $30 in 35 days? | 0.0250 |
| 6. | Would you prefer $32 tonight, or $55 in 20 days? | 0.0359 |
| 17. | Would you prefer $40 tonight, or $70 in 20 days? | 0.0375 |
| 13. | Would you prefer $24 tonight, or $55 in 10 days? | 0.1292 |
| 1. | Would you prefer $30 tonight, or $85 in 14 days? | 0.1310 |
| 5. | Would you prefer $15 tonight, or $35 in 10 days? | 0.1333 |

**Table 5.1:** 21-Item Monetary Choice Questionnaire (MCQ) by Kirby & Maraković [20]

The original MCQ approximates the k-value for each question for each participant. After 21 questions, the scoring mechanism better approximates the k-value. Because there already exists a scoring tool [9] for the original MCQ, it was essential to keep the modified version as similar to the original as possible. The reasoning behind keeping the scoring tool was due to the limited amount of time. Therefore, it was important to set a reference point or to identify the common underlying base for each modified question. Therefore, the same parameters from the MCQ were used, and the rewards and delays got adjusted based on the original discounting parameters. The process of adapting the MCQ is presented in Figure 5.1, conducted from February to mid-April 2023.

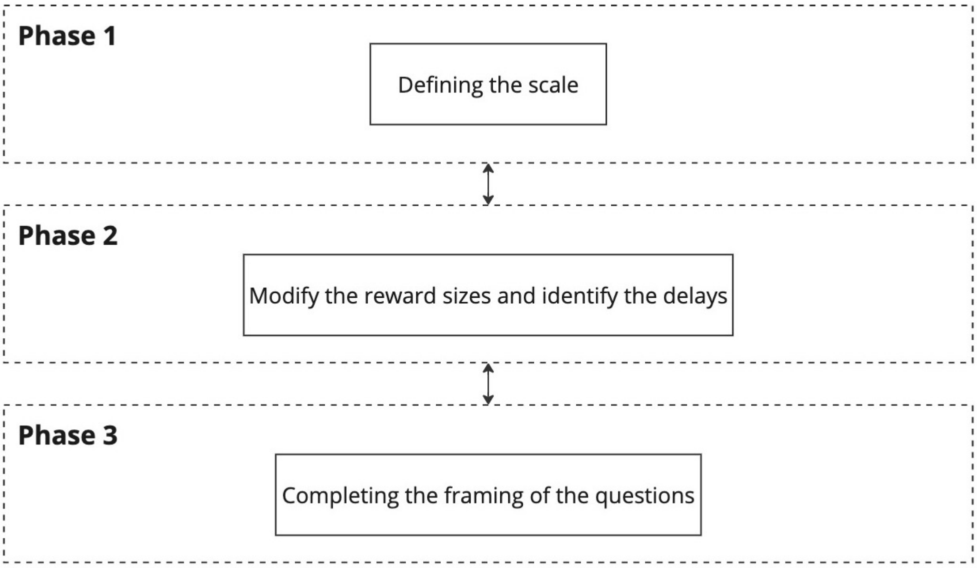

Phase 1
Defining the scale
Phase 2
Modify the reward sizes and identify the delays
Phase 3
Completing the framing of the questions

**Figure 5.1:** Adapting process of the MCQ

### 5.1.1 Phase 1 - Defining the scale

In order to adapt the original MCQ to an information security context while taking advantage of the automated scoring tool [9], the hyperbolic parameter associated with each of the 21 original questions presented in Table 5.1 was decided to be used without modifications. The reason for this decision was to ensure that the logic and calculations remained valid in the scoring tool when data were to be inserted. The MCQ was modified using an iterative approach. The first iteration identified the most appropriate scale of reward instead of $ amounts.

Research shows that several factors contribute towards the adaption of security measures [52–54]. The underlying common base for the information security measures was identified to be time. Implementing security measures takes time, and sometimes the controls require employees to change work patterns and lose productivity. However, some people value time in terms of information security controls as a loss, while others value it as a gain. Based on previous research [52–54], when employees face a choice of implementing a security control, they may not focus on the security gains but on the direct losses (e.g., interruptions and losses to productivity). In order to investigate this further, delay discounting was decided to measure both losses and gains.

| **Scaling options MCQ-L** |
|---|
| Would you spend X hours now, or spend Y hours in Z days? |
| Would you spend X minutes now, or spend Y minutes in Z days? |
| Would you spend X seconds now, or spend Y seconds in Z days? |

**Table 5.2:** The different scaling options for modified 21-Item Monetary Choice Questionnaire Loss

In the modified version for losses, 21-Item Monetary Choice Questionnaire Loss (MCQ-L), decided to use time as a scale due to previous research. Several options were discussed as Table 5.2 shows. It was essential to determine a scale that would fit all 21 questions. Because the scale was to be identical for all 21 questions, minutes were selected as the most appropriate scale in terms of losses because it was to fit the time spent on different types of security controls.

| **Scaling options MCQ-G** |
|---|
| Would you prefer protection from X potential attacks now, or protection from Y potential attacks in Z days? |
| Would you prefer protection from X security vulnerabilities now, or protection from Y security vulnerabilities in Z days? |
| Would you prefer protection from X cyber attacks now, or protection from Y cyber attacks in Z days? |
| Would you prefer protection from X potentially successful cyber attacks now, or protection from Y potentially successful cyber attacks in Z days? |
| Would you prefer protection from X potential attacks becoming successful now, or protection from Y potential attacks becoming successful in Z days? |
| Would you prefer protection from X potentially successful incidents now, or protection from Y potentially successful incidents in Z days? |

**Table 5.3:** The different scaling options for modified 21-Item Monetary Choice Questionnaire Gain

Finding an appropriate scale for security controls framed as gains, 21-Item Monetary Choice Questionnaire Gain (MCQ-G) was more challenging. Initially, the percent of incidents, number of attacks, number of people one would help, types of attacks, and number of protected accounts were elaborated. However, after discussing the different concepts with a security expert, other options came up, as presented in Table 5.3. Choosing the correct scale was important so respondents fully understood the questions; including non-information security people. Therefore, the questions in Table 5.3 were sent to several people working or studying in other fields. As a result, potentially successful cyber attacks were chosen as the appropriate scale in terms of the MCQ-G.

### 5.1.2 Phase 2 - Modify the reward sizes and identify the delays

The second iteration modified the reward sizes of the smaller immediate reward and the larger delay reward. The first modified version to be worked on was information security controls related to losses. For the reward sizes, the original MCQ divided the rewards for the large delayed rewards into three categories; small (S - $30-$35), medium (M - $55-$65), and large (L - $70-$85). The paper [20] described that seven non-identical delayed rewards were to be spread evenly across the seven ranges for each category. However, when analyzing the original 21-Item Monetary Choice Questionnaire displayed in Table 5.1 it was not done for the original MCQ. Table 5.4 presents the delayed reward sizes for each category, revealing that several of the delayed reward sizes are identical.

| **Reward sizes MCQ** | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Small (S - $30-$35)** | $35 | $35 | $30 | $35 | $35 | $30 | $30 |
| **Medium (M - $55-$65)** | $55 | $55 | $55 | $65 | $55 | $55 | $60 |
| **Large (L - $70-$85)** | $85 | $85 | $85 | $75 | $70 | $80 | $70 |

**Table 5.4:** Small, medium, and large delayed reward sizes from the original MCQ

For MCQ-L, a minimum and maximum point were set in terms of how long time it takes to implement security controls. The small category illustrates the time for simple security controls, such as typing in a password or pin, using two-factor authentication, or using a screen lock. The large category is meant to represent more time-consuming controls such as educational controls, courses, or reading through security policy requirements. The medium category represents the security controls in between, such as patching or updating a system. The purpose of the different timings is to reflect different types of security controls and how long it takes to implement them. The reward metric for MCQ-L was discussed with security experts and chosen to be 1-10 minutes for small, 11-59 minutes for medium, and 60-200 minutes for large reward sizes. Then, seven equally spread out values from each range were chosen as the Larger Delayed Loss (LDL). The Smaller Earlier Loss (SEL) was calculated using Equation 3.2 in Chapter 3 for each LDL, using the hyperbolic parameter from the original MCQ as previously elaborated on and presented in Table 5.1. When discussing the delays, it was decided that the same delay scale was to be used for MCQ-L. The argument behind keeping the same delays as the original MCQ was to keep the format as similar as possible to use the scoring tool. In addition, the general idea for MCQ-L was to investigate whether people postpone implementing security controls.

For MCQ-G, a minimum and maximum point were set regarding the number of potentially successful cyber attacks on an individual. The most challenging part of defining a metric was finding data on how to estimate the number of attacks on average at the individual level. Research [55–58] revealed that the amount of potential cyber-attacks depends on individual level depends on several factors, such as industry and role. It also depends on what each organization defines as a cyber attack. Based on several reports and articles, the reward metric for MCQ-G was chosen to be 2-10 attacks for small, 50-150 potential attacks for medium, and 500-1000 for large reward sizes. Then, the same process of defining seven equally spread out values from each range category was conducted and chosen as Larger Delayed Gain (LDG). Additionally, the Smaller Earlier Gain (SEG) was calculated using Equation 3.2. When discussing the delays, using the LDL metric made more sense to include the time spent implementing security controls to protect against potentially successful cyber attacks. Therefore, the delays were spread out evenly for 1-200 minutes. However, the same methodology was used for the delays in 21-Item Monetary Choice Questionnaire [20].

### 5.1.3 Phase 3 - Completing the framing of the questions

Until this point, the framing of the questions for both MCQ-L and MCQ-G were approximately the same as for the 21-Item Monetary Choice Questionnaire by Kirby & Maraković [20]. In the third phase, the modified questions were tested several times to check whether or not they made sense conceptually because, as of now, the focus had been on the questions making sense mathematically and logically. Based on the theory and research questions, the questions containing the new scale and delays needed to be meaningful.

| **Framing options MCQ-L** |
|---|
| Would you prefer to spend X minutes now (during work), or spend Y minutes in Z days? |
| Would you prefer to spend X minutes on setting up a security control now, or spend Y minutes in Z days? |
| Would you prefer to spend X minutes on implementing a security control now, or spend Y minutes on implementing a security control after Z days? |
| Would you prefer to spend X minutes on implementing a security control immediately, or spend Y minutes on implementing a security control after Z days? |

**Table 5.5:** The different framing options for modified MCQ-L

Table 5.5 presents several framing options for the MCQ-L. The options were discussed with supervisors, security experts, and non-information security people. It was important to frame the questions so that everyone would understand the meaning behind the question and keep it consistent and short. After several discussions, the framing was decided to be option number four: "*Would you prefer to spend X minutes on implementing a security control immediately, or spend Y minutes on implementing a security control after Z days?*" Adding the context of the questions contributes towards that the participants fully knew what was asked, and it made more sense to include the context *implementing a security control*.

Developing a suitable framing to the MCQ-G version was easier because the context was already used as the scale. From Table 5.3, "*Would you prefer protection from X potentially successful cyber attacks now, or protection from Y potentially* *successful cyber attacks in Z days?*" were chosen as the best scale. However, it was decided to keep the framing as similar to the MCQ-L as possible. Therefore, the finalized framing for MCQ-G was chosen to be "*Would you prefer protection from X potentially successful cyber attacks immediately, or protection from Y potentially successful cyber attacks after Z minutes?*"

Additionally, the introduction text for each questionnaire was developed similarly to the original MCQ. During this process, it was important to find a balance between describing the environment and ensuring the participants understood what to answer and not introducing a bias to the participants. For MCQ-L, it was important to clarify that they should pretend they were at work performing their daily tasks when answering the 21 questions. In addition, it was important to specify that loss of productivity or workflow would happen either way, so implementing a security control was to happen at work when choosing immediately or after a delay. After an iterative process with several modifications and updates, the final introduction text for MCQ-L was decided to be the following: "*Cybersecurity is a dynamic field, where the external environment changes constantly due to new threats and vulnerabilities. This means that there are several security controls that are implemented to keep security at a desired level. However, some security controls require a loss of productivity or workflow since they are to be done during work. For each of the next 21 choices, please indicate which option you would prefer: the smaller loss immediately, or the larger loss in/after the specified number of days. Please answer each question honestly and as if you actually make the choice when you are at work performing your daily tasks. Either if you select the smaller loss immediately, or the larger loss after the specified number of days, you will experience some loss of productivity or workflow.*"

For MCQ-G, the same requirements were set. However, since the framing described the context more fully, the introduction text was set to be shorter. The final introduction text for MCQ-G was decided to be the following: "*Cybersecurity is a dynamic field, where the external environment changes constantly due to new threats and vulnerabilities. This means that in order to maintain your desired/previous level of cybersecurity over time, you need to actively execute some actions on the systems you interact with. For each of the next 21 choices, please indicate which option you would prefer: the smaller benefit now or the larger benefit after the specified number of minutes.*"

## 5.2 Demographic information

The acquisition of demographic information is a crucial step in gaining a better understanding of the background characteristics of the sample. However, it is imperative to exercise caution when selecting demographic questions to include in a research questionnaire. Only questions that are pertinent to the research objectives should be included. The danger of respondent fatigue is real and should be avoided at all costs. Including too many questions in the survey can lead to fatigue, thus reducing the results' quality. Therefore, creating a brief questionnaire that provides valuable insights while minimizing the burden on the respondent [59, 60] was imperative. Age and gender are commonly used, and both demographics were included in the survey to analyze whether there is a difference between the groups. Because the questionnaire was sent out to different organizations, it was also decided to include current occupation as a demographic. Finally, the last demographic information to collect was whether the participant had managerial responsibilities. The organizational demographics are interesting when conducting the data analysis to check for a significant difference between the roles and responsibilities.

## 5.3 Stated attitudes and revealed behavior

During the survey design process, it was clear that to find any relationship between the three different MCQs and information security attitudes, and some attitude questions were also included. Faklaris et al. [61] published a paper revealing a six-item scale that can be used to assess human security attitudes. The authors did find a positive correlation with the Security Behavior Intentions Scale (SeBIS) by Egelman & Peer [62]. Therefore, to close the knowledge gap between delay discounting and security attitudes, the Self-Report Measure of End-User Security Attitudes (SA-6) was included in the finalized survey. Because research shows that there is a difference between stated and revealed attitudes [22–24], a self-developed questionnaire aiming to detect revealed preferences were included as well.

Developing a new questionnaire is challenging. Because of the limited time to test the questionnaire, it was important to also include the SA-6 as a countermeasure if the behavior questionnaire did not result in any important findings. Several approaches were discussed to measure revealed preferences; (1) participants were to estimate the number themselves regarding several security controls, (2) getting access logs on security behaviors from the organizations, (3) asking the respondents to check the evidence of the security behaviors on their systems, or (4) asking respondents regarding the first time they interacted with a set of security controls. Because the survey already included 69 questions in addition to the demographic questions, the behavior questionnaire needed not take as much time to complete. Therefore, a set of security controls was identified, and a six-point scale was identified for all security controls. The scale is presented in Table

5.6, and the security controls identified were two-step verification, screen lock, password manager, automatic updates, and verifying the sender's email address when receiving an email. The security controls needed to be familiar to the participants, so the chosen controls were very generic. The question text was framed as follows: "*Which of the following options best describe your past actions or future plans regarding the implementation of {control}?*"

| | | | | | |
|---|---|---|---|---|---|
| I have not implemented {control}. I am not planning to implement it ever. | I have not implemented {control}. I am planning to implement it later than this year. | I have not implemented {control}. I am planning to implement it this year. | I have implemented {control} less than a year ago. | I have implemented {control} between a year and 2 years ago. | I have implemented {control} more than 2 years ago. |

**Table 5.6:** Scale of behavior questionnaire

The introduction to the questionnaire was decided to be: "*There are several different security controls that exist. Please try to remember the first time you engaged in implementing the following security controls listed below. If you did not engage in the security control below, please state whether or not you intend to do so in the future. Please answer all of the questions as accurately and truthfully as you can.*" It was important to set the requirements and highlight that it was asked about the first time they engaged in the different security controls.

## 5.4 The translation process

Because the target group for the questionnaire was a few Norwegian organizations, it was seen as a limitation that the questionnaire was distributed in English. Because the survey research required a large sample, it was decided to translate the questionnaire so the participants could choose their preferred language. Another reason for translating the survey was the large number of questions, which could be a challenge if the survey language only was English. An English version of the survey was fully completed before the translation process started. Because most of the questions are similar, only changing a few numbers, the questionnaire was translated into Norwegian. Then a security expert, fluent in both languages, quality assured the translation. The translation was conducted using an iterative process based on feedback and suggestions.

In addition, it was decided that it was important that the participants fully understood the questions in terms of meaningfulness. Because the survey was sent out to Norwegian employees, the $ currency in the 21-Item Monetary Choice

Questionnaire by Kirby & Maraković [20] was translated into Norwegian krone (NOK). The currency translation was conducted on 11. April 2023, and 1 USD was equal to 10,58 NOK [63]. Because the Norwegian krone was low, the $ amount was multiplied by the exchange rate for all 21 immediate and 21 delayed rewards in the original MCQ.

## 5.5 Pilot study

A small pilot study was conducted before the survey was sent out to the target organizations. Because the survey consisted of modified and new questionnaires, it was essential to validate that the participants understood the meaning of each question. In addition, the pilot study was useful when approximating the time each participant would spend. The selection of $N = 10$ revealed no immediate challenges when conducting the survey. The approximate time was also set to 8-15 minutes based on the selection.

# Chapter 6

# Results and analysis

*This chapter presents the data analysis and results from the survey. The results from the literature review are presented in Chapter 3. The analysis aims to present the results to answer the research questions provided in Chapter 1. The chapter describes the data preparation process and the important findings from the descriptive and inferential analyses.*

## 6.1 Data preparation

The data was downloaded to a Microsoft Excel file and structured. All MCQ data was transferred into the automatic scoring tool by Kaplan et al.[9] to calculate the different k-values and consistencies. For the SA-6 questionnaire [61], Faklaris et al. present the scoring mechanism in a survey handout [64], which is set to be the average of items 1 through 6. The average scoring for each participant was performed in Microsoft Excel before the completed data set was transferred to Rstudio. The distributions of the individual SA-6 items are presented in Figure 6.2 and 6.3 while the average SA-6 score is presented in Figure 6.1. Figure 6.5 and 6.6 illustrates the distributions of the individual behavior scores, and the figures present skewed data, especially for two-step verification, screen lock, and automatic updates.

Several methods were tested to handle the skewed data; min-max normalization, log transformation, and z-score standardization. All correlations were calculated for the three types of methods; however, the results did not change significantly, and the histograms remained skewed. Another approach tested was removing the outliers; participants that answered the questionnaire below 480 seconds and above 10000 seconds. However, the results remained relatively the same. All re-scaling methods gave very similar results. Therefore, standardization was performed on the data set in order to perform the inferential analysis. In addition, a behavior score was calculated for all participants following the same procedure as for SA-6 [64]. Figure 6.4 presents the behavior score distribution. The behavior score turned out to be skewed. However, the skewness is better than the individual behaviors.

## 6.2 Descriptive analysis

Descriptive statistics aims to describe and understand the data. The techniques give short summaries of the data set and the sample [65]. This section presents the descriptive research done for the different questionnaires of the survey; demographics, MCQ, MCQ-L, MCQ-G, SA-6, and the behavior questionnaire.

### 6.2.1 Demographics and sample size

In total, 135 employees across the target organizations participated in the survey. Approximately 400 employees received the survey invitation by email, resulting in a response rate of 33.25%. Table 6.1 presents an overview of the demographic information. The sample includes individuals in all age ranges, where 50-59 (29.6%) and 40-49 (25.9%) were the largest. The sample includes both males (57.0%) and females (41.5%). The participants worked in different industries. The most common industries are IT and information security (53.3%) and healthcare (19.3%). The participants who stated other ($n = 10$) specified their occupation within sports, cleaning, public administration, education, and sales. Additionally, 28.1% of the participants had managerial responsibilities, while 69.9% had no managerial responsibilities. Males seem to be overrepresented based on the gender distribution in Norway, which in 2023 are approximately 50.38% males and 49.96% females [66]. However, no appropriate statistics were found in terms of the thesis context to verify the gender distributions or the age range or occupation distributions.

| **Age range** | **n** | **%** |
|---|---|---|
| 18-29 | 28 | 20.7% |
| 30-39 | 19 | 14.1% |
| 40-49 | 35 | 25.9% |
| 50-59 | 40 | 29.6% |
| 60 or older | 12 | 8.9% |
| I prefer not to say | 1 | 0.7% |
| | 135 | 100% |
| **Gender** | **n** | **%** |
| Male | 77 | 57.0% |
| Female | 56 | 41.5% |
| Other | 0 | 0.0% |
| I prefer not to say | 2 | 1.5% |
| | 135 | 100% |
| **Current occupation** | **n** | **%** |
| Purchasing and logistics | 8 | 5.9% |
| Finance | 1 | 0.7% |
| IT and information security | 72 | 53.3% |
| HR | 1 | 0.7% |
| Sustainability | 0 | 0.0% |
| Marketing | 3 | 2.2% |
| Communication | 2 | 1.5% |
| Production | 2 | 1.5% |
| General admin. and support | 7 | 5.2% |
| Healthcare | 26 | 19.3% |
| Other | 10 | 7.4% |
| I prefer not to say | 3 | 2.2% |
| | 135 | 100% |
| **Role** | **n** | **%** |
| Manager | 38 | 28.1% |
| No managerial responsibilities | 94 | 69.6% |
| I prefer not to say | 3 | 2.2% |

**Table 6.1:** Overview of questionnaire demographics

### 6.2.2 21-item monetary questionnaires

Across all reward sizes and for all participants ($N = 135$), the geomean k value (geometric mean referred to as geomean in the scoring tool) for the original MCQ was .0219. The k value has a range between .0007 and .1333. Males had an overall geomean k value of .0241 ($n = 77$), while females had an overall geomean k value of .0194 ($n = 56$). The overall consistency was 95%, meaning that subjects were very consistent in their choices for all reward sizes. Counting the cases of choosing Smaller Immediate Reward (SIR) before the specified k value and the instances of Larger Delayed Reward (LDR) after the specified k value yields the consistency score. This amount is divided by the 21 possible items [9]. The overall proportion of LDR choices has a mean of 55%, determining how frequently the subjects chose the larger rewards. The scoring tool [9] also provides the overall k for the small, medium, and large reward sizes. Kirby & Maraković [20] presented in their paper that the overall k value decreased from small to medium to large, resulting in the overall k value for the large rewards being the lowest value. These results comply with the results of this research. However, the small, medium, and large overall k were higher (.0113, .0066, and .0047 for small, medium, and large, respectively reported by Kirby & Maraković [20], and .0283, .0242, and .0190 from this research). The same pattern goes for MCQ-L (S=.1180, M=.1104, L=.1075) and MCQ-G (S=.0644, M=.0462, L=.0429).

The geomean k value for the MCQ-L was .1014. Males had an overall geomean k value of .1035, while females had an average score of .0974. The overall consistency was 89%, and the overall proportion of LDL was 14%.

The geomean k value for the MCQ-G was .0429, where males had an average score of .0450 while females had an average score of .0398. The overall consistency was 90%, and the overall proportion of LDG was 46%. Table 6.2 summarizes the findings from the automatic scoring tool [9].

| **Variable** | **Mean** | **SD** |
|---|---|---|
| Geomean k original | .0219 | .0336 |
| Overall consistency original | 95.41% | 5.22% |
| Overall proportion LDR chosen original | 54.92 % | 30.87% |
| Geomean k loss | .1014 | .0495 |
| Overall consistency loss | 89.21% | 15.56% |
| Overall proportion LDL chosen loss | 14.00% | 21.49% |
| Geomean k gain | .0429 | .0521 |
| Overall consistency gain | 89.84% | 10.27% |
| Overall proportion LDG chosen gain | 46.42% | 35.78% |

**Table 6.2:** Summary statistics for original MCQ, MCQ-L, and MCQ-G reported from the scoring tool by Kaplan et al. [9]

The k-value range is between .0007 and .1333, as stated before. A participant who always chose the immediate reward receives a k value of .1333, while a participant who always chose the delayed reward receives the smallest k value of .0007. Table 6.2 presents the summary statistics, revealing that the average discounting rate was the smallest in terms of the original MCQ. For MCQ-L, the discounting rate was very high (.1014) compared to the original MCQ and MCQ-G, indicating that participants preferred receiving the smaller loss immediately rather than the larger delay later. However, in terms of MCQ-G, the average k value was lower, indicating that the participants chose the delayed option more.

The timing of the rewards was elaborated on in Chapter 5. However, in terms of the MCQ-L they illustrate the time the participant must spend on the security control. If they chose the immediate reward, the idea is that they prefer to implement a security control right away rather than delaying it, which often requires the control to take more time (e.g., if a software update is prompted, usually the update is larger if one delays the update). Regarding the MCQ-G, people tend to choose the larger reward, suggesting that the participants preferred to protect themselves from a higher number of potential successful cyber attacks after a delay. However, the overall proportion of LDG chosen gain was still under 50% (46.42%), so the immediate reward was mainly selected.

| **Occupation** | **Variable** | **Mean** | **SD** |
|---|---|---|---|
| IT and information security | geomean k orig | .0178 | .0292 |
| Healthcare | | .0223 | .0315 |
| Other | | .0295 | .0417 |
| IT and information security | geomean k loss | .1044 | .0479 |
| Healthcare | | .1036 | .0486 |
| Other | | .0939 | .0538 |
| IT and information security | geomean k gain | .0371 | .0477 |
| Healthcare | | .0492 | .0575 |
| Other | | .0498 | .0565 |

**Table 6.3:** Mean and SD of geomean k values in different occupations

Table 6.3 shows the mean of the geomean k value for MCQ, MCQ-L, and MCQ-G divided into three occupation groups. Because the most common groups from the sample were IT and information security (IT) and healthcare (H), these groups were extracted to check for any differences between the means. The "other" category (O) represents all other participants, and the categories include all 135 subjects.

Firstly, the table presents the mean and SD of the geomean k value for the original MCQ between the three different occupation groups. The mean for IT is .0178, with a standard deviation of .0292, suggesting that the average k-value for people working in IT and information security is relatively low, and there is moderate variability in the k-values within this group. In terms of healthcare (M=.0223, SD=.0315), the average k value is slightly higher compared to IT. Additionally, the standard deviation indicates a similar level of variability compared to the IT group. The mean k value for "other" is .0295, with a standard deviation of .0417. The mean and the standard deviation for people working in other fields are higher than those of the IT and H groups. This indicates that the average k-value for the "Other" category is the highest among the three groups, and there is relatively higher variability in the k-values within this group compared to the other groups.

The table presents the mean and SD of the geomean k value for MCQ-L between the three different occupation groups. The mean for IT (M=.1044, SD=.0479) suggests that the average geomean k value for people working in IT and information security is relatively high, and there is a moderate level of variability in the k values. The results from healthcare (M=.1036, SD=.0486) reveal that the average geomean k value is slightly lower with similar variability compared to IT. The other category (M=.0939, SD=.0538) scores lower than IT and healthcare, indicating that the average geomean k value is comparatively lower. However, there is a similar level of variability within this group.

Lastly, Table 6.3 presents the mean and SD of the geomean k value for MCQ-G between the different occupations. IT (M=.0371, SD=.0477) has a relatively low k-value with moderate variability. The mean k value for healthcare is .0492, with a standard deviation of .0575. Comparing it to the mean of the IT group, the average k value for healthcare workers is slightly higher. The standard deviation indicates a higher variability level than the participants working in IT. The mean (M=.0498) and the standard deviation (SD=.0565) for subjects working in other fields are similar to those working in healthcare, indicating that the average k value for the "Other" category is comparable to the healthcare category. There is a similar level of variability in the k-values within the group of participants working in other fields.

Based on these observations, there seems to be a trend of increasing mean geomean k values from people working with IT and information security, to people working in healthcare, and to people working in other fields for the original MCQ values. Additionally, the increasing standard deviations suggest more significant variability in the geomean k values from IT, to healthcare, to "Other" in terms of MCQ. Regarding MCQ-L and MCQ-G, the mean geomean k values for all occupation groups are relatively close, with minor differences. The standard deviations also suggest a comparable level of variability among the three occupation groups. Therefore, the different geomean k values do not imply substantial distinctions between the groups. However, it is essential to note that these observations are based solely on the mean values, standard deviations, and the given range between .0007 and .1333.

### 6.2.3 SA-6 and behavior questionnaire

The SA-6 handout [64] stated that the average score of all six items were to be used. Table 6.4 presents the summary statistics for both SA-6 and the behavior score. The SA-6 score variable has a mean value of 21.53 (SD = 4.67), indicating the average score obtained by the participants. All six items have a scale of 1-5 (strongly disagree - strongly agree), meaning that the individual SA-6 score for each participant can have a range between 6-30. On the other hand, the Behavior score variable has a mean value of 19.74 (SD = 4.76), reflecting the average score related to behavior. These statistics provide a measure of the central tendency and variability within each variable. All five individual behaviors have a range of 1-5 (not implemented the control - implemented the control more than two years ago), meaning that the individual behavior score for each participant can have a range between 5-25.

| Variable | Mean | SD | $\alpha$ | N of items |
|---|---|---|---|---|
| SA-6 score | 21.53 | 4.67 | .855 | 6 |
| Behavior score | 19.74 | 4.76 | .607 | 5 |

**Table 6.4:** Summary statistics for SA-6 and behavior score

The SA-6 questionnaire demonstrated high internal consistency with a Cronbach's alpha coefficient of .855 for the six items, indicating a reliable measure of security attitudes. In the original paper by Faklaris et al. [61], they reported a Cronbach's alpha of .84 which is very similar to the reported SA-6 Cronbach's alpha from the data set. For the behavior score, Cronbach's alpha was also calculated because of the similarities between the data preparation methods. However, the behavior score questionnaire showed low internal consistency with a Cronbach's alpha coefficient of .607, suggesting poor reliability in assessing security behavior [67, 68]. Even though Cronbach's alpha is usually acceptable above .70, several scales indicate that an alpha above .6 can be seen as sufficient, especially in early research [68].

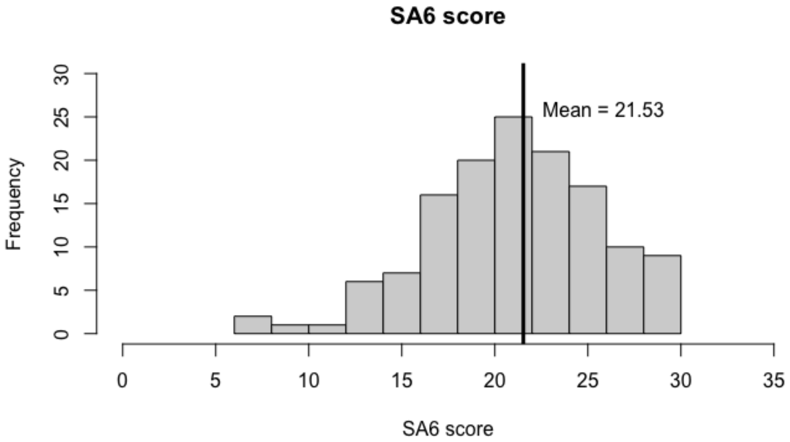
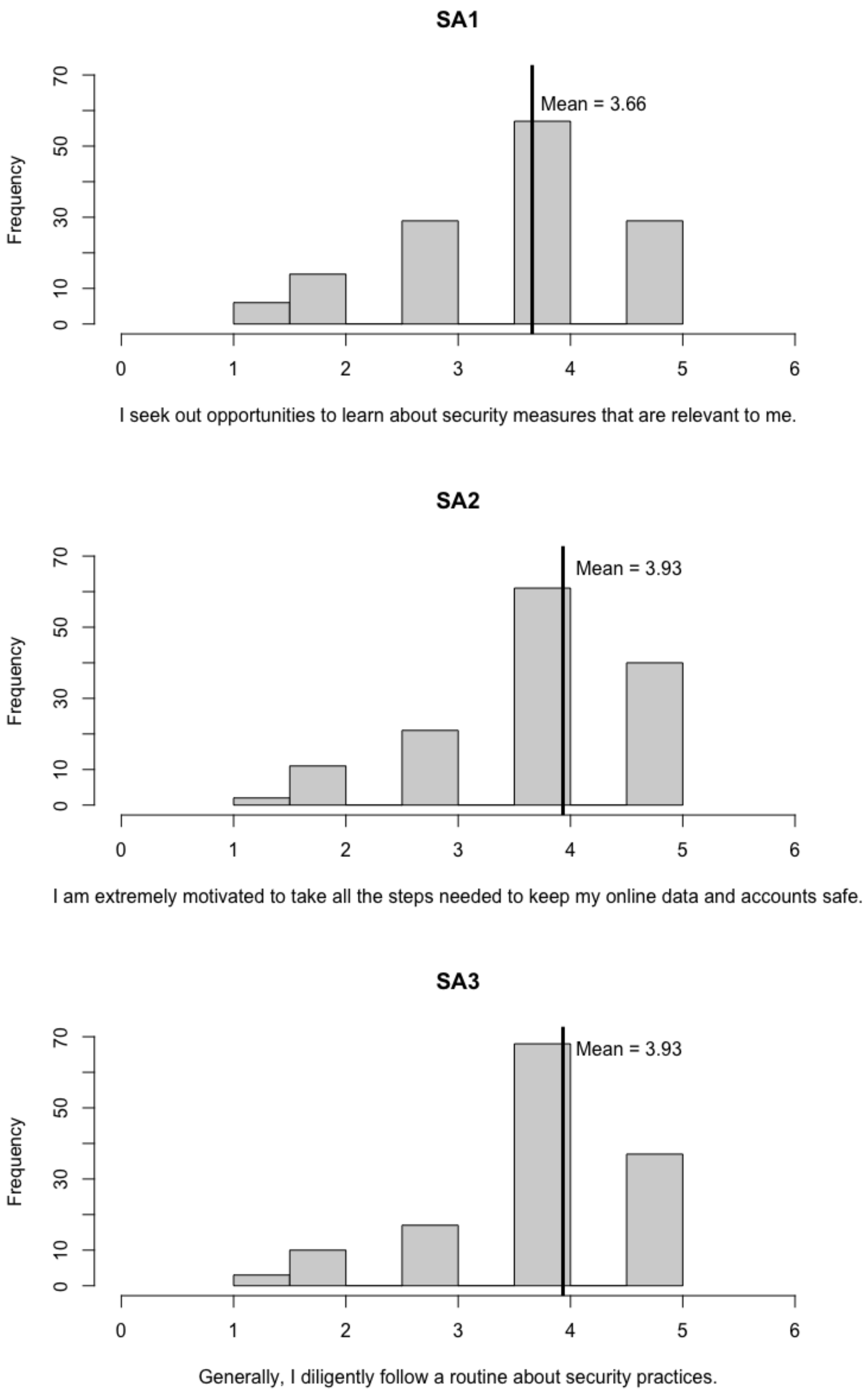


**Figure 6.1:** SA6 score distribution and mean

Figure 6.1 presents a histogram of the SA-6 score distribution and mean. The distribution shows that the individual scores are spread out around the mean. The Shapiro-Wilk test was performed to assess the normality of the SA-6 score variable in the data set [69]. The test revealed a test statistic (W) of .97593 and a p-value of .01703. The test statistic, W, ranges between 0 and 1, where values closer to 1 indicate that the data is more normally distributed. The p-value represents the probability of observing the data if sampled from a normally distributed population. Based on the Shapiro-Wilk test, the null hypothesis of normality was rejected for the SA-6 score variable (p=.01703, alpha=0.05), suggesting that the data significantly deviates from a normal distribution. Figure 6.2 and 6.3 presents a histogram of the individual SA-6 items and the mean.



SA1

SA2

SA3

**Figure 6.2:** Individual SA-6 distributions and mean - part 1

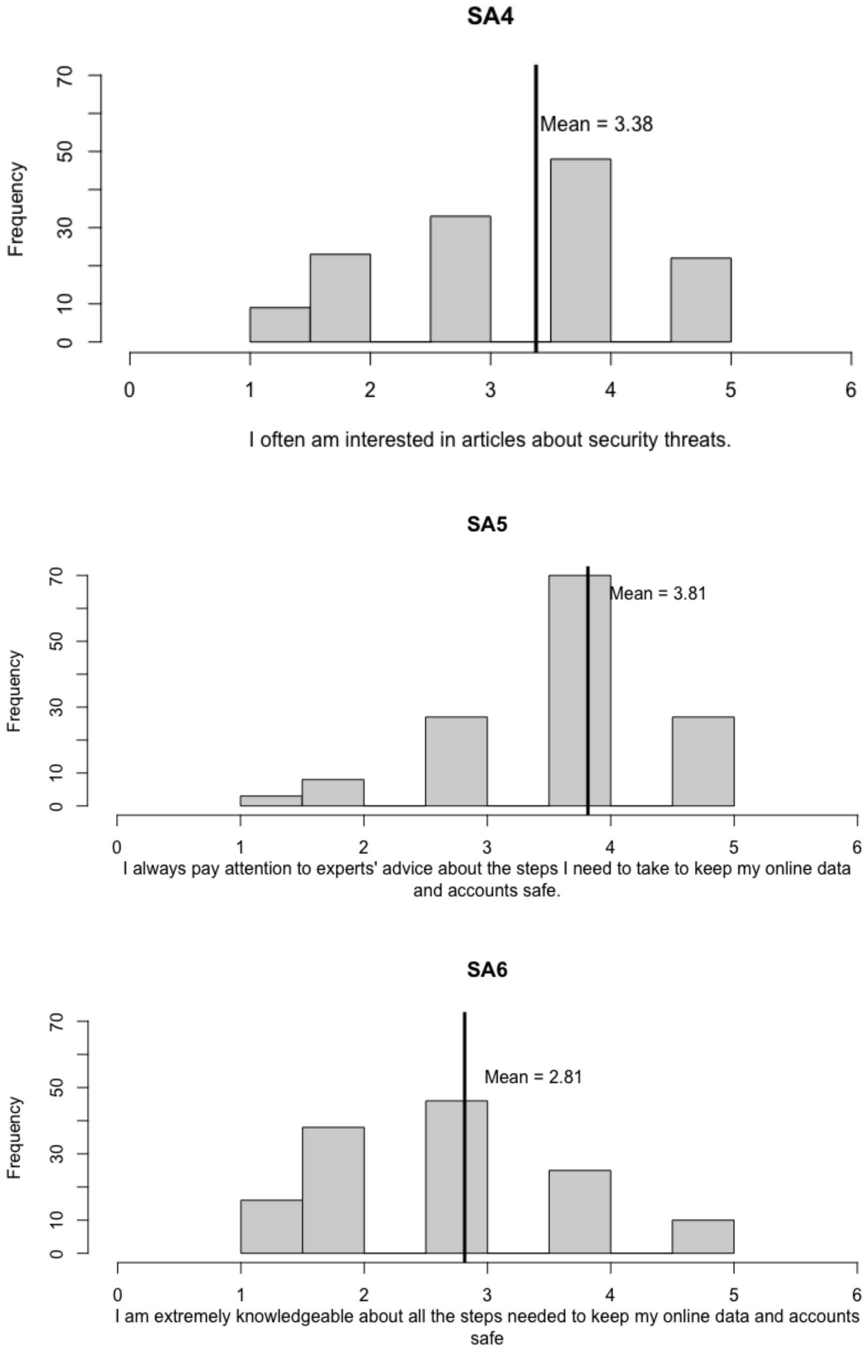


**Figure 6.3:** Individual SA-6 distributions and mean - part 2

Figure 6.4 presents a histogram of the behavior score distribution and mean. The behavior score was calculated based on the individual behaviors as a countermeasure for the skewed data. The distribution is still very right skewed; however, it is better than the individual behaviors illustrated in Figure 6.5 and 6.6. The Shapiro-Wilk test was performed to assess the normality of the behavior score variable in the data set, even though the data was skewed.

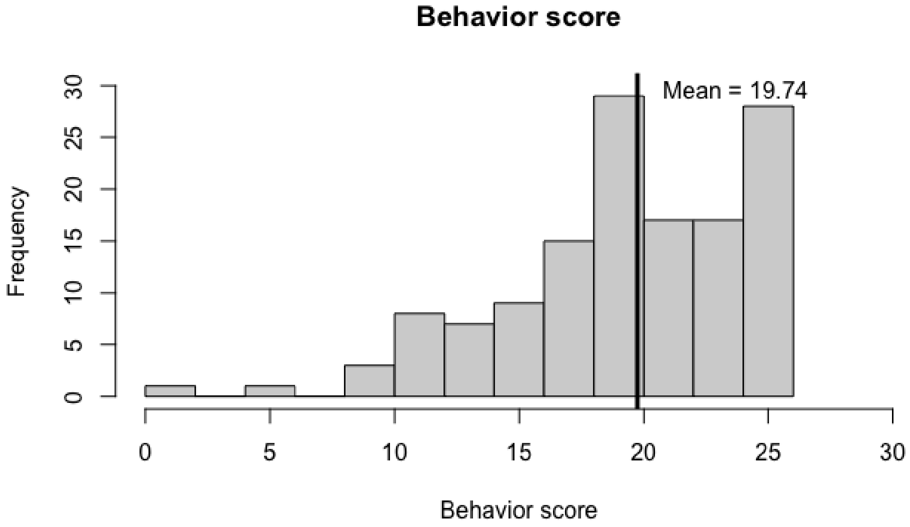


**Figure 6.4:** Behavior score distribution and mean

The test revealed a test statistic (W) of .90006 and a p-value of 4.954e-08. Based on the Shapiro-Wilk test, the null hypothesis of normality was rejected for the behavior score variable, concluding that the data is not normally distributed [69]. These results show that the behavior score was more non-normal distributed than the SA-6 score. Figure 6.5 and 6.6 shows the distribution of the individual behavior variables and illustrates why several scaling methods were tested on the data set as described in Section 6.1. Checking the distributions is crucial because different inferential analysis methods have different requirements.

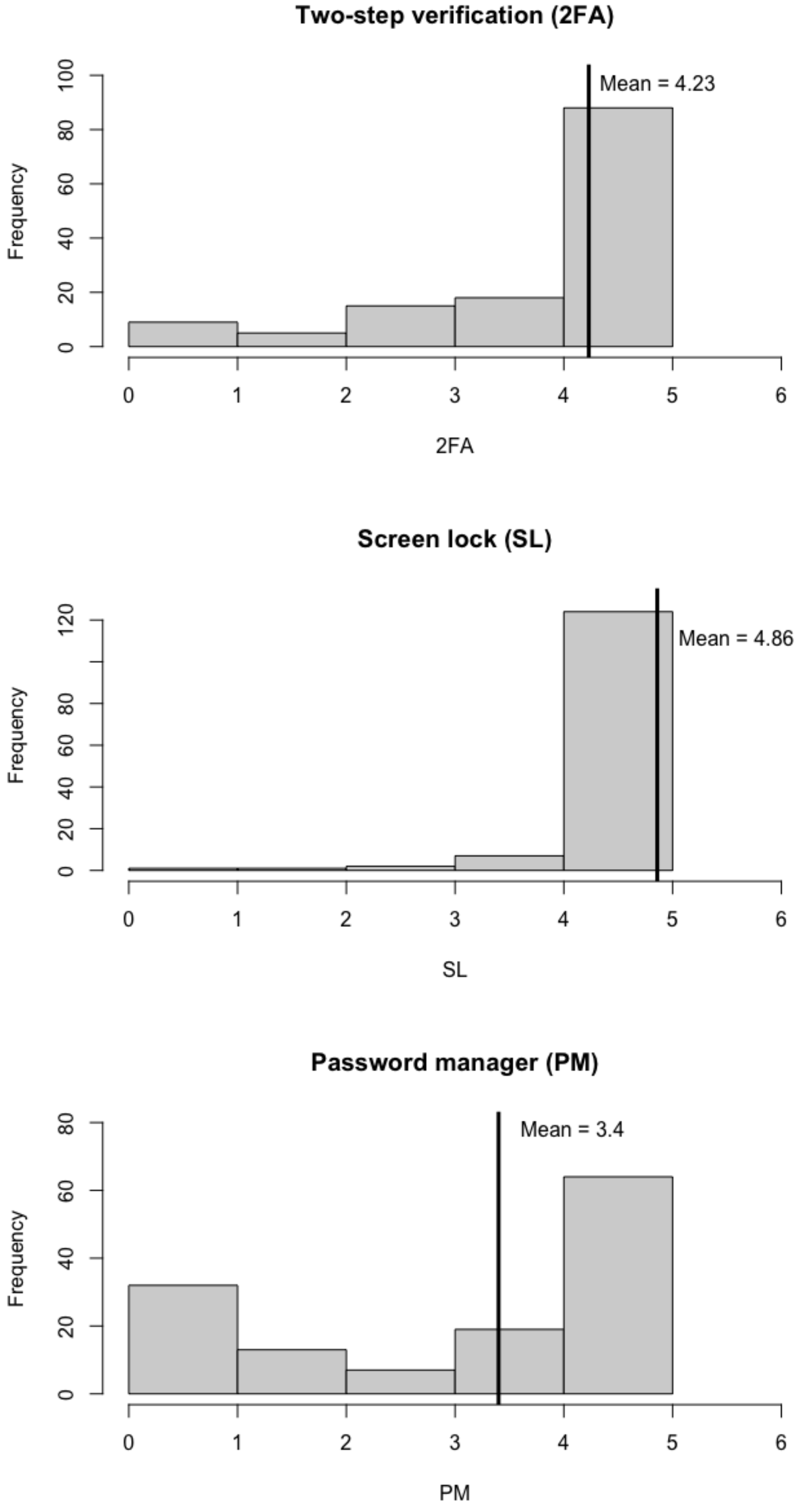


**Figure 6.5:** Individual behavior distributions and mean - part 1

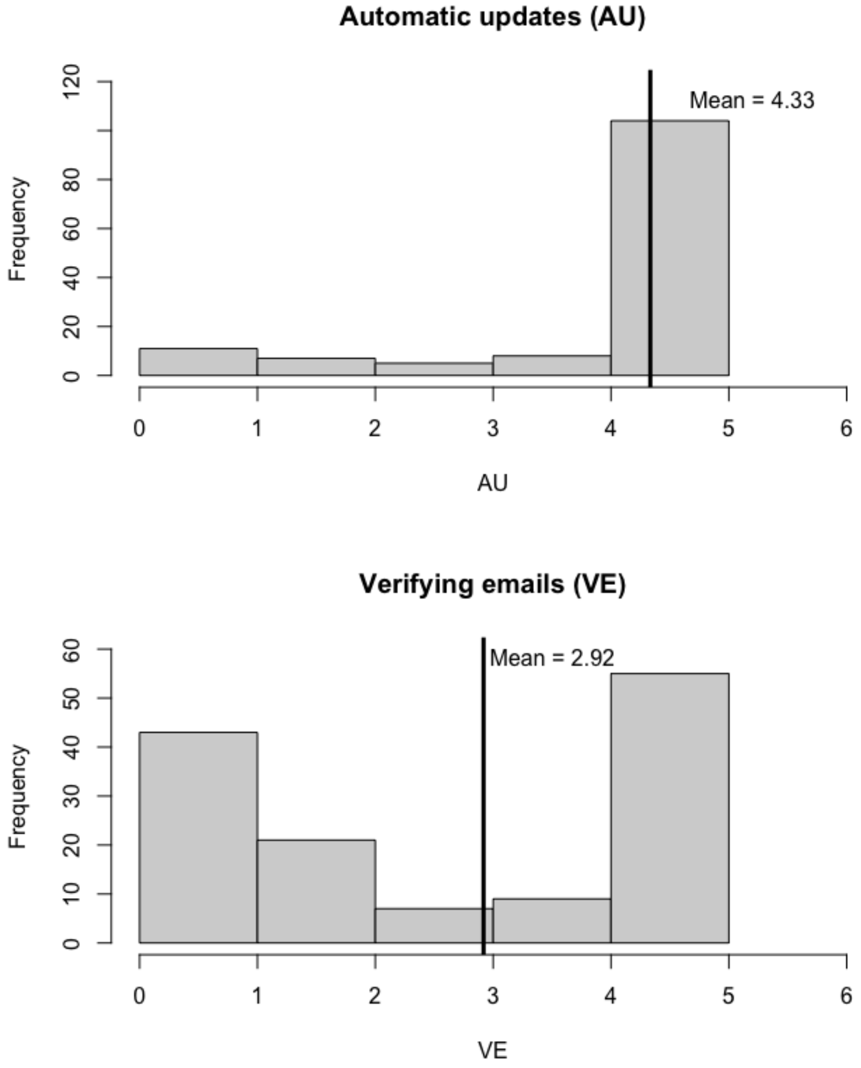


**Figure 6.6:** Individual behavior distributions and mean - part 2

## 6.3 Inferential analysis

Inferential statistics use the sample and the descriptive analysis to understand the larger population [70, 71]. This section uses the standardized data set and presents the inferential analysis performed on the data. The section includes correlations, Welch's t-test, and regression analysis.

### 6.3.1 Correlations

Correlation measures how quantitative or categorical variables are related. Correlation analysis is important to identify variables' relationships to create future behavior. The correlation coefficients have a value between -1 and 1. Values close to 0 imply no relationship between the variables, whereas values closer to -1 or 1 implies strong negative or positive correlations. There are several existing correlations coefficient, where Pearson's correlation coefficient is the most common. However, several factors must be considered when choosing the coefficient [72].

One can perform two general types of tests: parametric and non-parametric. The main difference between these tests is that non-parametric tests do not require normally distributed data. However, parametric tests can yield reliable results even when dealing with data sets exhibiting skewness or not following a normal distribution. The non-parametric alternative to Pearson's correlation is Spearman's correlation [73]. Because the data do not follow a normal distribution, Pearson's and Spearman's correlation were calculated on the data set. However, the results were similar. Therefore, the correlations are presented using Pearson's correlation because it is the most common coefficient. Additionally, Pearson's correlation coefficient is reported in the original SA-6 paper [61]. The correlations are performed on the standardized data set containing 135 subjects.

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1. SA1 | - | | | | | |
| 2. SA2 | .59$^b$ | | | | | |
| 3. SA3 | .44$^b$ | .41$^b$ | | | | |
| 4. SA4 | .69$^b$ | .49$^b$ | .53$^b$ | | | |
| 5. SA5 | .42$^b$ | .43$^b$ | .61$^b$ | .35$^b$ | | |
| 6. SA6 | .56$^b$ | .46$^b$ | .45$^b$ | .65$^b$ | .34$^b$ | |
| 7. Geomean k orig | .14 | .13 | .19$^a$ | .14 | .16 | .22$^a$ |
| 8. Geomean k loss | .27$^b$ | .30$^b$ | .19$^a$ | .15 | .23$^b$ | .13 |
| 9. Geomean k gain | -.24 | .10 | .19$^a$ | -.06 | .13 | .07 |

*Note:*
$^a p < .05$
$^b p < .01$

**Table 6.5:** Pearson's correlation matrix for individual SA-6 scores and geomean k values (n = 135)

A Pearson's correlation test was computed to examine the relationships between individual SA-6 scores (SA1 to SA6) and the three geomean k values. A p-value less than .05 indicates statistical significance, while a p-value less than .01 indicates even stronger statistical significance. As shown in Table 6.5, several significant correlations emerged. Firstly, SA2 demonstrated a significant positive correlation with SA1 (r=.59, p<.01). Similarly, SA3 showed significant positive correlations with SA1 (r=.44,p<.01) and SA2 (r=.41, p<.01). Moreover, SA4 exhibited significant positive correlations with SA1 (r=.69, p<.01), SA2 (r=.49, p<.01), and SA3 (r=.53, p<.01). SA5 demonstrated significant positive correlations with SA1 (r=.42, p<.01), SA2 (r=.43, p<.01), SA3 (r=.61, p<.01), and SA4 (r=.35, p<.01). Furthermore, SA6 showed significant positive correlations with SA1 (r=.56, p<.01), SA2 (r=.46, p<.01), SA3 (r=.45, p<.01), SA4 (r=.65, p<.01), and SA5 (r=.34, p<.01).

Regarding the geomean k values, significant correlations were observed. Geomean k orig showed significant positive correlations with SA3 (r=.19, p<.05) and SA6 (r=.22, p<.01). Geomean k loss exhibited significant positive correlations with SA1 (r=.27, p<.01), SA2 (r=.30, p<.01), SA3 (r=.19, p<.05), and SA5 (r=.23, p<.01). Geomean k gain showed significant positive correlations with SA3 (r=.19, p<.05). No other significant correlations were observed for the geomean k values.

These findings suggest significant associations between the individual SA-6 scores and highlight the associations between the individual SA-6 scores and some of the geomean k values. Table 6.5 does not display the correlations between the different k values because they are presented with the SA-6 score and behavior score in Table 6.6 below.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1. SA-6 | - | | | | |
| 2. Behavior score | .47$^b$ | | | | |
| 3. Geomean k orig | .22$^a$ | .05 | | | |
| 4. Geomean k loss | .27$^b$ | .09 | .07 | | |
| 5. Geomean k gain | .08 | .07 | .43$^b$ | .11 | |

*Note:*
$^a p < .05$
$^b p < .01$

**Table 6.6:** Pearson's correlation matrix for SA-6, behavior scores, and k-values (n = 135)

Table 6.6 displays the correlations between the SA-6 score, behavior score, and the geomean k values. The findings suggest that there are significant correlations between certain variables. Specifically, the behavior score is positively associated with the SA-6 score (r=.47, p<.01), indicating that higher behavior scores are related to higher values of the SA-6 score. Moreover, the geomean k original variable shows positive correlations with the SA-6 score (r=.22, p<.05). Geomean k loss exhibited significant positive correlations with the SA-6 score (r=.27, p<.01). Geomean k gain shows a strong significant positive correlation with the geomean k original variable (r=.43, p<.01), suggesting that as the values of geomean k gain increase, the values of geomean k original tend to increase as well. No other statistically significant correlations were observed.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1. B1 | - | | | | |
| 2. B2 | .24$^b$ | | | | |
| 3. B3 | .31$^b$ | .11 | | | |
| 4. B4 | .34$^b$ | .28$^b$ | .26$^b$ | | |
| 5. B5 | .39$^b$ | .12 | .27$^b$ | .23$^b$ | |
| 6. Geomean k orig | -.04 | -.16 | .03 | .10 | .08 |
| 7. Geomean k loss | .06 | -.06 | .04 | .06 | .10 |
| 8. Geomean k gain | .07 | -.16 | -.02 | .10 | .12 |

*Note:*
$^b p < .01$

**Table 6.7:** Pearson's correlation matrix for individual behavior scores and geomean k values (n = 135)

A Pearson's correlation matrix was constructed to investigate the relationships between individual behavior scores and geomean k values. The behavior scores corresponded to specific actions: B1 (two-step verification), B2 (screen lock), B3 (password manager), B4 (automatic updates), and B5 (verifying emails) and the geomean k values. The results are presented in Table 6.7.

Firstly, B2 demonstrated a significant positive correlation with B1 (r=.24, p<.01). Similarly, B3 exhibited a significant positive correlation with B1 (r=.31, p<.01), but a non-significant correlation with B2 (r=.11). Additionally, B4 displayed significant positive correlations with B1 (r=.34, p<.01), B2 (r=.28, p<.01), and B3 (r=.26, p<.01). B5 showed significant positive correlations with B1 (r=.39, p<.01), B3 (r=.27, p<.01), and B4 (r=.23, p<.01), while having a non-significant correlation with B2 (r=.12).

No statistically significant correlations were observed between the individual behavior scores and the geomean k values. However, it is worth noting that the correlations were generally weak and close to zero, with values ranging from -.06 to .12. These findings suggest limited or non-existent relationships between the individual behavior scores and the geomean k values. Furthermore, the lack of significant correlations between behavior scores and the geomean k values indicates that these variables may operate independently.

### 6.3.2 Welch's t-test

Welch's t-test is an adaptation of the Student's t-test and a two-sample test designed for unequal variances between the variables. Additionally, Welch's t-test is more appropriate when dealing with skewed distributions. The t-test checks whether two sample means are significantly different [74]. The t-tests were calculated on several variables, including gender, k values, behavior score, and SA-6 score. However, table 6.8 presents only the significant results from the t-tests.

The t-test requires the grouping variable to contain two levels only. Therefore, the individual behavior scores were converted into binary values (0, 1): people who had not implemented the control (0) and people who had implemented the control (1).

| | Mean of Group 0 | Mean of Group 1 | Lower | Upper | t | df | p-value |
|---|---|---|---|---|---|---|---|
| SA-6 score, gender | 22.52 | 20.09 | .8521897 | 4.0081999 | 3.0491 | 120.36 | .002823 |
| B1, gender | 4.44 | 3.91 | .06378521 | .99790310 | 2.2538 | 104.15 | .0263 |
| B3, gender | 3.69 | 3.04 | .003550607 | 1.301644198 | 1.9918 | 113.95 | .04878 |
| B5, gender | 3.30 | 2.41 | .215163 | 1.560811 | 2.6121 | 124.51 | .0101 |
| k orig overall, B4 | .01 | .02 | -.0228334612 | -.0004286755 | -2.0867 | 48.781 | .04216 |
| k orig overall log, B2 | -1.66 | -2.14 | .001080044 | .959126498 | 4.3107 | 2.0008 | .04979 |
| k loss geomean, B2 | .13 | .10 | .02169693 | .03876968 | 7.0058 | 132 | 1.133e-10 |
| k loss geomean log, B2 | -.88 | -1.16 | .1900684 | .3732895 | 6.0821 | 132 | 1.198e-08 |
| k loss overall, B2 | .13 | .12 | .008365661 | .022568625 | 4.3083 | 132 | 3.188e-05 |
| k loss overall log, B2 | -.88 | -1.10 | .116456 | .341853 | 4.0222 | 132 | 9.653e-05 |
| k gain overall log, B2 | -1.01 | -1.99 | .2129351 | 1.7513604 | 6.1665 | 1.7883 | .0329 |
| SA-6 score, B1 | 17.29 | 22.02 | -7.678612 | -1.799546 | -3.4272 | 15.471 | .003602 |
| SA-6 score, B3 | 19.78 | 22.41 | -4.3408879 | -.9257788 | -3.0692 | 79.612 | .002934 |
| SA-6 score, B4 | 18.83 | 21.95 | -5.6031484 | -.6276209 | -2.5971 | 22.003 | .01645 |
| SA-6 score, B5 | 19.78 | 23.11 | -4.833780 | -1.829072 | -4.3879 | 127.37 | 2.377e-05 |

**Table 6.8:** Significant results from Welch Two Sample t-test

#### Gender differences

Several Welch's Two Sample t-tests were conducted to compare males and females. Because the participants had four options when specifying gender (1-male, 2-female, 3-other, 4-prefer not to say), the t-tests are performed on the answers by males and females only ($n = 133$).

Firstly, a t-test was performed to compare the mean SA-6 scores between the two gender groups, males (M=22.52) and females (M=20.09); t(120.36)=3.0491, p=.002823. The results conclude a significant difference in the mean SA-6 scores between males and females. Furthermore, males had a higher score than females, with a 95% confidence interval for the difference in means between .85 and 4.01.

Additionally, the t-test revealed significant gender differences regarding the different types of behaviors. The t-test provides evidence to conclude that there is a significant difference in the mean values of the B1 variable (two-step verification) between males (M=4.44) and females (M=3.91); t(104.15)=2.2538, p=.0263. Males have a higher mean value compared to females. The p-value is less than the typical significance level of .05, indicating that the observed difference in means is unlikely to be due to random chance alone. Moreover, the 95% confidence interval does not include zero, further confirming the presence of a meaningful difference.

The analysis found a significant difference in the mean values of the B3 variable (password manager) between males and females. The results were males (M=3.69) and females (M=3.04); t(113.95)=1.9918, p=.04878. Based on the p-value and the 95% confidence interval (.004-1.3), there is a significant difference, and males had a higher mean than females for password manager.

The last results based on gender from Table 6.8 provide evidence to reject the null hypothesis and supports the conclusion that there is a significant difference in the mean values of the B5 variable (verifying emails) between males (M=3.30) and females (2.41); t(124.51)=2.6121, p=.0101. The p-value is less than .05, and the confidence interval (.22-1.56) does not include zero. There is a significant difference in the mean values of the B5 variable between the two groups, with males having a higher mean value than females.

### Behavior differences by k-values

The t-tests were performed on all subjects ($N = 133$), and several significant differences were identified. The scoring tool provides six different k values for each questionnaire; overall k, overall k log, overall k ln, geomean k, geomean k log, and geomean k ln. The correlations are based on the geomean k because it revealed more significance; however, the t-test was performed on all k values. Therefore, Table 6.8 presents different types of k values due to the small number of significant results. The log and ln variables provide the same results; therefore, only the log variable is included in the table.

The analysis suggests that there is a significant difference in the mean values of the k orig overall variable between the participants who did not implement the control (M=.01) and participants who implemented the control (M=.02) for variable B4 (automatic updates); t(48.781)=-2.0867, p=.04216. Because the p-value is less than .05 and the confidence interval does not include zero, one can conclude that there is a significant difference in the mean values of the original overall k-value between the participants who implemented the control and those who did not. The people who implemented the control had a higher mean.

Additionally, the t-test was performed to compare the mean of k orig overall log between the ones who did not implement the B2 (screen lock) control (M=-

1.66) and those who did implement the control (M=-2.14); t(2.0008)=4.3107, p=.04979. The results conclude that there is a significant difference in the mean original k overall log value between the two groups. Furthermore, people who did not implement the control had a higher mean value than those who implemented it, with a 95% confidence interval for the difference in means between .001 and .96.

Regarding the k-values, all four revealed significant differences in the mean for people who implemented B2 (screen lock) and those who did not. Firstly, the analysis of k geomean loss and group 0 (M=.13) and group 1 (M=.10); t(132)= 7.0058, p=1.133e-10. The p-value is extremely small (<.01), indicating strong evidence against the null hypothesis. Furthermore, the 95% confidence interval supports the conclusion that the actual difference in means is likely to be between .02 and .04. The results of k loss geomean log were group 0 (M=-.88) and group 1 (M=-1.16); t(132)=6.0821, p=1.198e-08 with a 95% confidence for the difference in means between .19 and .37. The analysis of k loss overall suggested a significant difference where the mean of group 0 (M=.13) and group 1 (M=.12); t(132)=4.3083, p=3.188e-05 with a 95% confidence interval between .008 and .023. Lastly, the k loss overall log results revealed that the sample estimates for the mean value in group 0 and group 1 are -.88 and -1.10, respectively. Table 6.8 shows that t(132)=4.0222, p=9.653e-05, meaning a significant difference between the groups in terms of the mean values of the k loss overall log variable. The small p-value and the 95% confidence interval support the conclusion that the true difference means is likely to be in between .12 and .34. Those who did not implement the control (group 0) have a higher mean of all the k values related to MCQ-L, compared to those who implemented the control (group 1).

For the last questionnaire, MCQ-G, only the k gain overall log variable gave any results in terms of differences between those who did not implement screen lock (group 0, M=-1.01) and those who did (group 1, M=-1.99); t(1.7883)=6.1665, p=.0329. The alternative hypothesis states that there exists a true difference in means between group 0 and group 1 that is not equal to zero. The 95% confidence interval for this difference in means is calculated as (.2129351, 1.7513604). The analysis reveals a significant difference between group 0 and group 1 concerning the mean values of the k gain overall log variable. The p-value (.0329) is below the typical significance level of .05, indicating strong evidence against the null hypothesis. The 95% confidence interval (.2129351, 1.7513604) suggests that the true difference in means likely falls within this range. Furthermore, the mean value in group 0 is -1.012870, while the mean value in group 1 is -1.995018, indicating a higher mean value in group 0.

No other significant differences in mean related to the k-values were found between the two groups.

### Behavior differences by SA-6 score

Several Welch's Two Sample t-tests were performed to analyze the SA-6 score by the individual behaviors. Table 6.8 shows significant results with all binary behaviors except for B2 (screen lock). As before, the individual behaviors were converted into two groups; Group 0 contains the participants who did not implement the control, and Group 1 contains the ones who did.

The t-test was conducted to compare the mean values of the SA-6 score variable between group 0 and group 1 for the B1 variable (two-step verification). There was a significant difference in SA-6 score between group 0 (M=17.29) and group 1 (M=22.02; t(15.471)=-3.4272, p=.003602 with a confidence interval between -7.68 and -1.80. The analysis provides evidence to reject the null hypothesis and suggests a significant difference in the mean values of the SA-6 score variable between group 0 and group 1.

Additionally, the t-test compared the mean values of the SA-6 score between group 0 (M=19.78) and 1 (M=22.41) for the B3 variable (password manager); t(79.612)=-3.0692, p=.002934, with a 95% confidence interval between -.93 and -3.07. The p-value is less than the significance level of 0.05, indicating that the observed difference in means is unlikely to be due to random chance alone. Additionally, the 95% confidence interval does not include zero, further supporting the presence of a meaningful difference. Therefore, there is a significant difference in the mean values of the SA-6 score between group 0 and group 1 in variable B3.

In terms of the two groups in B4 (automatic updates), the test statistics were for group 0 (M=18.83) and group 1 (M=21.95); t(22.003)=-2.5971, p=.01645. The analysis shows a significant difference in the mean values of the SA-6 score variable between group 0 and group 1, with a 95% confidence interval between -5.60 and -.63.

Lastly, the t-test was conducted to compare the mean values of the SA-6 score variable between the participants who did not implement B5 (group 0) and those who did implement B5 (group 1). B5 is the variable representing the verifying email control. The test statistics revealed for group 0 (M=19.78) and group 1 (23.11); t(127.37)=-4.3879, p=2.377e-05. The alternative hypothesis states that there exists a true difference in means between group 0 and group 1 that is not equal to zero. The analysis reveals compelling evidence to reject the null hypothesis, indicating a significant disparity in the mean values of the SA-6 score variable between group 0 and group 1. The low p-value (2.377e-05) signifies that the observed difference in means is doubtful to have occurred randomly. Furthermore, the 95% confidence interval (-4.833780, -1.829072) confirms that the difference is meaningful and substantiates the presence of a significant distinction.

All of the test results above show that group 1 had a higher mean value compared to group 0, indicating that those who implemented the control have a higher SA-6 score compared to the participants who did not implement it.

### 6.3.3 Regression analysis

The regression analysis aims to see how well delay discounting correlates and predicts information security decision-making in terms of behavior and attitudes. Multiple linear regression is a statistical procedure that predicts the values of a dependent variable from a set of independent variables. If some variables are known, others can be estimated [75, 76]. Multiple linear regression is the statistical procedure used for the regression analysis. The analysis was performed using RStudio on the standardized data ($N = 133$).

A forward stepwise linear regression model was used to identify possible predictors of security behavior and the following variables were considered in the scope of the selection:

- $X_1$ = SA-6 score
- $X_2$ = age
- $X_3$ = gender
- $X_4$ = occupation
- $X_5$ = role
- $X_6$ = k orig geomean
- $X_7$ = k loss geomean
- $X_8$ = k gain geomean

The independent variables used represent all other variables from the data set. The Akaike Information Criterion (AIC) was used as the criterion for variable selection. AIC is a statistical measure that expresses the trade-off between a model's complexity and adequacy of fit. The measure aims to identify the model that best strikes a balance between these elements. The model is considered to be better the lower the AIC score. As a result, when comparing models, the one with the lowest AIC is typically chosen since it offers the best balance between simplicity and adequacy of fit [77]. The initial model was constructed using the following formula:

```
behavior score ~ SA-6 score
```

| Step | Variables added | Df | Sum of Sq | RSS | AIC |
|---|---|---|---|---|---|
| 1 | occupation | 1 | 7.8870 | 96.56 | -39.240 |
| 2 | gender | 1 | 2.37312 | 94.187 | -40.599 |
| <none> | | | | | -40.599 |
| + | age | 1 | 1.14321 | 93.044 | -40.248 |
| + | k gain geomean | 1 | .68274 | 93.504 | -39.581 |
| + | role | 1 | 0.41913 | 93.768 | -39.201 |
| + | k orig geomean | 1 | .33942 | 93.848 | -39.086 |
| + | k loss geomean | 1 | .27137 | 93.916 | -38.989 |
| | *Note:*<br>*Df = Degrees of Freedom*<br>*Sum of sq = Sum of Squares*<br>*RSS = Residual Sum of Squares* | | | | |

**Table 6.9:** The stepwise model selection results predicting security behavior on standardized data

Table 6.9 presents the stepwise model selection results based on the initial model. The first step includes adding the occupation variable, which results in a decrease in the AIC value. In the second step, the gender variable is added, further reducing the AIC value. Finally, the table indicates that no more variables were added, and the final model is presented with its associated AIC value (-40.599). However, Table 6.9 does present the other variables and the AIC value if the variable were to be added below the dashed line. The final model, obtained through stepwise model selection, was a linear regression model with the following formula:

```
summary(lm(behavior score ~ SA-6 score + occupation + gender))
```

The model was fitted using the least squares method, and the coefficient estimates, standard errors, t-values, and p-values are presented in Table 6.10.

| Coefficient | Estimate | Std. Error | t-value | p-value |
|---|---|---|---|---|
| (Intercept) | 2.399e-16 | 7.298e-02 | .000 | 1.00000 |
| SA-6 score | 3.763e-01 | 7.739e-02 | 4.862 | 3.27e-06$^b$ |
| occupation | -2.243e-01 | 7.869e-02 | -2.851 | .00507$^b$ |
| gender | -1.385e-01 | 7.622e-02 | -1.817 | .07154 |
| *Note:*<br>$^b p < .01$ | | | | |

**Table 6.10:** The output from the multiple linear regression model on standardized data

Table 6.10 shows the coefficient, which represents the estimated effects of the predictor variables on the response variable. A positive coefficient implies that the dependent variable's mean tends to increase when the value of the independent variable increases. A negative coefficient indicates that the dependent variable tends to decrease as the independent variable increases [78]. Firstly, (Intercept) represents the estimated mean value of the response variable (behavior score) when all the predictor variables are zero. The SA-6 score coefficient represents the estimated change in the response variable for a one-unit increase in the SA-6 score predictor variable while holding other variables constant. Then, the occupation and gender coefficient represents the same thing as the SA-6 coefficient. For each coefficient, the corresponding standard error estimates the variability or uncertainty associated with the coefficient estimate. Meaning it determines how far apart from the regression line the observed data are on average. Utilizing the units of the response variable, the standard error conveniently informs how consistently the regression model is [79]. Table 6.10 shows the standard error for the intercept (7.298e-02), SA-6 score (7.739e-02), occupation (7.869e-02), and gender (7.622e-02). The t-value is the ratio of the coefficient estimate to its standard error and is used to assess the statistical significance of the coefficient. The p-value indicates the probability of observing a coefficient as extreme as the estimated coefficient under the null hypothesis of no effect. The p-values in Table 6.10 indicate the significance of each variable in predicting the behavior score. For example, the gender variable showed a p-value of .07154, which suggest a marginal level of significance ($p<.1$) [80]. These results suggest that SA6 Score and Occupation significantly impact the behavior score, while Gender has a marginal effect.

The model's performance was assessed using the residual standard error of .8479 on 131 degrees of freedom. The multiple R-squared value was .2971, indicating that the model explains approximately 29.71% of the behavior score variability. The adjusted R-squared value, which accounts for the number of predictors, was .281. The F-statistic was 18.46 with a p-value of 4.765e-10, suggesting that the overall model was statistically significant.

## 6.4 Summary of results

Of the 400 employees invited, 135 participated in the survey (33.25% response rate). The sample included individuals from various ages and genders working in different industries. However, no specific statistics were available to verify the distributions regarding the target group.

The geomean k value for the original MCQ was .0219 (N = 135). Males had a slightly higher geomean k value (.0241) than females (.0194). Overall consistency was 95%, and the proportion of choosing larger delayed rewards was 55%. For MCQ-L, the geomean k value was .1014. Males (.1035) and females (.0974) showed slight variations. Overall consistency was 89%, and the proportion of choosing larger delayed rewards was 14%. For MCQ-G, the geomean k value was .0429. Males (.0450) and females (.0398) differed slightly. Overall consistency was 90%, and the proportion of choosing larger delayed rewards was 46%. The k value ranges from .0007 to .1333, indicating participants' discounting rates. MCQ-L shows a preference for immediate smaller losses, while MCQ-G indicates a preference for larger rewards after a delay.

The SA-6 score has a mean of 21.53 (SD = 4.67), indicating the average score obtained by participants on a scale of 6-30. The Behavior score has a mean of 19.74 (SD = 4.76) on a scale of 5-25. The SA-6 questionnaire shows high internal consistency (Cronbach's alpha=.855), indicating a reliable measurement of security attitudes. However, the behavior score questionnaire demonstrates low internal consistency (Cronbach's alpha=.607), suggesting poor reliability in assessing security behavior. The individual behavior scores revealed a skewed distribution, which is why the total behavior score was calculated.

The k geomean k values showed significant correlations with the individual SA-6 items. The results from MCQ-L had the most significant results with positive correlations with SA1, SA2, SA3, and SA5. The SA-6 score had a significant positive correlation with the behavior score. No significant correlations were detected for the k values and behavior score. However, the k-values from MCQ-L showed a significant positive correlation with the SA-6 score. The k values from the original MCQ and MCQ-G had a positive significant correlation as well. The individual behavior scores had a strong correlation with each other, except for B2 (screen lock) and B3 (password manager), and B2 and B5 (verifying email). No significant correlations were found in terms of individual behaviors and the k-values.

Welch's Two Sample t-tests revealed several significant gender differences. Males had a higher mean for the SA-6 score and also for the individual behaviors B1 (two-step verification), B3 (password manager), and B5 (verifying emails). In terms of the k values, all the different k values from MCQ-L revealed significant differences regarding the participants who implemented screen lock (B2) and those who did not. However, for the original MCQ and MCQ-G, only the overall log k value revealed significant differences with B2. Additionally, k original overall log had significant differences with B4 (automatic updates). No other significant differences were identified for the individual behaviors and k values. Interestingly, the k values had significant differences with the implementation of the screen lock; however, when it came to the SA-6 score, significant differences were identified with all individual behaviors but the screen lock.

A multiple linear regression analysis was performed on the standardized data set, and a forward stepwise linear regression model was used to identify possible predictors of security behavior. The results from the regression analysis show that the SA-6 score and occupation significantly impact the behavior score. The gender variable has a marginal level of significance. The stepwise linear regression model chose no other variables. The residual standard error is .8479, indicating the average distance of observed data from the regression line. The multiple R-squared value is .2971, indicating that the model explains about 29.71% of the behavior score variability. The adjusted R-squared value, accounting for the number of predictors, is .281. The F-statistic is 18.46 with a very low p-value, indicating that the overall model is statistically significant.

# Chapter 7

# Discussion

*The objective of this chapter is to interpret and analyze the results to answer the RQs, and to discuss the significance of the research in a broader context. The RQs have guided the study and are the ones that set the stage for the subsequent discussion. The research questions are as follows:*

***RQ1*** *What is the current state of research on delay discounting in information security, and what are the key findings based on literature?*

***RQ2*** *How well can a survey measuring delay discounting be modified to fit an information security context with similar qualities?*

***RQ3*** *How does delay discounting impact individual decision-making in the context of information security in Norwegian organizations?*

***RQ4*** *How useful is it to discuss delay discounting on how it affects security related decisions in Norwegian organizations?*

*The chapter is divided into five sections, where the first four discuss each RQs as they are presented above. The final section discusses the thesis limitations, including the validity and reliability of the survey design. The aim of the final section is to reflect on the conducted research.*

## 7.1 The current state of research on delay discounting in an information security context

The traditional literature review revealed that the current state of research on delay discounting when it comes to security related decisions is limited. The results revealed seven articles, presented in Table 4.6 that were relevant to the scope and problem description. The important findings are presented in Chapter 3, but the aim of this section is to summarize the findings to discuss the other RQs in a larger context. Delay discounting is a term used in psychology and economics to describe the phenomenon where individuals assign a lower value to rewards that are received at a later point in time, compared to rewards received immediately [6–8]. Acquisti & Grossklags [8, 22] found that individuals tend to discount the value of their personal information when deciding whether to disclose it online. Privacy concerns can outweigh the benefit of discounting, leading to less disclosure even for larger rewards. Grossklags & Barradale [24] observed that people's impatience and socioeconomic status can influence their willingness to invest in security measures. Mishra & Lalumière [33] discovered that delay discounting rates vary across different contexts and that uncertainty plays a role in decision-making. Frik et al. [34] highlighted the challenge of implementing security controls, as people tend to procrastinate costs and prioritize immediate benefits. Vaniea & Rashidi [35] found that inconvenient timing of software updates led to users disabling automatic updates. Rajivan et al. [36] showed that after experiencing a cyber attack, people underestimated future risks and often delayed or skipped necessary updates. Delay discounting can cause people to value immediate benefits over long-term security controls in the context of information security. Employees might be less likely to use strong password practices, for instance, if they believe the rewards of doing so will come too far in the future, like preventing a security breach. Because people may act in ways that expose their organization's sensitive data to attack, this type of conduct might raise the likelihood of security incidents and data breaches.

## 7.2 How well delay discounting can be measured in an information security context

No existing tool was identified that measures delay discounting when it comes to information security decisions. Several approaches have been used previously. For instance, employing experimental designs that involve observing or actively engaging participants in choosing between two distinct options [31, 48, 49]. Due to time constraints, physical observations or experimental investigations were not feasible. Therefore, the questionnaire-based measurement of delay discounting, specifically the 21-Item Monetary Choice Questionnaire (MCQ) developed by Kirby & Maraković, was employed as a reference tool for constructing the questionnaire in this thesis. The 21-Item Monetary Choice Questionnaire (MCQ) by Kirby & Maraković [20] is a validated measure that have been used in several studies. Additionally, an automatic scoring tool [9] has been created which calculates the different values based on the questionnaire. Previous research on delay discounting in general, states that people discount differently in different domains [33]. Two modified versions was developed, aiming to measure delay discounting in an information security context. Specifically, measuring delay discounting when it comes to employees implementing security controls. The results from the MCQ, MCQ-L, and MCQ-G in Table 6.2 shows that the discounting rate (geomean k values) differ between the three questionnaires, supporting that the individual delay discounting rate can variate when investigating different contexts. The results from the original MCQ suggest that people tended to chose the LDR over the SIR with an overall proportion of LDR by 54.92%, compared to an overall proportion of 14% for the MCQ-L and 46.42% for the MCQ-G. In terms of the original MCQ, the results somewhat contradicts the underlying assumption of delay discounting where people tend to prefer smaller, immediate rewards over larger, delayed rewards [6–8]. However, the questionnaire was distributed to employees working in Norwegian organizations which might be an explanation towards the lower discounting rate. The sample group might have a high average income, compared to the original paper where the survey was distributed to collage students, but this was not measured or asked about in the questionnaire. The MCQ, MCQ-L, and MCQ-G followed the same pattern for small, medium, and large reward sized discovered by Kirby & Maraković [20], where the small category had the highest average k-value, and the large had the smallest average k-value.

Both MCQ-L and MCQ-G was constructed based on the same logistics as the original MCQ. The analysis revealed a positive strong correlation (p<.01) between MCQ and MCQ-G. Further, the analysis suggest that there is an improvement when it comes to MCQ-L and the SA-6 score, compared to the MCQ, with a higher positive correlation and a significance level p<.01. Additionally, the variance of the modified versions are similar in terms of the performance to the original questionnaire, with the assumption that the MCQ is reliable and valid. The analysis suggest that it might be more meaningful to measure delay discounting in terms of losses when it comes to security related decision-making.

## 7.3 How delay discounting impact and influence individual information security decision-making

Previous research state that delay discounting is a cognitive process when it comes to decision-making. The concept of discounting explains why people do not always supports the choice that seems to be the best [23, 32]. The analysis from the MCQ, MCQ-L, and MCQ-G reveales that there is a difference between the three modified versions in terms of discounting rate. The results from the MCQ-L indicate that people tend to chose the Smaller Earlier Loss over the Larger Delayed Loss with only a 14% proportion of the LDL chosen. In terms of spending time, the sample prefer to spend as little time as possible in terms of implementing a security control. The overall proportion of subjects selecting the LDL reflects how often the delayed loss were chosen, indicating that sometimes, the subject chose the larger loss with a delay. When framing information security controls as loss, it contradicts the assumptions that people tend to postpone implementing security controls [34–36].

It is important to note that there is a possibility that the introduction text biased the subjects, or that people did not accurately read the instructions. The introduction text to MCQ-L specifies that the participants were to answer as if they actually were to make the choice at work performing their daily tasks. It is interesting that the discouting rate for MCQ-L is much higher than MCQ and MCQ-G. The MCQ-L was framed in terms of loss of productivity, which seems to be the most robust for certain attitudes. However, the results from the MCQ-G revealed a lower average discounting rate. Which supports the assumptions and previous research that people tend to postpone implementing security controls [34–36] to protect themselves from a higher number of potential successful cyber attack. This further supports the findings that people tend to value loss of productivity and workflow more than the security work itself. The results indicate that the main motivation when it comes to information security controls is to avoid the loss, rather than receiving a gain.

Interestingly, the discounting rate did not differ as much across the different occupational categories. Overall, people working in IT and information security had a slightly higher score for MCQ-L, and a slightly lower score for MCQ-G. This supports the previous research by Acquisti [8] that highlights the gap between security attitude and actual security behavior. The results suggest that security aware individuals also can avoid the security steps due to the current needs such as performing a task. Previous research have found that people tend to postpone updating a system, even though updating right away is the best practice [34–36].

The MCQ-G frames an uncertain future by presenting potentially successfully cyber attacks. The results imply that the subjects slightly tend to chose the SEG over the LDG (46.42%). The results supports the findings by Mishra and Lalumière [33], who reflected on the uncertainty aspect within delay discounting. However, the difference between SEG and LDG for MCQ-G was not as significant.

## 7.4 The usefulness of delay discounting and security related decisions

Delay discounting refers to the tendency of individuals to devalue future rewards or benefits as the delay to their receipt increases. Based on previous literature and new findings, delay discounting is an important concept in decision-making and has implications for various domains, including security. The research highlight that people discount differently in different contexts, but also in terms of losses and gains. The context is set to be the same for MCQ-L and MCQ-G, but the average discounting score is very different between the two. The conducted research indicate that employees value time, specifically in terms of loss of workflow or productivity at work, reflected by the subjects mostly choosing the Smaller Earlier Loss. Avoiding loss seems to be a better motivating factor rather than receiving a gain. The research show that delay discounting can affect employees willingness to invest time, effort, and resources into information security compliance activities. Those who heavily discount future consequences may be less likely to invest in robust security controls that takes time to implement, if they do not immediately see the benefits. Employees might underestimate the long-term importance of such measures. Additionally, delay discounting seems to impact employees adherence to security policies if they perceive the benefits as distant or inconsequential. When measuring delay discounting in terms of losses, the results highlight the need for smaller loss rather than larger loss. Short-term actions seems to be the tendency when discussing delay discounting as losses.

Especially the 21-Item Monetary Choice Questionnaire Loss k-value showed positive significant correlations with the SA-6 (r=.27, p<.01), suggesting that as the discounting rate for mcql increase, the SA-6 score tend to increase as well. However, in terms of delay discounting and its impact on actual behavior it seems that the phenomena is not as useful. No correlations were found between the behavior score and k values in Table 6.6, or between individual behaviors in Table 6.7.

Interestingly, the k values had significant differences with the implementation of the screen lock; however, when it came to the SA-6 score, significant differences were identified with all individual behaviors but the screen lock.

The regression analysis shows that the best predictor for behavior is stated attitudes from the SA-6 questionnaire. The different k-values slightly increased the AIC value, and resulted in a slightly lower multiple R-squared value which indicates the models variability in the behavior score. Table 6.10 provides an overview of the regression analysis results. The coefficients represent the estimated effects of the predictor variables on the response variable. Positive coefficients indicate that the mean of the dependent variable (behavior score) tends to increase as the independent variable increases, while negative coefficients suggest a decrease in the dependent variable with an increase in the independent variable [78]. The (Intercept) coefficient represents the estimated mean value of the behavior score when all predictor variables are zero. The SA-6 score coefficient shows the estimated change in the behavior score for a one-unit increase in the SA-6 score predictor variable, while keeping other variables constant. Similarly, the occupation and gender coefficients represent the same concept as the SA-6 coefficient. The corresponding standard errors provide an estimate of the variability or uncertainty associated with each coefficient. They indicate how closely the observed data align with the regression line on average, taking into account the units of the response variable [79].

Table 6.10 presents the standard errors for the intercept (7.298e-02), SA-6 score (7.739e-02), occupation (7.869e-02), and gender (7.622e-02). The t-value, calculated as the ratio of the coefficient estimate to its standard error, is used to assess the statistical significance of each coefficient. The p-values in Table 6.10 indicate the significance of the variables in predicting the behavior score. The gender variable showed a p-value of .07154, suggesting a marginal level of significance (p<.1) [80]. Therefore, the results indicate that SA-6 score and occupation have a significant impact on the behavior score, while gender has a marginal effect.

The model's performance was evaluated using the residual standard error, which was .8479 on 131 degrees of freedom. The multiple R-squared value, representing the proportion of variability in the behavior score explained by the model, was .2971, indicating that approximately 29.71% of the variability is accounted for. The adjusted R-squared value, which considers the number of predictors, was .281. The F-statistic of 18.46 with a p-value of 4.765e-10 suggests that the overall model was statistically significant. The regression analysis results suggest that delay discounting might not be as useful in terms of actual security behaviors.

Delay discounting in an information security decision-making context remains largely unexplored, emphasizing the significance of investigating the cognitive mechanisms that drive decision-making and real-world choices. This study makes a valuable contribution in advancing research in this area.

## 7.5 Limitations

The aim of this section is to address the limitations and reflect on the conducted research. Additionally, the section aims to discuss the validity and reliability of the research. The section is divided into three main categories: scope, literature review, and questionnaires.

### 7.5.1 Scope and sample

The research was conducted to investigate delay discounting as an impact on information security decision-making in Norwegian organizations. The data collection included a traditional literature review, and a questionnaire. The target group was employees in Norwegian organizations. Convenience sampling were used to recruit the participants. 135 employees across Norway participated in the study. Choosing a convenience sample can lead towards sampling bias because it does not result in a statistically balanced selection. However, convenience sample were chosen to get a satisfying response rate, and it resulted in a response rate of approximately 33%. Additionally, three different target organizations were chosen in terms of sample, which contributed towards different occupations and ages. The 135 employees are a sufficient sample size based on previous research [46, 47]. The results (Table 6.3) suggest some differences in delay discounting rates between individuals working in the IT and information security field, healthcare, and people working in other fields. For the original MCQ geomean k values, there is a trend of an increasing mean from IT to healthcare and further to the "Other" category. However, for MCQ-L and MCQ-G values, the mean geomean k values are relatively close to each other with minor differences. The standard deviations indicate a comparable level of variability among the three occupation groups. Based on these observations, it can be inferred that the discounting rate for MCQ-L and MCQ-G are similar across the occupation groups. This suggest that the occupation did not have a major impact on the discounting rate in terms of these specific measures. The findings suggest that the results can be generalized to the larger target group.

### 7.5.2 Literature review

Relevant material may have been excluded or overlooked in the literature review conducted for this research project. For example, certain articles had restricted access. The scoping review was highly reliant on the Boolean search string keywords. However, reference lists and cited papers were also investigated. If most studies comes from one country, the study may not be generalized to the Norwegian context. Some studies were conducted in the United States [22, 23, 34], but the literature review also includes studies from the Netherlands [24] and the UK [33]. However, due to the limited amount of previous research it was important to include all relevant papers available.

### 7.5.3 Questionnaire

The 21-Item Monetary Choice Questionnaire Loss (MCQ-L) and 21-Item Monetary Choice Questionnaire Gain (MCQ-G) was developed based on the validated 21-Item Monetary Choice Questionnaire (MCQ) by Kirby & Maraković [20]. Even though the questionnaire is validated, it does not necessary mean that it is validated for the purpose of this research project. The MCQ have been validated in a certain context and developed in the United States. Additionally, the questionnaires were translated to Norwegian and from USD to NOK as a measure to increase the response rate, resulting in some loss of the validity for the MCQ. The translation was seen as necessary to gain a high response rate, and to ensure that the participants fully understood the requirements. The SA-6 questionnaire have the same validity concerns in terms of the translation process. Acquisti & Grossklags [23] found that people tend to be influenced by previous information and previous situations in terms of security decisions. It was important to set the scene for the subjects in order to make them understand what to do. However, it is a possibility that the instructions made the participants biased. The results are based on the assumptions that all participants answered accurately and honestly.

In terms of the behavior questionnaire, the results revealed very skewed distributions. There was no way to randomize the order of the different questionnaires to check if participants got tired when it came to the last ones. However, the SA-6 was close to the end and after the behavioral block, and the SA-6 had a somewhat normal looking distribution. The problem regarding the behavior questionnaire was not really the sample and unreliable results, but the ranges implemented can be improved. Mostly, the participants chose that the controls were implemented more than two years ago. By changing the ranges, there is a possibility that the distributions gets more evenly spread out. Additionally, the research does not measure to what extent the participants had a freedom in making the behavioral choices. If the organizations have implemented the controls listed in the questionnaire, people might have been forced by the controls to implement them. The skewed data can imply that the organizations might have strict policies. A weakness regarding the behavior questionnaire is that the introduction text did not really specify if the aim was forced behavior or free choice behavior. However, people who scored high on SA-6 also had a high behavior score. It might be that controls such as screen lock are default controls, while the verifying email control is mostly up to the individual which is the control that was mostly spread out in terms of distribution. Although the behavior score questionnaire is a novel instrument, it is important to note that the obtained Cronbach's alpha coefficient of .607 indicates a low level of internal consistency. This suggests that the items within the behavior score questionnaire may not be reliably measuring the intended construct. The low alpha score implies that the questionnaire may require further refinement and additional items to improve its reliability. Future revisions and validation studies are recommended to enhance the internal consistency and ensure the accuracy of the behavior score measurement, even though a Cronbach's alpha might be seen as sufficient above .6 in early research [68]. Considering the relatively weak and non-significant associations observed by k-values and behaviors, further research and a larger sample size may be necessary to gain a more comprehensive understanding between the relationships.

### 7.5.4 Data analysis

It is important to acknowledge that correlations does not imply causation. Further analysis or experimental designs are necessary to establish causality. Additionally, the Pearson's correlation coefficient was used even though the data was not normally distributed. However, several other approaches, such as the Spearman's correlation, to check if the results changed significantly. Several statistical techniques was used on the data set in order to deal with the skewed data, such as the min-max normalization, log transformation, and z-score standardization. However, all re-scaling methods gave very similar results.

# Chapter 8

# Suggestions for future work

This research project produced new knowledge about delay discounting and its impact on information security decision-making. Nevertheless, the topic still needs to be fully explored and requires further research in adapting the findings into specific suggestions for organizations. In order to measure MCQ-L and MCQ-G more comprehensively, it is recommended to develop a scoring tool that considers the given delays and reward sizes. This tool should provide a more comprehensive assessment of the outcomes and better understand the overall impact. Future improvements should maintain consistency in the introductions to the questionnaires, particularly concerning multiple-choice questions (MCQs) and behavior scores, to ensure clarity and coherence in the survey instruments.

The behavior score questionnaire showed low internal consistency (Cronbach's alpha coefficient=.0607). To enhance reliability, future revisions should refine and add more items. Validation studies are recommended for improved internal consistency and accuracy. Adjusting ranges in the skewed behavior questionnaire data can enhance data representation and minimize biases. The questionnaire may primarily reflect organizational strictness rather than intended constructs. Future work should explore alternative approaches for accurate behavior assessment. Incorporating methods for detecting revealed preferences can enhance reliability and validity, even without access to organizational data.

Finally, it would be beneficial to investigate how delay discounting can assist organizational management in understanding individuals. Delay discounting can provide valuable insights into how security controls should be presented and the types of measures that are effective.

# Chapter 9

# Conclusion

The master's thesis aimed to investigate the highly unexplored field of delay discounting and its impact on information security decision-making. Mixed-method research was conducted to explore the previous research by conducting a traditional literature review and to investigate it further by developing a questionnaire to measure delay discounting in an information security decision-making context. The results from the questionnaire were analyzed in order to present the statistics in a larger context.

The results revealed that the field of delay discounting and information security decision-making needs to be explored. Additionally, the results suggest that it might be beneficial to frame security decisions as a loss of productivity or workflow due to the high discounting rate for MCQ-L. Interestingly, the high discounting score contradicts other research and the assumptions that people prefer to postpone implementing security measures.

The modified versions of the MCQ, MCQ-L, and MCQ-G was based on the same parameters as MCQ, where the rewards and delays got adjusted based on the original discounting parameters to ensure that they were compatible with the scoring tool. The results from both MCQ-L and MCQ-G followed the same pattern as the MCQ. The original MCQ and MCQ-G showed a strong positive correlation. A strong, positive correlation indicates that as one variable increases, the other tends to increase consistently. In other words, there is a direct relationship between the two variables. When there is a strong positive correlation, it suggests a strong linear association between the variables, indicating that they tend to move together in the same direction.

Regarding actual behavior, delay discounting does not have a significant impact based on the results. The stepwise multiple regression analysis revealed that attitudes are the best predictor in this field. Approximately 30% of the variability of security behavior is accounted for using attitudes from the SA-6, occupation, and gender.

The project encompassed several challenges and limitations. First, the literature review may have excluded relevant material due to restricted access and specific search keywords. Additionally, validity concerns exist due to contextual differences and translation issues for the MCQ and SA-6. Lastly, the behavior questionnaire showed skewed distributions and weak to non-significant associations between the k-values. Future research, larger sample size, and range improvements might be beneficial.

The field is quite an unexplored area, and exploring the cognitive mechanisms underlying decision-making and real-world choices is important. By considering delay discounting in the context of security-related decisions, organizations can better understand human decision biases and develop strategies to address them.

# Bibliography

[1] T. Schlienger and S. Teufel, ‘Information security culture,’ in *Security in the Information Society*, Springer, 2002, pp. 191–201.

[2] K. Hughes-Lartey, M. Li, F. E. Botchey and Z. Qin, ‘Human factor, a critical weak point in the information security of an organization’s internet of things,’ *Heliyon*, vol. 7, no. 3, e06522, 2021.

[3] C. C. Wood and W. W. Banks Jr, ‘Human error: An overlooked but significant information security problem,’ *Computers & Security*, vol. 12, no. 1, pp. 51–60, 1993.

[4] M. Ahmed, L. Sharif, M. Kabir and M. Al-Maimani, ‘Human errors in information security,’ *International Journal*, vol. 1, no. 3, pp. 82–87, 2012.

[5] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson and C. Jerram, ‘The influence of organizational information security culture on information security decision making,’ *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 117–129, 2015.

[6] C. F. Kurz and A. N. König, ‘Predicting time preference from social media behavior,’ *Future Generation Computer Systems*, vol. 130, pp. 155–163, 2022.

[7] A. Szekeres and E. A. Snekkenes, ‘Inferring delay discounting factors from public observables: Applications in risk analysis and the design of adaptive incentives,’ in *Proceedings of the 5th International Conference on Computer-Human Interaction Research and Applications*, SciTePress, 2021.

[8] A. Acquisti and J. Grossklags, ‘Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior,’ in *2nd Annual Workshop on Economics and Information Security-WEIS*, Citeseer, vol. 3, 2003, pp. 1–27.

[9] B. A. Kaplan, M. Amlung, D. D. Reed, D. P. Jarmolowicz, T. L. McKerchar and S. M. Lemley, ‘Automating scoring of delay discounting for the 21-and 27-item monetary choice questionnaires,’ *The Behavior Analyst*, vol. 39, no. 2, pp. 293–304, 2016.

[10] J. Nikrerk and V. SOLMS, ‘Information security culture: A management perspective,’ 2009.

[11] A. Tsohou, M. Karyda and S. Kokolakis, 'Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs,' *Computers & security*, vol. 52, pp. 128–141, 2015.

[12] L. Green and J. Myerson, 'A discounting framework for choice with delayed and probabilistic rewards.,' *Psychological bulletin*, vol. 130, no. 5, p. 769, 2004.

[13] I. PricewaterhouseCoopers Dublin. 'Conti cyber attack on the hse: Independent post incident review.' (), [Online]. Available: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf (visited on 03/10/2022).

[14] S. Peisert, B. Schneier, H. Okhravi, F. Massacci, T. Benzel, C. Landwehr, M. Mannan, J. Mirkovic, A. Prakash and J. B. Michael, 'Perspectives on the solarwinds incident,' *IEEE Security & Privacy*, vol. 19, no. 2, pp. 7–13, 2021.

[15] SolarWinds. 'Solarwinds: Simple. powerful. secure it.' (), [Online]. Available: https://www.solarwinds.com/company/home (visited on 11/10/2022).

[16] M. B. Jørgenrud. 'Solarwinds gir praktikant skylda for lekkasje av passordet «solarwinds123».' (), [Online]. Available: https://www.digi.no/artikler/solarwinds-gir-praktikant-skylda-for-lekkasje-av-passordet-solarwinds123/507404 (visited on 11/10/2022).

[17] SolarWinds. 'Det var svært lett å gjette passordet til solarwinds' oppdateringsserver.' (), [Online]. Available: https://www.digi.no/artikler/det-var-svaert-lett-a-gjette-passordet-til-solarwinds-oppdateringsserver/504393 (visited on 11/10/2022).

[18] W. E. Forum. 'The global risks report 2022 17th edition insight report.' (), [Online]. Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (visited on 11/10/2022).

[19] D. Malaysia. '91% of all cyber attacks begin with a phishing email to an unexpected victim.' (), [Online]. Available: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html (visited on 11/10/2022).

[20] K. N. Kirby and N. N. Maraković, 'Delay-discounting probabilistic rewards: Rates decrease as amounts increase,' *Psychonomic bulletin & review*, vol. 3, no. 1, pp. 100–104, 1996.

[21] C. Lee, C. C. Lee and S. Kim, 'Understanding information security stress: Focusing on the type of information security compliance activity,' *Computers & Security*, vol. 59, pp. 60–70, 2016.

[22] A. Acquisti, 'Privacy in electronic commerce and the economics of immediate gratification,' in *Proceedings of the 5th ACM conference on Electronic commerce*, 2004, pp. 21–29.

[23] A. Acquisti and J. Grossklags, 'Privacy and rationality in individual decision making,' *IEEE security & privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[24] J. Grossklags and N. J. Barradale, 'Social status and the demand for security and privacy,' in *Privacy Enhancing Technologies: 14th International Symposium, PETS 2014, Amsterdam, The Netherlands, July 16-18, 2014. Proceedings 14*, Springer, 2014, pp. 83–101.

[25] H. A. Simon, 'Bounded rationality,' *Utility and probability*, pp. 15–18, 1990.

[26] D. Ashenden, 'Information security management: A human challenge?' *Information security technical report*, vol. 13, no. 4, pp. 195–201, 2008.

[27] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius and C. Jerram, 'A study of information security awareness in australian government organisations,' *Information Management & Computer Security*, vol. 22, no. 4, pp. 334–345, 2014.

[28] J. D'Arcy, T. Herath and M. K. Shoss, 'Understanding employee responses to stressful information security requirements: A coping perspective,' *Journal of management information systems*, vol. 31, no. 2, pp. 285–318, 2014.

[29] A. Beautement, M. A. Sasse and M. Wonham, 'The compliance budget: Managing security behaviour in organisations,' in *Proceedings of the 2008 new security paradigms workshop*, 2008, pp. 47–58.

[30] D. Box and D. Pottas, 'Improving information security behaviour in the healthcare context,' *Procedia Technology*, vol. 9, pp. 1093–1103, 2013.

[31] A. d. Matta, F. L. Gonçalves and L. Bizarro, 'Delay discounting: Concepts and measures,' *Psychology & Neuroscience*, vol. 5, pp. 135–146, 2012.

[32] G. F. Loewenstein, 'Frames of mind in intertemporal choice,' *Management science*, vol. 34, no. 2, pp. 200–214, 1988.

[33] S. Mishra and M. L. Lalumière, 'Associations between delay discounting and risk-related behaviors, traits, attitudes, and outcomes,' *Journal of Behavioral Decision Making*, vol. 30, no. 3, pp. 769–781, 2017.

[34] A. Frik, S. Egelman, M. Harbach, N. Malkin and E. Peer, 'Better late (r) than never: Increasing cyber-security compliance by reducing present bias,' in *Symposium on Usable Privacy and Security*, 2018, pp. 12–14.

[35] K. Vaniea and Y. Rashidi, 'Tales of software updates: The process of updating software,' in *Proceedings of the 2016 chi conference on human factors in computing systems*, 2016, pp. 3215–3226.

[36] P. Rajivan, E. Aharonov-Majar and C. Gonzalez, 'Update now or later? effects of experience, cost, and risk preference on update decisions,' *Journal of Cybersecurity*, vol. 6, no. 1, tyaa002, 2020.

[37] B. Reynolds and R. Schiffbauer, 'Measuring state changes in human delay discounting: An experiential discounting task,' *Behavioural processes*, vol. 67, no. 3, pp. 343–356, 2004.

[38] J. E. Mazur, 'An adjusting procedure for studying delayed reinforcement,' *Quantitative analyses of behavior*, vol. 5, pp. 55–73, 1987.

[39] T. Busch, *Akademisk skriving for bachelor- og masterstudenter*. Bergen, Norway: Fagbokforlaget, 2013.

[40] J. E. O. Paul D. Leedy, *Practical Research Planning and Design*. United Kingdom: Pearson Education Limited, 2021.

[41] A. Bryman, 'Integrating quantitative and qualitative research: How is it done?' *Qualitative research*, vol. 6, no. 1, pp. 97–113, 2006.

[42] J. C. Greene, V. J. Caracelli and W. F. Graham, 'Toward a conceptual framework for mixed-method evaluation designs,' *Educational evaluation and policy analysis*, vol. 11, no. 3, pp. 255–274, 1989.

[43] J. Jesson, L. Matheson and F. M. Lacey, 'Doing your literature review: Traditional and systematic techniques,' 2011.

[44] Z. Munn, M. D. Peters, C. Stern, C. Tufanaru, A. McArthur and E. Aromataris, 'Systematic review or scoping review? guidance for authors when choosing between a systematic or scoping review approach,' *BMC medical research methodology*, vol. 18, pp. 1–7, 2018.

[45] H. Arksey and L. O'Malley, 'Scoping studies: Towards a methodological framework,' *International journal of social research methodology*, vol. 8, no. 1, pp. 19–32, 2005.

[46] C. W. VanVoorhis, B. L. Morgan *et al.*, 'Understanding power and rules of thumb for determining sample sizes,' *Tutorials in quantitative methods for psychology*, vol. 3, no. 2, pp. 43–50, 2007.

[47] ResearchGaps, *Existing sample size guidelines*, Last accessed 26 April 2023, 2023. [Online]. Available: `https://www.researchgaps.com/existing-sample-size-guidelines/`.

[48] M. Field, M. Santarcangelo, H. Sumnall, A. Goudie and J. Cole, 'Delay discounting and the behavioural economics of cigarette purchases in smokers: The effects of nicotine deprivation,' *Psychopharmacology*, vol. 186, pp. 255–263, 2006.

[49] L. Green, J. Myerson and P. Ostaszewski, 'Discounting of delayed rewards across the life span: Age differences in individual discounting functions,' *Behavioural Processes*, vol. 46, no. 1, pp. 89–96, 1999.

[50] K. Nikolopoulou, *What is convenience sampling? | definition & examples*, Last accessed 26 April 2023, 2022. [Online]. Available: `https://www.scribbr.com/methodology/convenience-sampling/`.

[51] Sikt, *Sikt - kunnskapssektorens tjenesteleverandør*, Last accessed 28 May 2023, 2023. [Online]. Available: `https://sikt.no/`.

[52] A. Beautement, M. A. Sasse and M. Wonham, 'The compliance budget: Managing security behaviour in organisations,' in *Proceedings of the 2008 new security paradigms workshop*, 2008, pp. 47–58.

[53] C. Herley, 'So long, and no thanks for the externalities: The rational rejection of security advice by users,' in *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009, pp. 133–144.

[54] N. Rodríguez-Priego, R. Van Bavel, J. Vila and P. Briggs, 'Framing effects on online security behavior,' *Frontiers in Psychology*, p. 2833, 2020.

[55] NTB, *Oljefondet utsettes for tre alvorlige dataangrep daglig*, Last accessed 20 March 2023, 2022. [Online]. Available: `https://www.digi.no/artikler/na-kan-du-bruke-iphone-mobilen-i-windows/530175`.

[56] DNB, *Annual report 2022*, Last accessed 20 March 2023, 2023. [Online]. Available: `https://www.dnb.no/portalfront/nedlast/no/om-oss/samfunnsansvar/2022/2022-CDC_Annual_Report_v1.0.pdf`.

[57] Kantar, *Europeans' attitudes towards cyber security*, Last accessed 25 March 2023, 2020. [Online]. Available: `https://europa.eu/eurobarometer/surveys/detail/2249`.

[58] G. Snape, *People being proactive about their personal cyber risks, but poor behaviors remain – survey*, Last accessed 20 March 2023, 2022. [Online]. Available: `https://www.insurancebusinessmag.com/us/news/cyber/people-being-proactive-about-their-personal-cyber-risks-but-poor-behaviors-remain--survey-427250.aspx`.

[59] E. Taylor, *18 demographic survey questions (with examples)*, Last accessed 20 April 2023, 2023. [Online]. Available: `https://www.driveresearch.com/market-research-company-blog/7-types-of-demographic-questions-to-include-in-a-market-research-survey/`.

[60] SurveyMonkey, *Demographic survey questions: What they are and why you need them*, Last accessed 20 April 2023, 2023. [Online]. Available: `https://www.surveymonkey.com/mp/gathering-demographic-information-from-surveys/`.

[61] C. Faklaris, L. Dabbish and J. I. Hong, 'A self-report measure of end-user security attitudes (sa-6),' in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[62] S. Egelman and E. Peer, 'Scaling the security wall: Developing a security behavior intentions scale (sebis),' in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 2873–2882.

[63] Google, *Amerikansk dollar til norsk krone*, Last accessed 11 April 2023, 2023. [Online]. Available: `https://www.google.com/finance/quote/USD-NOK?sa=X&sqi=2&ved=2ahUKEwjE2I_C9aH-AhVP6CoKHZQtDh0QmY0JegQICBAd&window=1M`.

[64] C. Faklaris, L. Dabbish and J. I. Hong, *Sa-6, the six-item security attitude scale*, Last accessed 20 April 2023, 2019. [Online]. Available: https://socialcybersecurity.org/files/SA6handout.pdf.

[65] A. Hayes, *Descriptive statistics: Definition, overview, types, example*, Last accessed 26 May 2023, 2023. [Online]. Available: https://www.investopedia.com/terms/d/descriptive_statistics.asp.

[66] SSB, *07459: Population, by sex, contents and year*, Last accessed 24 May 2023, 2023. [Online]. Available: https://www.ssb.no/en/statbank/table/07459/tableViewLayout1/.

[67] S. Glen, *Cronbach's alpha: Definition, interpretation, spss*, Last accessed 24 May 2023, 2023. [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/.

[68] K. S. Taber, 'The use of cronbach's alpha when developing and reporting research instruments in science education,' *Research in science education*, vol. 48, pp. 1273–1296, 2018.

[69] ProjectPro, *What is shapiro test? how to perform it in r*, Last accessed 24 May 2023, 2022. [Online]. Available: https://www.projectpro.io/recipes/what-is-shapiro-test-perform-it-r.

[70] S. Glen, *Inferential statistics: Definition, uses*, Last accessed 25 May 2023, 2023. [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/inferential-statistics/.

[71] P. Bhandari, *Inferential statistics | an easy introduction & examples*, Last accessed 25 May 2023, 2022. [Online]. Available: https://www.scribbr.com/statistics/inferential-statistics/.

[72] S. Glen, *Correlation in statistics: Correlation analysis explained*, Last accessed 24 May 2023, 2023. [Online]. Available: https://www.statisticshowto.com/probability-and-statistics/correlation-analysis/.

[73] J. Frost, *Nonparametric tests vs. parametric tests*, Last accessed 25 May 2023, 2023. [Online]. Available: https://statisticsbyjim.com/hypothesis-testing/nonparametric-parametric-tests/.

[74] S. Glen, *Welch's test for unequal variances*, Last accessed 25 May 2023, 2022. [Online]. Available: https://www.statisticshowto.com/welchs-test-for-unequal-variances/.

[75] S. Sinharay, 'An overview of statistics in education,' in *International Encyclopedia of Education (Third Edition)*, P. Peterson, E. Baker and B. McGaw, Eds., Third Edition, Oxford: Elsevier, 2010, pp. 1–11, ISBN: 978-0-08-044894-7. DOI: https://doi.org/10.1016/B978-0-08-044894-7.01719-X. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B978008044894701719X.

[76] R. Winters, A. Winters and R. G. Amedee, ‘Statistics: A brief overview,’ *Ochsner Journal*, vol. 10, no. 3, pp. 213–216, 2010.

[77] S. Glen, *Akaike’s information criterion: Definition, formulas*, Last accessed 26 May 2023, 2023. [Online]. Available: `https://www.statisticshowto.com/akaikes-information-criterion/`.

[78] J. Frost, *How to interpret p-values and coefficients in regression analysis*, Last accessed 26 May 2023, 2023. [Online]. Available: `https://statisticsbyjim.com/regression/interpret-coefficients-p-values-regression/`.

[79] J. Frost, *Standard error of the regression*, Last accessed 26 May 2023, 2023. [Online]. Available: `https://statisticsbyjim.com/glossary/standard-error-regression/`.

[80] T. Dahiru, ‘P-value, a true test of statistical significance? a cautionary note,’ *Annals of Ibadan postgraduate medicine*, vol. 6, no. 1, pp. 21–26, 2008.

# Appendix A

# Questionnaire (English)

Nettskjema

# Delay discounting in an information security context

## The implementation of cyber security controls in organizations

Cyber threats are increasing in terms of sophistication and impact on organizations. Therefore, employees need to implement security controls to protect organizational assets against cyber attacks. A cyber attack is defined as any attempt to gain unauthorized access to a computing system, computer, or computer network with the intent to cause damage to an organization.
Information security tasks, policies, and guidelines often create unnecessary hurdles and put additional burdens on staff preventing the effective completion of important business activities. Similarly, as employees, we are often required to make choices that result in extra work and a reduction in system usability. This study aims to better understand the negative effects of information security controls, policies, requirements, and norms.

*This study aims to better understand the negative effects of information security controls, policies, requirements, and norms. The survey is part of a 30 ECTS master's thesis in Information Security at NTNU (Norwegian University of Science and Technology). The findings will contribute to the human aspect of security controls to understand employee decision-making.*
***The questionnaire will take approximately 8-15 minutes to complete and the responses are anonymous.***
*Thank you in advance for the time and answers. Do not hesitate to contact me at martemso@stud.ntnu.no if you have any questions. You are also welcome to distribute the survey to colleagues or people working in other organizations.*

## Demographic information

Demographic information is important to describe the population represented in the research which are helpful when analyzing the data. In addition, it allows the researcher to identify and compare different patterns between the demographics.

### What is your age range?

18-29
30-39
40-49
50-59
60 or older
I prefer not to say

### What is your gender?

Male
Female
Other
I prefer not to say

### Which of the following best describes your current occupation?

Purchasing and logistics
Finance

IT and information security

HR

Sustainability

Marketing

Communication

Production

General administration and support to other staff

Healthcare

Other (please specify below)

I prefer not to say

### Please specify your current occupation here:

*This element is only shown when the option 'Other (please specify below)' is selected in the question 'Which of the following best describes your current occupation?'*

### Which of the following best describes your role in the organization you currently work in?

Manager

No managerial responsibilities

I prefer not to say

### The 21-Monetary Choice Questionnaire

For each of the next 21 choices, please indicate which reward you would prefer: the smaller reward tonight, or the larger reward in the specified number of days. Although you will not actually receive any of the money, pretend that you will actually be receiving the amount that you indicate. Therefore, please answer each question honestly and as if you will actually receive the amount chosen either tonight or after a specified number of days.
*To indicate your choice, please select the answer you would like by checking the box. All questions are framed in a similar way, such as:*
*0. Would you prefer 1000 NOK tonight, or 1000 NOK in 45 days?*

### Would you prefer 317 NOK tonight, or 899 NOK in 14 days?

317 NOK tonight

899 NOK in 14 days

### Would you prefer 423 NOK tonight, or 582 NOK in 25 days?

423 NOK tonight

582 NOK in 25 days

### Would you prefer 709 NOK tonight, or 899 NOK in 35 days?

709 NOK tonight

899 NOK in 35 days

### Would you prefer 360 NOK tonight, or 370 NOK in 43 days?

360 NOK tonight

370 NOK in 43 days

**Would you prefer 159 NOK tonight, or 370 NOK in 10 days?**

159 NOK tonight

370 NOK in 10 days

**Would you prefer 338 NOK tonight, or 582 NOK in 20 days?**

338 NOK tonight

582 NOK in 20 days

**Would you prefer 878 NOK tonight, or 899 NOK in 35 days?**

878 NOK tonight

899 NOK in 35 days

**Would you prefer 222 NOK tonight, or 317 NOK in 75 days?**

222 NOK tonight

317 NOK in 75 days

**Would you prefer 508 NOK tonight, or 582 NOK in 45 days?**

508 NOK tonight

582 NOK in 45 days

**Would you prefer 423 NOK tonight, or 687 NOK in 70 days?**

423 NOK tonight

687 NOK in 70 days

**Would you prefer 264 NOK tonight, or 370 NOK in 25 days?**

264 NOK tonight

370 NOK in 25 days

**Would you prefer 687 NOK tonight, or 793 NOK in 50 days?**

687 NOK tonight

793 NOK in 50 days

**Would you prefer 254 NOK tonight, or 582 NOK in 10 days?**

254 NOK tonight

582 NOK in 10 days

**Would you prefer 317 NOK tonight, or 370 NOK in 20 days?**

317 NOK tonight

370 NOK in 20 days

**Would you prefer 561 NOK tonight, or 582 NOK in 55 days?**

561 NOK tonight

582 NOK in 55 days

**Would you prefer 497 NOK tonight, or 635 NOK in 50 days?**

497 NOK tonight

635 NOK in 50 days

### Would you prefer 423 NOK tonight, or 740 NOK in 20 days?

423 NOK tonight

740 NOK in 20 days

### Would you prefer 529 NOK tonight, or 846 NOK in 70 days?

529 NOK tonight

846 NOK in 70 days

### Would you prefer 476 NOK tonight, or 740 NOK in 35 days?

476 NOK tonight

740 NOK in 35 days

### Would you prefer 286 NOK tonight, or 317 NOK in 35 days?

286 NOK tonight

317 NOK in 35 days

### Would you prefer 169 NOK tonight, or 317 NOK in 35 days?

169 NOK tonight

317 NOK in 35 days

## The implementation of security controls

There are several different security controls that exist. Please try to remember the first time you engaged in implementing the following security controls listed below. If you did not engage in the security control below, please state whether or not you intend to do so in the future. Please answer all of the questions as accurately and truthfully as you can.

**2 factor authentication (2FA is an extra layer of protection used to ensure the security of online accounts beyond just a username and password)**

I have not implemented the control. I am not planning to implement it ever.

I have not implemented the control. I am planning to implement it later than this year.

I have not implemented the control. I am planning to implement it this year.

I have implemented the control less than a year ago.

I have implemented the control between a year and 2 years ago.

I have implemented the control more than 2 years ago.

**Screen lock (A device has a screen lock activated if you have to unlock the device with a PIN, pattern, biometrics (fingerprint or face ID), or password)**

I have not implemented the control. I am not planning to implement it ever.

I have not implemented the control. I am planning to implement it later than this year.

I have not implemented the control. I am planning to implement it this year.

I have implemented the control less than a year ago.

I have implemented the control between a year and 2 years ago.

I have implemented the control more than 2 years ago.

**Password manager (A password manager is an application or software that allows you to create, store, and manage your passwords securely)**

I have not implemented the control. I am not planning to implement it ever.

I have not implemented the control. I am planning to implement it later than this year.

I have not implemented the control. I am planning to implement it this year.

I have implemented the control less than a year ago.

I have implemented the control between a year and 2 years ago.

I have implemented the control more than 2 years ago.

**Automatic updates (Automatic updates allow you to keep your applications and softwares updated without having to check for and install available updates manually)**

I have not implemented the control. I am not planning to implement it ever.

I have not implemented the control. I am planning to implement it later than this year.

I have not implemented the control. I am planning to implement it this year.

I have implemented the control less than a year ago.

I have implemented the control between a year and 2 years ago.

I have implemented the control more than 2 years ago.

**Verifying the sender email address when receiving an email**

I have not implemented the control. I am not planning to implement it ever.

I have not implemented the control. I am planning to implement it later than this year.

I have not implemented the control. I am planning to implement it this year.

I have implemented the control less than a year ago.

I have implemented the control between a year and 2 years ago.

I have implemented the control more than 2 years ago.

## Security controls and loss of productivity or workflow

Cybersecurity is a dynamic field, where the external environment changes constantly due to new threats and vulnerabilities. This means that there are several security controls that are implemented to keep security at a desired level. However, some security controls require a loss of productivity or workflow since they are to be done during work. For each of the next 21 choices, please indicate which option you would prefer: the smaller loss immediately, or the larger loss in/after the specified number of days.

Please answer each question honestly and as if you actually make the choice when you are at work performing your daily tasks. Either if you select the smaller loss immediately, or the larger loss after the specified number of days, you will experience some loss of productivity or workflow.

*To indicate your choice, please select the answer you would like by checking the box. All questions are framed in a similar way, such as:*

*0. Would you prefer to spend 90 minutes on implementing a security control immediately, or spend 100 minutes on implementing a security control after 45 days?*

### Would you prefer to spend 21 minutes on implementing a security control immediately, or spend 60 minutes on implementing a security control after 14 days?

21 minutes immediately

60 minutes after 14 days

### Would you prefer to spend 22 minutes on implementing a security control immediately, or spend 30 minutes on implementing a security control after 25 days?

22 minutes immediately

30 minutes after 25 days

**Would you prefer to spend 110 minutes on implementing a security control immediately, or spend 140 minutes on implementing a security control after 35 days?**

110 minutes immediately

140 minutes after 35 days

**Would you prefer to spend 9,7 minutes on implementing a security control immediately, or spend 10 minutes on implementing a security control after 43 days?**

9,7 minutes immediately

10 minutes after 43 days

**Would you prefer to spend 3 minutes on implementing a security control immediately, or spend 8 minutes on implementing a security control after 10 days?**

3 minutes immediately

8 minutes after 10 days

**Would you prefer to spend 13 minutes on implementing a security control immediately, or spend 22 minutes on implementing a security control after 20 days?**

13 minutes immediately

22 minutes after 20 days

**Would you prefer to spend 176 minutes on implementing a security control immediately, or spend 180 minutes on implementing a security control after 35 days?**

176 minutes immediately

180 minutes after 35 days

**Would you prefer to spend 2 minutes on implementing a security control immediately, or spend 3 minutes on implementing a security control after 75 days?**

2 minutes immediately

3 minutes after 75 days

**Would you prefer to spend 46 minutes on implementing a security control immediately, or spend 53 minutes on implementing a security control after 45 days?**

46 minutes immediately

53 minutes after 45 days

**Would you prefer to spend 24 minutes on implementing a security control immediately, or spend 39 minutes on implementing a security control after 70 days?**

24 minutes immediately

39 minutes after 70 days

**Would you prefer to spend 4 minutes on implementing a security control immediately, or spend 5 minutes on implementing a security control after 25 days?**

4 minutes immediately

5 minutes after 25 days

**Would you prefer to spend 139 minutes on implementing a security control immediately, or spend 160 minutes on implementing a security control after 50 days?**

139 minutes immediately

160 minutes after 50 days

**Would you prefer to spend 5 minutes on implementing a security control immediately, or spend 11 minutes on implementing a security control after 10 days?**

5 minutes immediately

11 minutes after 10 days

**Would you prefer to spend 3 minutes on implementing a security control immediately, or spend 4 minutes on implementing a security control after 20 days?**

3 minutes immediately

4 minutes after 20 days

**Would you prefer to spend 57 minutes on implementing a security control immediately, or spend 59 minutes on implementing a security control after 55 days?**

57 minutes immediately

59 minutes after 55 days

**Would you prefer to spend 36 minutes on implementing a security control immediately, or spend 46 minutes on implementing a security control after 50 days?**

36 minutes immediately

46 minutes after 50 days

**Would you prefer to spend 46 minutes on implementing a security control immediately, or spend 80 minutes on implementing a security control after 20 days?**

46 minutes immediately

80 minutes after 20 days

**Would you prefer to spend 75 minutes on implementing a security control immediately, or spend 120 minutes on implementing a security control after 70 days?**

75 minutes immediately

120 minutes after 70 days

**Would you prefer to spend 64 minutes on implementing a security control immediately, or spend 100 minutes on implementing a security control after 35 days?**

64 minutes immediately

100 minutes after 35 days

**Would you prefer to spend 0,9 minutes on implementing a security control**

**immediately, or spend 1 minute on implementing a security control after 35 days?**

0,9 minutes immediately

1 minute after 35 days

**Would you prefer to spend 4 minutes on implementing a security control immediately, or spend 7 minutes on implementing a security control after 35 days?**

4 minutes immediately

7 minutes after 35 days

## SA-6 questionnaire

Below you will find six different statements. Please answer all the statements as accurately and truthfully as you can.

**I seek out opportunities to learn about security measures that are relevant to me.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

**I am extremely motivated to take all the steps needed to keep my online data and accounts safe.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

**Generally, I diligently follow a routine about security practices.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

**I often am interested in articles about security threats.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

**I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

**I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.**

Strongly disagree

Disagree

Neither agree nor disagree

Agree

Strongly agree

## Security controls and protection against cyber attacks

Cybersecurity is a dynamic field, where the external environment changes constantly due to new threats and vulnerabilities. This means that in order to maintain your desired/previous level of cybersecurity over time, you need to actively execute some actions on the systems you interact with.
For each of the next 21 choices, please indicate which option you would prefer: the smaller benefit now or the larger benefit after the specified number of minutes.
Please answer each question honestly and as if you actually make the choice when you are at work performing your daily tasks.
*To indicate your choice, please select the answer you would like by checking the box. All questions are framed in a similar way, such as:*
*0. Would you prefer protection from 90 potentially successful cyber attacks immediately, or protection from 100 potentially successful cyber attacks after 45 minutes?*

### Would you prefer protection from 656 potentially successful cyber attacks immediately, or protection from 1000 potentially successful cyber attacks after 4 minutes?

656 immediately

1000 after 4 minutes

### Would you prefer protection from 43 potentially successful cyber attacks immediately, or protection from 50 potentially successful cyber attacks after 10 minutes?

43 immediately

50 after 10 minutes

### Would you prefer protection from 769 potentially successful cyber attacks immediately, or protection from 1000 potentially successful cyber attacks after 39 minutes?

769 immediately

1000 after 39 minutes

### Would you prefer protection from 9,6 potentially successful cyber attacks immediately, or protection from 10 potentially successful cyber attacks after 59 minutes?

9,6 immediately

10 after 59 minutes

**Would you prefer protection from 7 potentially successful cyber attacks immediately, or protection from 10 potentially successful cyber attacks after 3 minutes?**

7 immediately

10 after 3 minutes

**Would you prefer protection from 40 potentially successful cyber attacks immediately, or protection from 50 potentially successful cyber attacks after 7 minutes?**

40 immediately

50 after 7 minutes

**Would you prefer protection from 985 potentially successful cyber attacks immediately, or protection from 1000 potentially successful cyber attacks after 22 minutes?**

985 immediately

1000 after 22 minutes

**Would you prefer protection from 1 potentially successful cyber attack immediately, or protection from 2 potentially successful cyber attacks after 180 minutes?**

1 immediately

2 after 180 minutes

**Would you prefer protection from 42 potentially successful cyber attacks immediately, or protection from 50 potentially successful cyber attacks after 60 minutes?**

42 immediately

50 after 60 minutes

**Would you prefer protection from 62 potentially successful cyber attacks immediately, or protection from 150 potentially successful cyber attacks after 160 minutes?**

62 immediately

150 after 160 minutes

**Would you prefer protection from 9 potentially successful cyber attacks immediately, or protection from 10 potentially successful cyber attacks after 11 minutes?**

9 immediately

10 after 11 minutes

**Would you prefer protection from 534 potentially successful cyber attacks immediately, or protection from 666 potentially successful cyber attacks after 80 minutes?**

534 immediately

666 after 80 minutes

**Would you prefer protection from 44 potentially successful cyber attacks immediately, or protection from 50 potentially successful cyber attacks after 1 minute?**

44 immediately

50 after 1 minute

**Would you prefer protection from 9,6 potentially successful cyber attacks immediately, or protection from 10 potentially successful cyber attacks after 5 minutes?**

9,6 immediately

10 after 5 minutes

**Would you prefer protection from 46 potentially successful cyber attacks immediately, or protection from 50 potentially successful cyber attacks after 120 minutes?**

46 immediately

50 after 120 minutes

**Would you prefer protection from 65 potentially successful cyber attacks immediately, or protection from 100 potentially successful cyber attacks after 100 minutes?**

65 immediately

100 after 100 minutes

**Would you prefer protection from 385 potentially successful cyber attacks immediately, or protection from 500 potentially successful cyber attacks after 8 minutes?**

385 immediately

500 after 8 minutes

**Would you prefer protection from 377 potentially successful cyber attacks immediately, or protection from 832 potentially successful cyber attacks after 140 minutes?**

377 immediately

832 after 140 minutes

**Would you prefer protection from 289 potentially successful cyber attacks immediately, or protection from 500 potentially successful cyber attacks after 46 minutes?**

289 immediately

500 in 46 minutes

**Would you prefer protection from 1,8 potentially successful cyber attacks immediately, or protection from 2 potentially successful cyber attacks after 30**

### minutes?

1,8 immediately

2 after 30 minutes

### Would you prefer protection from 1 potentially successful cyber attack immediately, or protection from 2 potentially successful cyber attacks after 53 minutes?

1 immediately

2 after 53 minutes

### Thank you for your time and answers! Click &#34;Send&#34; to submit.

*By submitting this form, I consent to participate in this study. I understand that because my participation is anonymous, I cannot withdraw consent once I have submitted my answers.*

# Appendix B

# Questionnaire (Norwegian)

# Delay discounting i en informasjonssikkerhetskontekst

## Implementering av cybersikkerhetstiltak i organisasjoner

Cybertrusler øker ved at de blir mer sofistikert og har en større innvirkning pa organisasjoner. Ansatte ma derfor implementere sikkerhetstiltak for a beskytte organisatoriske eiendeler mot cyberangrep. Et cyberangrep er definert som ethvert forsøk pa a fa uautorisert tilgang til et datasystem, datamaskin eller datanettverk med den hensikt a forarsake skade pa en organisasjon.
Informasjonssikkerhetsoppgaver, policyer og retningslinjer skaper ofte unødvendige hindringer og legger ekstra byrder pa de ansatte som forhindrer effektiv gjennomføring av viktige forretningsaktiviteter. Tilsvarende er vi som ansatte ofte palagt a ta valg som resulterer i ekstraarbeid og redusert systembrukbarhet.

*Denne studien har som mal a bedre forsta de negative effektene av informasjonssikkerhetstiltak, policyer og retningslinjer. Undersøkelsen er en del av en 30 stp. masteroppgave i Informasjonssikkerhet ved NTNU (Norges teknisk-naturvitenskapelige universitet). Funnene vil bidra til det menneskelige aspektet ved sikkerhetstiltak for a forsta ansattes beslutningstaking.*
***Spørreundersøkelsen vil ta omtrent 8-15 minutter a fylle ut og svarene er anonyme.***
*På forhånd takk for tiden og dine svar. Ikke nøl med å kontakte meg på martemso@stud.ntnu.no dersom du har spørsmål. Du kan også gjerne distribuere undersøkelsen til kolleger eller personer som jobber i andre organisasjoner.*

## Demografisk informasjon

Demografisk informasjon er viktig for a beskrive befolkningen som er representert i forskningen, noe som er nyttig nar man analyserer dataene. I tillegg lar det forskeren identifisere og sammenligne ulike mønstre mellom demografien.

### Hva er din aldersgruppe?

18-29
30-39
40-49
50-59
60 eller eldre
Jeg ønsker å ikke oppgi

### Hva er ditt kjønn?

Mann
Kvinne
Annet
Jeg ønsker å ikke oppgi

### Hvilket av følgende alternativer beskriver best ditt nåværende yrke?

Innkjøp og logistikk
Finans og økonomi
IT og Informasjonssikkerhet
HR
Bærekraft

Markedsføring

Kommunikasjon

Produksjon

Generell administrasjon og støtte til øvrige ansatte

Helse

Annet (spesifiser nedenfor)

Jeg ønsker å ikke oppgi

### Spesifiser ditt nåværende yrke her:

*Dette elementet vises kun dersom alternativet «Annet (spesifiser nedenfor)» er valgt i spørsmålet «Hvilket av følgende alternativer beskriver best ditt nåværende yrke?»*

### Hvilket av følgende beskriver best din rolle i organisasjonen du jobber i?

Leder

Ingen lederansvar

Jeg ønsker å ikke oppgi

### The 21-Monetary Choice Questionnaire

Vennligst angi hvilken belønning du foretrekker for hvert av de neste 21 valgene: den mindre belønningen i kveld, eller den større belønningen etter det angitte antall dager. Selv om du faktisk ikke vil motta noen av pengene, forestill deg at du faktisk vil motta beløpet du angir. Svar derfor ærlig pa hvert spørsmal, og som om du faktisk kommer til a fa beløpet som er valgt enten i kveld eller etter et spesifisert antall dager.
*For a angi ditt valg, velg svaret du ønsker ved a merke av i boksen. Alle spørsmal er formulert pa en lignende mate, for eksempel:*
*0. Ville du foretrukket 1000 NOK i kveld, eller 1000 NOK om 45 dager?*

### Ville du foretrukket 317 NOK i kveld, eller 899 NOK om 14 dager?

317 NOK i kveld

899 NOK om 14 dager

### Ville du foretrukket 423 NOK i kveld, eller 582 NOK om 25 dager?

423 NOK i kveld

582 NOK om 25 dager

### Ville du foretrukket 709 NOK i kveld, eller 899 NOK om 35 dager?

709 NOK i kveld

899 NOK om 35 dager

### Ville du foretrukket 360 NOK i kveld, eller 370 NOK om 43 dager?

360 NOK i kveld

370 NOK om 43 dager

### Ville du foretrukket 159 NOK i kveld, eller 370 NOK om 10 dager?

159 NOK i kveld

370 NOK om 10 dager

### Ville du foretrukket 338 NOK i kveld, eller 582 NOK om 20 dager?

338 NOK i kveld

582 NOK om 20 dager

**Ville du foretrukket 878 NOK i kveld, eller 899 NOK om 35 dager?**

878 NOK i kveld

899 NOK om 35 dager

**Ville du foretrukket 222 NOK i kveld, eller 317 NOK om 75 dager?**

222 NOK i kveld

317 NOK om 75 dager

**Ville du foretrukket 508 NOK i kveld, eller 582 NOK om 45 dager?**

508 NOK i kveld

582 NOK om 45 dager

**Ville du foretrukket 423 NOK i kveld, eller 687 NOK om 70 dager?**

423 NOK i kveld

687 NOK om 70 dager

**Ville du foretrukket 264 NOK i kveld, eller 370 NOK om 25 dager?**

264 NOK i kveld

370 NOK om 25 dager

**Ville du foretrukket 687 NOK i kveld, eller 793 NOK om 50 dager?**

687 NOK i kveld

793 NOK om 50 dager

**Ville du foretrukket 254 NOK i kveld, eller 582 NOK om 10 dager?**

254 NOK i kveld

582 NOK om 10 dager

**Ville du foretrukket 317 NOK i kveld, eller 370 NOK om 20 dager?**

317 NOK i kveld

370 NOK om 20 dager

**Ville du foretrukket 561 NOK i kveld, eller 582 NOK om 55 dager?**

561 NOK i kveld

582 NOK om 55 dager

**Ville du foretrukket 497 NOK i kveld, eller 635 NOK om 50 dager?**

497 NOK i kveld

635 NOK om 50 dager

**Ville du foretrukket 423 NOK i kveld, eller 740 NOK om 20 dager?**

423 NOK i kveld

740 NOK om 20 dager

### Ville du foretrukket 529 NOK i kveld, eller 846 NOK om 70 dager?

529 NOK i kveld

846 NOK om 70 dager

### Ville du foretrukket 476 NOK i kveld, eller 740 NOK om 35 dager?

476 NOK i kveld

740 NOK om 35 dager

### Ville du foretrukket 286 NOK i kveld, eller 317 NOK om 35 dager?

286 NOK i kveld

317 NOK om 35 dager

### Ville du foretrukket 169 NOK i kveld, eller 317 NOK om 35 dager?

169 NOK i kveld

317 NOK om 35 dager

## Implementering av sikkerhetstiltak

Det finnes flere ulike sikkerhetstiltak. Prøv a huske første gang du implementerte de sikkerhetstiltakene som er oppført nedenfor. Hvis du ikke har implementert sikkerhetstiltaket nedenfor, vennligst oppgi om du har tenkt til a gjøre det i fremtiden eller ikke. Vennligst svar pa alle spørsmalene sa nøyaktig og sannferdig som du kan.

**2-faktor autentisering (2FA er et ekstra lag med beskyttelse som brukes for å sikre sikkerheten til nettkontoer utover bare et brukernavn og passord)**

Jeg har ikke implementert tiltaket. Jeg kommer aldri til å implementere det.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det senere enn i år.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det i år.

Jeg implementerte tiltaket for mindre enn ett år siden.

Jeg implementerte tiltaket for mellom et år og 2 år siden.

Jeg implementerte tiltaket for mer enn 2 år siden.

**Skjermlås (En enhet har en skjermlås aktivert hvis du må låse opp enheten med en PIN-kode, mønster, biometri (fingeravtrykk eller ansikts-ID) eller passord)**

Jeg har ikke implementert tiltaket. Jeg kommer aldri til å implementere det.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det senere enn i år.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det i år.

Jeg implementerte tiltaket for mindre enn ett år siden.

Jeg implementerte tiltaket for mellom et år og 2 år siden.

Jeg implementerte tiltaket for mer enn 2 år siden.

**Passordhåndteringsprogram (Et passordhåndteringsprogram er en applikasjon eller programvare som lar deg opprette, lagre og administrere passordene dine på en sikker måte)**

Jeg har ikke implementert tiltaket. Jeg kommer aldri til å implementere det.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det senere enn i år.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det i år.

Jeg implementerte tiltaket for mindre enn ett år siden.

Jeg implementerte tiltaket for mellom et år og 2 år siden.

Jeg implementerte tiltaket for mer enn 2 år siden.

**Automatiske oppdateringer (Automatiske oppdateringer lar deg holde applikasjoner og programvare oppdatert uten å måtte se etter og installere tilgjengelige oppdateringer manuelt)**

Jeg har ikke implementert tiltaket. Jeg kommer aldri til å implementere det.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det senere enn i år.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det i år.

Jeg implementerte tiltaket for mindre enn ett år siden.

Jeg implementerte tiltaket for mellom et år og 2 år siden.

Jeg implementerte tiltaket for mer enn 2 år siden.

**Bekrefte avsenderens e- postadresse når du mottar en e-post**

Jeg har ikke implementert tiltaket. Jeg kommer aldri til å implementere det.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det senere enn i år.

Jeg har ikke implementert tiltaket. Jeg planlegger å implementere det i år.

Jeg implementerte tiltaket for mindre enn ett år siden.

Jeg implementerte tiltaket for mellom et år og 2 år siden.

Jeg implementerte tiltaket for mer enn 2 år siden.

## Sikkerhetstiltak og tap av produktivitet eller arbeidsflyt

Cybersikkerhet er et dynamisk felt hvor det ytre miljøet hele tiden endres pa grunn av nye trusler og sarbarheter. Dette betyr at det er flere sikkerhetstiltak som ma implementeres for a holde sikkerheten pa et ønsket niva. Noen sikkerhetstiltak krever imidlertid tap av produktivitet eller arbeidsflyt siden de skal utføres under arbeid. Vennligst angi hvilket alternativ du foretrekker for hvert av de neste 21 valgene: det mindre tapet umiddelbart, eller det større tapet i/etter det angitte antallet dager.
Svar ærlig pa hvert spørsmal og som om du tar valget nar du er pa jobb og mens du utfører dine daglige arbeidsoppgaver. Du vil oppleve noe tap av produktivitet eller arbeidsflyt enten om du velger det mindre tapet umiddelbart, eller det større tapet etter det angitte antallet dager.
*For a angi ditt valg, velg svaret du ønsker ved a merke av i boksen. Alle spørsmal er formulert pa en lignende mate, for eksempel:*
*0. Ville du foretrukket a bruke 90 minutter pa a implementere et sikkerhetstiltak umiddelbart, eller bruke 100 minutter pa a implementere et sikkerhetstiltak etter 45 dager?*

### Ville du foretrukket å bruke 21 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 60 minutter på å implementere et sikkerhetstiltak etter 14 dager?

21 minutter umiddelbart

60 minutter etter 14 dager

### Ville du foretrukket å bruke 22 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 30 minutter på å implementere et sikkerhetstiltak etter 25 dager?

22 minutter umiddelbart

30 minutter etter 25 dager

### Ville du foretrukket å bruke 110 minutter på å implementere et sikkerhetstiltak

**umiddelbart, eller bruke 140 minutter på å implementere et sikkerhetstiltak etter 35 dager?**

110 minutter umiddelbart

140 minutter etter 35 dager

**Ville du foretrukket å bruke 9,7 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 10 minutter på å implementere et sikkerhetstiltak etter 43 dager?**

9,7 minutter umiddelbart

10 minutter etter 43 dager

**Ville du foretrukket å bruke 3 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 8 minutter på å implementere et sikkerhetstiltak etter 10 dager?**

3 minutter umiddelbart

8 minutter etter 10 dager

**Ville du foretrukket å bruke 13 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 22 minutter på å implementere et sikkerhetstiltak etter 20 dager?**

13 minutter umiddelbart

22 minutter etter 20 dager

**Ville du foretrukket å bruke 176 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 180 minutter på å implementere et sikkerhetstiltak etter 35 dager?**

176 minutter umiddelbart

180 minutter etter 35 dager

**Ville du foretrukket å bruke 2 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 3 minutter på å implementere et sikkerhetstiltak etter 75 dager?**

2 minutter umiddelbart

3 minutter etter 75 dager

**Ville du foretrukket bruke 46 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 53 minutter på å implementere et sikkerhetstiltak etter 45 dager?**

46 minutter umiddelbart

53 minutter etter 45 dager

**Ville du foretrukket å bruke 24 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 39 minutter på å implementere et sikkerhetstiltak etter 70 dager?**

24 minutter umiddelbart

39 minutter etter 70 dager

**Ville du foretrukket å bruke 4 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 5 minutter på å implementere et sikkerhetstiltak etter 25 dager?**

4 minutter umiddelbart

5 minutter etter 25 dager

**Ville du foretrukket å bruke 139 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 160 minutter på å implementere et sikkerhetstiltak etter 50 dager?**

139 minutter umiddelbart

160 minutter etter 50 dager

**Ville du foretrukket å bruke 5 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 11 minutter på å implementere et sikkerhetstiltak etter 10 dager?**

5 minutter umiddelbart

11 minutter etter 10 dager

**Ville du foretrukket å bruke 3 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 4 minutter på å implementere et sikkerhetstiltak etter 20 dager?**

3 minutter umiddelbart

4 minutter etter 20 dager

**Ville du foretrukket å bruke 57 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 59 minutter på å implementere et sikkerhetstiltak etter 55 dager?**

57 minutter umiddelbart

59 minutter etter 55 dager

**Ville du foretrukket å bruke 36 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 46 minutter på å implementere et sikkerhetstiltak etter 50 dager?**

36 minutter umiddelbart

46 minutter etter 50 dager

**Ville du foretrukket å bruke 46 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 80 minutter på å implementere et sikkerhetstiltak etter 20 dager?**

46 minutter umiddelbart

80 minutter etter 20 dager

**Ville du foretrukket å bruke 75 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 120 minutter på å implementere et sikkerhetstiltak etter 70 dager?**

75 minutter umiddelbart

120 minutter etter 70 dager

### Ville du foretrukket å bruke 64 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 100 minutter på å implementere et sikkerhetstiltak etter 35 dager?

64 minutter umiddelbart

100 minutter etter 35 dager

### Ville du foretrukket å bruke 0,9 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 1 minutt på å implementere et sikkerhetstiltak etter 35 dager?

0,9 minutter umiddelbart

1 minutt etter 35 dager

### Ville du foretrukket å bruke 4 minutter på å implementere et sikkerhetstiltak umiddelbart, eller bruke 7 minutter på å implementere et sikkerhetstiltak etter 35 dager?

4 minutter umiddelbart

7 minutter etter 35 dager

## SA-6 questionnaire

Nedenfor finner du seks ulike utsagn. Vennligst svar pa alle utsagnene sa nøyaktig og sannferdig som du kan.

**Jeg oppsøker muligheter for å lære om sikkerhetstiltak som er relevante for meg.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

**Jeg er ekstremt motivert til å ta alle nødvendige steg for å holde mine data og kontoer trygge.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

**Generelt følger jeg aktivt en rutine om sikkerhetspraksis.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

**Jeg er ofte interessert i artikler om sikkerhetstrusler.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

**Jeg følger alltid ekspertenes råd om stegene jeg må ta for å holde mine data og kontoer trygge.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

**Jeg er ekstremt kunnskapsrik om alle stegene som trengs for å holde mine data og kontoer trygge.**

Svært uenig

Uenig

Hverken enig eller uenig

Enig

Svært enig

## Sikkerhetstiltak og beskyttelse mot cyberangrep

Cybersikkerhet er et dynamisk felt hvor det ytre miljøet hele tiden endres pa grunn av nye trusler og sarbarheter. Det betyr at for a opprettholde ønsket/tidligere niva av cybersikkerhet over tid, ma du aktivt utføre noen handlinger pa systemene du bruker. Vennligst angi hvilket alternativ du foretrekker for hvert av de neste 21 valgene: den mindre fordelen na eller den større fordelen etter det angitte antallet minutter.
Svar ærlig pa hvert spørsmal og som om du faktisk tar valget nar du er pa jobb og utfører dine daglige oppgaver.
*For a angi ditt valg, velg svaret du ønsker ved a merke av i boksen. Alle spørsmal er formulert pa en lignende mate, for eksempel:*
*0. Ville du foretrukket beskyttelse mot 90 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 100 potensielt vellykkede cyberangrep etter 45 minutter?*

### Ville du foretrukket beskyttelse mot 656 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 1000 potensielt vellykkede cyberangrep etter 4 minutter?

656 umiddelbart

1000 etter 4 minutter

### Ville du foretrukket beskyttelse mot 43 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 50 potensielt vellykkede cyberangrep etter 10 minutter?

43 umiddelbart

50 etter 10 minutter

### Ville du foretrukket beskyttelse mot 769 potensielt vellykkede cyberangrep

**umiddelbart, eller beskyttelse mot 1000 potensielt vellykkede cyberangrep etter 39 minutter?**

769 umiddelbart

1000 etter 39 minutter

**Ville du foretrukket beskyttelse mot 9,6 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 10 potensielt vellykkede cyberangrep etter 59 minutter?**

9,6 umiddelbart

10 etter 59 minutter

**Ville du foretrukket beskyttelse mot 7 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 10 potensielt vellykkede cyberangrep etter 3 minutter?**

7 umiddelbart

10 etter 3 minutter

**Ville du foretrukket beskyttelse mot 40 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 50 potensielt vellykkede cyberangrep etter 7 minutter?**

40 umiddelbart

50 etter 7 minutter

**Ville du foretrukket beskyttelse mot 985 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 1000 potensielt vellykkede cyberangrep etter 22 minutter?**

985 umiddelbart

1000 etter 22 minutter

**Ville du foretrukket beskyttelse mot 1 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 2 potensielt vellykkede cyberangrep etter 180 minutter?**

1 umiddelbart

2 etter 180 minutter

**Ville du foretrukket beskyttelse mot 42 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 50 potensielt vellykkede cyberangrep etter 60 minutter?**

42 umiddelbart

50 etter 60 minutter

**Ville du foretrukket beskyttelse mot 62 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 150 potensielt vellykkede cyberangrep etter 160 minutter?**

62 umiddelbart

150 etter 160 minutter

**Ville du foretrukket beskyttelse mot 9 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 10 potensielt vellykkede cyberangrep etter 11 minutter?**

9 umiddelbart

10 etter 11 minutter

**Ville du foretrukket beskyttelse mot 534 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 666 potensielt vellykkede cyberangrep etter 80 minutter?**

534 umiddelbart

666 etter 80 minutter

**Ville du foretrukket beskyttelse mot 44 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 50 potensielt vellykkede cyberangrep etter 1 minutt?**

44 umiddelbart

50 etter 1 minutt

**Ville du foretrukket beskyttelse mot 9,6 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 10 potensielt vellykkede cyberangrep etter 5 minutter?**

9,6 umiddelbart

10 etter 5 minutter

**Ville du foretrukket beskyttelse mot 46 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 50 potensielt vellykkede cyberangrep etter 120 minutter?**

46 umiddelbart

50 etter 120 minutter

**Ville du foretrukket beskyttelse mot 65 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 100 potensielt vellykkede cyberangrep etter 100 minutter?**

65 umiddelbart

100 etter 100 minutter

**Ville du foretrukket beskyttelse mot 385 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 500 potensielt vellykkede cyberangrep etter 8 minutter?**

385 umiddelbart

500 etter 8 minutter

**Ville du foretrukket beskyttelse mot 377 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 832 potensielt vellykkede cyberangrep etter 140 minutter?**

377 umiddelbart

832 etter 140 minutter

### Ville du foretrukket beskyttelse mot 289 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 500 potensielt vellykkede cyberangrep etter 46 minutter?

289 umiddelbart

500 etter 46 minutter

### Ville du foretrukket beskyttelse mot 1,8 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 2 potensielt vellykkede cyberangrep etter 30 minutter?

1,8 umiddelbart

2 etter 30 minutter

### Ville du foretrukket beskyttelse mot 1 potensielt vellykkede cyberangrep umiddelbart, eller beskyttelse mot 2 potensielt vellykkede cyberangrep etter 53 minutter?

1 umiddelbart

2 etter 53 minutter

### Takk for din tid og dine svar! Trykk på «Send» for å sende inn.

*Ved a sende inn dette skjemaet samtykker jeg til a delta i denne studien. Jeg forstar at fordi min deltakelse er anonym, kan jeg ikke trekke tilbake samtykket nar jeg har sendt inn svarene mine.*

# Appendix C

# Survey invitation

Dear participant,
My name is Marte, and I am inviting you to participate in a survey that aims to better understand the negative effects of information security controls, policies, and requirements. The target group are employees at all organizational levels in all types of positions.

The survey is part of a 30 ECTS master's thesis in Information Security at NTNU (Norwegian University of Science and Technology). The findings will contribute to the human aspect of security controls to understand employee decision-making.

- The questionnaire takes approximately X minutes to complete.
- Responses are anonymous.

The survey can be displayed in both English and Norwegian. To participate, click on the link directing you to your preferred language.

- Norwegian version: *<link to Nettskjema>*
- English version: *<link to Nettskjema>*

Please complete the questionnaire by 30.04.2023. Do not hesitate to contact me at *<NTNU e-mail address>* if you have any questions and/or wish to be informed about the survey results.

Thank you in advance and thank you for your time!

Best regards,
Marte Marjorie Søgnen

------------------------- Norwegian below -------------------------

Kjære deltaker,
Mitt navn er Marte, og jeg inviterer deg med dette til å delta i en undersøkelse med mål om å bedre forstå de negative effektene av informasjonssikkerhetstiltak, policyer og retningslinjer. Målgruppen er ansatte på alle organisasjonsnivåer i alle typer stillinger.

Undersøkelsen er en del av en 30 stp. masteroppgave i Informasjonssikkerhet ved NTNU (Norges teknisk-naturvitenskapelige universitet). Funnene vil bidra til det menneskelige aspektet ved sikkerhetskontroller for å forstå ansattes beslutningstaking.

- Spørreskjemaet tar omtrent 8-15 minutter å fylle ut.
- Svarene er anonyme.

Undersøkelsen kan vises på både engelsk og norsk. For å delta, klikk på lenken som leder deg til ditt foretrukne språk.

- Norsk versjon: *<link til Nettskjema>*
- Engelsk versjon: *<link til Nettskjema>*

Fyll ut spørreskjemaet innen 30.04.2023. Ikke nøl med å kontakte meg på *<NTNU e-postadresse>* dersom du har spørsmål og/eller ønsker å bli informert om undersøkelsesresultatene.

På forhånd tusen takk og takk for at du tok deg tid!

Med vennlig hilsen,
Marte Marjorie Søgnen

NTNU

Norwegian University of
Science and Technology