Implementation of Information Security Controls Now or Later: Delay Discounting of Losses and Gains*

Marte Søgnen[1 [0009−0000−1189−7835]], Adam Szekeres[1 [0000−0003−0715−5382]], and Einar Snekkenes[1 [0000−0002−2277−6964]]

Department of Information Security and Communication Technology,
Norwegian University of Science and Technology - NTNU,
Gjøvik, Norway
marte.sognen@hotmail.com,
adamszekeres@hotmail.com,
einar.snekkenes@ntnu.no

Abstract. Delay discounting is a behavioral process which explains certain peculiarities of human decision-making when choices and their consequences are separated from each other in time. The concept has been used in psychology and behavioral economics to explain how individuals make sub-optimal choices with undesirable individual and societal consequences. Existing research shows that individuals can be characterized by several discounting parameters (k) across contexts, capturing the rate at which future gains and losses decrease in value as seen from the present. The present paper investigates how the concept of delay discounting can be utilized to better understand human choices regarding the implementation of information security-controls in organizational settings. The study relies on a validated psychometric instrument (MCQ-21) to collect gold-standard k parameters with monetary outcomes. Furthermore, two novel variants are developed to estimate individuals' k parameters with outcomes specific to the information security context. Within the framework of a non-experimental correlational research design, an online survey was distributed among the employees ($n = 135$) of three Norwegian organizations. Contrary to expectations none of the k parameters provided predictive utility as predictors of real-world behavior in organizational settings. Nevertheless, the same behaviors were predicted by an attitude-based measure with an accuracy (adjusted $R^2 = 0.22$), that is observed generally in the literature of behavior prediction using attitudes as predictors. The paper contributes the first results on assessing the utility of delay discounting parameters for behavior prediction within the context of information security.

Keywords: Delay discounting · Information security · Instrument development · Temporal trade-offs · Human decision-making.

* This work was partially supported by the Health Democratization project, funded by the Research Council of Norway, IKTPLUSS program, grant number 288856.

1 Introduction

Information technology's impact on organizations is growing due to digitization, offering enhanced opportunities and efficiency. Despite various advantages, individuals and organizations face novel risks, necessitating robust countermeasures. Information security (IS) - a vital aspect of information technology - aims to mitigate these risks. Unfortunately, organizations often emphasize technical measures over human factors [33], overlooking the fact that employees can represent a significant vulnerability in IS [4, 18, 39]. Despite secure technical components, organizational vulnerability persists if users do not comply with policies. Human decision-making is influenced by various factors like attitudes, IT knowledge, values, personality traits and cognitive biases [30]. Delay discounting (DD) is a behavioral process which has been used to explain temporal dynamics of human decision-making. DD captures how people make trade-offs between immediate and delayed benefits and/or costs. People - in general - tend to favor smaller instant rewards over larger delayed ones [24, 32]. Delayed rewards are discounted by a factor that increases with the length of the delay [2, 19, 37]. The DD parameter denoted by k, quantifies the rate at which future rewards or losses are discounted when viewed from the present [19]. A higher value of k indicates higher impulsivity (i.e. higher degree of present bias). Empirical investigations have demonstrated that the choices of real-world decision-makers are best approximated by a hyperbolic function [21, 32], shown in Equation 1:

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

where V is the discounted present value of a delayed reward, A is the objective amount of the reward, k is an individual's DD parameter and D is the amount of delay until the receipt of the reward/loss (unit of delay may be minutes, hours, days, months, years, etc.).

Figure 1 illustrates preference reversal (i.e. change of preference from a larger delayed reward (LDR) to a smaller earlier reward (SER) with the passage of time). The vertical axis specifies perceived utility (i.e. discounted present value of delayed rewards). The horizontal axis specifies calendar time when the subject is asked to state his perceived utility of SER and LDR as a function of time, defining the subject's utility functions. Notation is as follows:

$V_{\text{SER}}(t), V_{\text{LDR}}(t)$: Perceived utility of SER, LDR respectively at time t.
$t_{\text{SER}}, t_{\text{LDR}}$: Time when subject is to receive SER, LDR respectively. These times are constant, and told to the subject ahead of the experiment.
t_A: Time when the experiment starts.
t_B: Time when preference reversal occurs.

The relative preference of SER vs. LDR is determined by checking the sign of $V_{\text{LDR}}(t) - V_{\text{SER}}(t)$, when $t_A \leq t \leq t_{\text{SER}}$. Note that it is not meaningful to rank the preferences after t_{SER}, as this would be a time when SER has already been given to the subject, thus there is no longer a choice situation. We see that preference

reversal occurs at time t_B. The relationship between the preference reversal graph and the hyperbolic discounting function above can then be expressed as follows:

$$V_{\text{LDR}}(t) = A_{\text{LDR}}/(1 + k * (t_{\text{LDR}} - t))$$
$$V_{\text{SER}}(t) = A_{\text{SER}}/(1 + k * (t_{\text{SER}} - t))$$

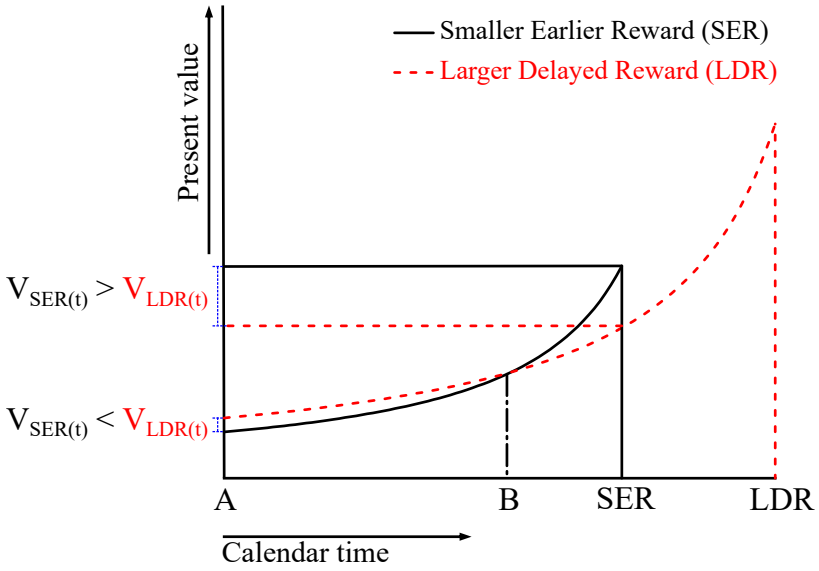

Fig. 1. The concept of hyperbolic DD: the vertical axis represents the discounted present value (perceived utility) of delayed rewards, the horizontal axis represents calendar time when the subject is asked to state his perceived utility of SER and LDR as a function of time. Adapted from [20].

1.1 Problem Statement and Research Questions

While DD has been successfully used in a variety of fields for explaining individual differences in choices [15], the concept has also generated mixed and often contradictory findings [29]. A review of the DD construct and its measures revealed that DD is highly context-dependent, meaning that people use different discounting parameters depending on the outcomes under consideration (e.g. money, health, etc.) [26]. Similarly, a systematic review of the literature found evidence for both state-like and trait-like characteristics of DD [29]. The key finding was that people use different discounting functions across different contexts or domains. Nevertheless, the concept has some degree of stability across contexts: people who discount at a high rate in one context, tend to discount

at a high rate in other contexts as well. These pieces of evidence necessitate the adaptation of existing instruments and the development of new ones to enable the accurate estimation of DD parameters within the context of IS for behavior prediction. Furthermore, instruments are lacking for the measurement of DD parameters in terms of losses within the context of IS, which represents a significant obstacle to the prediction of individuals' choices in real-world settings. Based on these considerations the following research questions (RQs) were formulated:

1.1.1 Research Questions

1: To what extent can individuals' discounting parameter k derived from a validated instrument predict self-reported IS-related behaviors in real-world organizational settings?
2: To what extent can two novel psychometric instruments operationalizing discounting parameter ks adapted to an IS context increase the original instrument's predictive utility?
3: To what extent can individuals' IS attitudes derived from a validated instrument predict self-reported IS-related behaviors in real-world organizational settings?
4: What is the maximum accuracy for predicting self-reported IS-related behaviors in organizational settings using a combination of predictor variables based on demographics, DD and attitudes?

The paper is structured as follows: Section 2 presents existing results about DD in the context of IS, Section 3 presents the sample and instruments for data collection, Section 4 presents the results of the analyses, Section 5 discusses results in the context of existing knowledge, including limitations and future work. Section 6 provides conclusions of the study and Section 7 contains supplemental materials.

2 Related Work

Acquisti [1] highlights DD as a potential factor influencing rational decision-making when individuals make privacy-related choices. Even well-informed, individuals often neglect security measures when present needs outweigh future concerns, leading to a disconnect between security attitudes and behaviors.

In another study, Acquisti & Grossklags [3] investigate information disclosure during online purchases. They examine the role of discounting and its interplay with privacy concerns. Through experiments involving varied rewards, personal information requests, and requester reliability, they uncover that participants discount their personal information's value. This prompts greater information sharing for smaller rewards, an effect amplified among those less privacy-concerned. Notably, privacy concerns can override discounting, as participants aware of privacy risks resist sharing despite higher rewards.

Grossklags & Barradale [16] emphasize the economic evaluation underlying privacy decisions, where investing in security now prevents future breaches. Their

work explores the impatience of individuals across different socioeconomic backgrounds, illuminating the gap between security attitudes and actions.

Mishra & Lalumière [27] delves into the connection between DD, risk-related behaviors, and traits. They unveil context-dependent variations in individuals' risk acceptance, suggesting varied DD rates. Uncertainty plays a pivotal role: people favor immediate rewards under uncertain future conditions and future rewards under uncertain present conditions. Individual differences further modulate rates of DD.

Frik et al. [13] mention the challenge of timing when implementing security controls. People delay costs and expedite benefits, impacting security decisions. Their study reveals preferences for delayed system updates, reflecting convenience concerns. Vaniea & Rashidi [38] find individuals disabling automatic updates due to inconvenient timing.

Rajivan et al. [31] demonstrate, through behavioral economics experiments, that experiencing cyber-attacks leads to underestimation of future risks, influencing suboptimal updating decisions. Despite the best approach being immediate updating, most participants delay or skip updates.

Evaluation of instruments for operationalizing and measuring DD can be found in research papers reviewing the existing literature [26, 29].

3 Methods

This section provides an overview about the sample, selection and development of the instruments utilized in the online survey for data collection and details of data preparation and analysis procedures.

3.1 Sample and Procedure

For the purpose of the study, an online survey was developed and hosted on university servers which provided secure access to the survey for potential participants in possession of the link. The survey was completely anonymous and started with a description of the study's purpose, followed by a mandatory informed consent form before start. The survey link was distributed to contact persons at three small and medium-sized enterprises (SMEs) both from public and private sectors in Norway. The contact persons forwarded the invitation within their organizations reaching approximately 400 employees using non-probabilistic convenience sampling technique. The survey was available in Norwegian and English, the Norwegian translation was completed by one of the authors and the final version was refined following the feedback of a native speaker IS professional.

A total of 135 participants (77 male - 57.0 %, 56 female - 41.5 % and 2 respondents with unspecified gender - 1.5 %) completed the survey resulting in an approximate response rate of 33.25 %. Most participants completed the Norwegian (92.6 %) version of the survey, while 7.4 % of subjects completed it in English. All demographic data collected from respondents is provided in

Table 1. The survey was open for participants for a total of 15 days and the average completion time of the survey was 34.2 minutes (median: 11.4 minutes). Removal of outliers on completion time did not have a significant impact on the results, therefore all 135 participants who completed the entire survey were retained in the final dataset.

Instruments in the online survey were presented in the following blocks in a fixed order: demographic questions, MCQ-21 (original instrument) [21], IS control-related behaviors, DISCQ-L (new instrument), SA-6, DISCQ-G (new instrument). Items within blocks were also presented in a fixed order. The English variant of the whole survey (including all instruments) is provided in Section 7 (Appendix). All analyses were conducted using RStudio (Build 421).

Table 1. Descriptive statistics of sample demographics.

	n	%		n	%
Language			**Occupation**		
Norwegian	125	92.6	Purchasing and logistics	8	5.9
English	10	7.4	Finance	1	0.7
	135	100.0	IT and information security	72	53.3
			HR	1	0.7
Age			Sustainability	0	0.0
18-29	28	20.7	Marketing	3	2.2
30-39	19	14.1	Communication	2	1.5
40-49	35	25.9	Production	2	1.5
50-59	40	29.6	General admin. and support	7	5.2
>60	12	8.9	Healthcare	26	19.3
Prefer not to say	1	0.7	Other	10	7.4
	135	100.0	Prefer not to say	3	2.2
				135	100.0
Gender			**Role**		
Male	77	57.0	Manager	38	28.1
Female	56	41.5	No managerial responsibilities	94	69.6
Prefer not to say	2	1.5	Prefer not to say	3	2.2
	135	100.0		135	100.0

3.2 Measures

3.2.1 Delay Discounting with Monetary Outcomes (MCQ-21)

A slightly modified version of the Monetary Choice Questionnaire (MCQ-21) was utilized to collect responses from participants to calculate their discounting parameter k [21]. The MCQ-21 presents 21 binary choice tasks (trials) to assess

preference between small immediate rewards (SIR) and larger delayed rewards (LDR) in terms of monetary outcomes. MCQ is one of the most commonly used discounting scales in clinical and research settings [19]. In each choice task respondents have to make a choice between a SIR and a LDR across three levels of LDR reward size: 7 small ($30-$35), 7 medium ($55-$65) and 7 large ($70-$85). For each pair of alternatives the value of the k parameter can be calculated for which the discounted value of the LDR is equal to the SIR by rearranging Equation 1 so that k is on the left side of the equation $k = \frac{\frac{A}{V}-1}{D}$. Thus for each trial, the SIR amount corresponding to an indifference point is calculated by the pre-defined k values, which were established for each trial in the original MCQ and remain fixed when using the original instrument. MCQ uses days as units of delay between SIRs and LDRs (range: 10-75 days). The final parameter estimation is based on the 20 bounded ranges of discounting parameter values as explained in [21] and in [19]. A Microsoft Excel-based scoring tool was used to calculate the value of each respondent's discounting parameter k from the raw binary choices assuming a hyperbolic discounting function [19]. The scoring tool provides several metrics at the subject-level and for the sample: consistency metrics, overall k and geomean k (determined by taking the geometric mean of the small, medium, and large k values). Both metrics are available in non-transformed and logarithmic-transformed forms. Since the k values tend to be skewed, the analyses rely on the log-transformed form of the geomean scores for each respondent. Log-transformation turns raw k values from range: (0.0007 to 0.13116) into the range: (-3.15 to -0.88) as no k values measured by the instrument is greater than or equal to 1. A deviation from the original MCQ-21 was that monetary amounts were presented in NOK (Norwegian krone) currency instead of USD by converting all of the original USD amounts to NOK based on the actual currency conversation rates (1 USD = 10.58 NOK [14]) before survey distribution. Thus, the original 1st item of the MCQ (*Would you prefer 30 dollars* ***(SIR)*** *tonight or 85 dollars* ***(LDR)*** *in 14 days****(delay)****?*) resulted in: *Would you prefer 317 NOK tonight, or 899 NOK in 14 days?* in the English version of the survey (see item 1. in section 7.1.3 in the Appendix).

3.2.2 Delay Discounting in the Context of Information Security (DISCQ-L and DISCQ-G)

The Discounting within IS Choice Questionnaire-Loss variant (DISCQ-L) and the Discounting within IS Choice Questionnaire-Gain variant (DISCQ-G) were utilized for collecting the necessary data to quantify discounting parameter ks in an IS context. Both questionnaires were based on the original MCQ-21 due to a lack of scales operationalizing the DD concept in the context of IS. To maintain desirable properties (i.e. construct validity, process for parameter estimation, efficiency) of the original MCQ-21 and its automated scoring tool, both variants rely on the same number of trials and same discounting parameter ks in each trial. The questionnaire instructions, framing of choice trials, delays and reward/loss amounts were adjusted based on considerations relevant for the IS context. During the adaptation of both versions an iterative approach was followed, where

the relevant literature, experts and end-users were consulted in order to reach an optimal format for the instruments. The aim of the adaptation procedure was to identify the most suitable format (including framing, dimensions along which trade-offs occur, units of measurement) for both variants which fulfill key criteria such as: objectively quantifiable and unambiguous dimensions and units of measurement, universal applicability to all kinds of IS controls, applicability to a broad range of stakeholders, considering existing results about user perceptions that facilitate/inhibit adoption of IS-controls for end-users, minimal number of external conditions that the outcomes depend on (i.e. least dependencies other than the end-user's choice in the present), real-world relevance (units provided on a dimension for each item have a matching realistic scenario in the real-world, e.g. time to implement 2fa can be measured in 5-15 minutes of time sacrificed). Options were framed as gains/losses from a reference point which was defined in the questionnaire's instructions as follows: *Cybersecurity is a dynamic field, where the external environment changes constantly due to new threats and vulnerabilities.* For DISCQ-L, instructions continue as follows: *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 DISCQ-G, instructions continue as follows: *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 the DISCQ-L variant, a relevant and unambiguously quantifiable dimension underlying most decisions was determined to be time (i.e. time sacrificed by end-users when implementing/using IS controls) [5, 17]. Minutes (of user effort) were selected as the most appropriate unit of time, as this unit made it possible to express a wide range of loss amounts corresponding to controls with varying levels of required user effort. Following the logic of the original MCQ-21, three ranges of larger delayed losses (LDL)s were defined: small (1-10 minutes), medium (11-59 minutes), large (60-200 minutes). Thus, each category reflects varying levels of effort required for implementing/using control measures (e.g. small loss: entering a PIN, medium: installing software updates, large: education, learning about security controls). Within each category seven values were selected as LDL amounts, which were used to calculate the associated smaller immediate loss (SIL) amounts using the original amount of delays (in days) and the original discounting parameter value ks for each trial. All choice trials used the following format: *Would you prefer to spend 21 minutes **(SIL)** on implementing a security control immediately or spend 60 minutes **(LDL)** on implementing a security control after 14 days **(delay)**?*. As the outcomes of decisions in the IS domain are highly uncertain and depend on a wide range of factors beyond the user's control (e.g. probability of attacks, motivation, skill of attackers, etc.) it is challenging to develop an instrument which can accommodate all the complexities involved in real-world decisions and outcomes. Therefore, the aim was to construct a basic instrument where trade-offs are in the same one dimension (a bit of time sacrificed now vs. more time sacrificed later) without the introduc-

tion of other dimensions (e.g. sacrifice of some user time + loss of certain data with some probability at an uncertain point in the future) that would make the results more ambiguous and more difficult to interpret. DISCQ-L is available in section 7.1.5 in the Appendix.

Since finding a true gain-frame within IS - which is strongly associated with (potential) losses - is challenging, for the DISCQ-G variant, the "protection from a number of potentially successful cyber attacks" was selected as an appropriate (i.e. quantifiable, easy to understand with real-world relevance) dimension quantifying the amount of rewards. Lack of reliable data sources presented a challenge when defining the range of potential LDR amounts representing realistic values. Therefore, three categories (small: 2-10 attacks, medium: 50-150 attacks, large: 500-1000 attacks) were created to cover a wide range of possibilities suitable for decision-makers in various sectors and roles [9, 10, 28, 35]. Amounts of delay were expressed in minutes using each unique LDL amount from DISCQ-L, since they captured realistic estimates about the time needed to implement/use a control measure, thus they are equivalent to the objective amount of delay between maintaining the current level of protection by not doing anything vs. implementing a control and gaining increased protection. Finally, for each choice trial, the associated SIR amounts were pre-calculated using the delay amounts (in minutes) and the original k values. For example item 9 of DISCQ-G (where the amount of delay equals the amount of LDL from item 1 of DISCQ-L) reads as follows: *Would you prefer protection from 42 potentially successful cyber attacks* ***(SIR)*** *immediately, or protection from 50 potentially successful cyber attacks* ***(LDR)*** *after 60 minutes* ***(delay)****?*. DISCQ-G is available in section 7.1.7 in the Appendix.

Raw data was entered from all variants into the original automated scoring tool [19] and the log-transformed geomean scores were used for each respondent in all analyses to enable an unbiased comparison between variants.

3.2.3 Information Security Attitudes (SA-6)

General attitudes about IS were collected by a self-report measure of end-user security attitudes (SA-6) [12]. SA-6 is a validated six-item instrument to quantify end-user IS attitudes, which can be completed in a short time and has demonstrated desirable psychometric properties (i.e. convergent, discriminant and predictive validity, generating sufficient response variance) in the validation study. The six items of SA-6 explore various aspects of IS-related attitudes and respondents are asked to rate their degree of agreement/disagreement with six statements using a 5-point response format (1 = Strongly disagree, 5 = Strongly agree). A total score for attitudes is derived by taking the average of the six item-level scores, where higher scores represent more favourable attitudes toward IS [11]. In the present analysis, the sum of item-level raw scores was used (range: 6-30). The inclusion of SA-6 was motivated by the need to establish a baseline for assessing the predictive performance of the other instruments. Finally, the inclusion of SA-6 was important when considering established findings from several meta-analyses related to the importance of the attitude concept:

attitudes are the most important antecedents of behavioral intentions which are the direct antecedents of behavior in the Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB). TPB represents a state-of-the-art theoretical model for behavior prediction utilized across many domains and attitudes are deemed the most useful predictors of real-world behavior [23, 36]. SA-6 is available in section 7.1.6 in the Appendix.

3.2.4 Information Security Control-Related Behaviors

In order to assess the extent to which the previously discussed constructs can predict real-world behavior, various data collection possibilities were considered in terms of validity and availability. While stated preferences (preferences reported by people) may deviate from revealed preferences (i.e. choices in the real-world) [3], collecting evidence of revealed preferences would have required intrusive data collection methods (providing access to organizational systems) and a high degree of commitment and effort from subjects, which would have negatively impacted response rates. Therefore, the study relies on the elicitation of stated preferences.

The set of questions was designed to elicit responses about past actions / planned future behaviors from subjects. Five well-known IS controls mechanisms were identified (i.e. two-factor authentication, screen lock, password manager, automatic updates and verifying the sender's email address when receiving an e-mail) and a 6-point response format was designed which fulfills requirements for generating data at the ratio level (i.e. values represent an underlying continuum, values are ordered, equal distance between values and 0 represents a true absence of the variable) [8]. Respondents were asked to rate all five IS control mechanisms following the question: *Which of the following options best describe your past actions or future plans regarding the implementation of [control]?* The response format for the options was as follows: *0 - I have not implemented the control. I am not planning to ever implement it. 1 - I have not implemented the control. I am planning to implement it later than this year. 2 - I have not implemented the control. I am planning to implement it this year. 3 - I have implemented the control less than a year ago. 4 - I have implemented the control between a year and 2 years ago. 5 - I have implemented the control more than 2 years ago.* Control was replaced by the name of the specific control mechanisms in each case. Higher scores capture longer times spent with improved protection against potential cyber attacks, lower scores represent the varying levels of behavioral intentions while 0 captures total lack of intention.

Since most of the control-related behavior items exhibited ceiling-effects, the raw scores were summed, generating an overall behavior score metric with range: $(0 - 25)$. The overall behavior scores were used in subsequent analyses. The set of questions operationalizing past experiences / intentions related to IS control-related behaviors is available in section 7.1.4 in the Appendix.

4 Results

This section provides a detailed description of the analyses performed to investigate the quality of the dataset to support comparisons between studies before reporting the results related to each research question.

Overview of descriptive statistics for the k discounting parameters derived from MCQ-21, DISCQ-L and DISCQ-G, total score from SA-6, and overall behavior score from the IS control-related questions are shown in Table 2. The range of values for the three discounting parameter k variants (i.e. k_MCQ-21, k_DISQ-L, k_DISQ-G) are identical since the novel variants are based on the original instrument's internal logic and scoring mechanism to estimate k parameters.

Table 2. Summary of descriptive statistics

Variable	Min	Max	Median	Mean	SD
k_MCQ-21	-3.15	-0.88	-2.06	-2.14	0.69
k_DISQ-L	-3.15	-0.88	-0.88	-1.16	0.53
k_DISQ-G	-3.15	-0.88	-1.92	-1.93	0.83
Total SA-6 score	6.00	30.00	22.00	21.53	4.67
Overall behavior score	0.00	25.00	20.00	19.74	4.76

Abbreviations: k_MCQ-21, k_DISQ-L, k_DISQ-G: geomean of log-transformed k parameters from MCQ-21, DISCQ-L and DISCQ-G, SA-6: Security Attitudes questionnaire.

The item-level and overall distribution of scores for the MCQ-21, DISCQ-L and DISCQ-G are shown in Fig 2.

The lowest DD mean scores were generated by MCQ-21, showing that in terms of monetary outcomes, the sample exhibited a great degree of self-control and respondents rarely selected SIRs over LDRs. Losses in terms of productivity from DISCQ-L generated the highest mean k score signifying that in case of losses people prefer smaller losses sooner than greater losses later. The data provides additional evidence that the general assumption "that underlies most of the models is that realization of a desirable outcome is preferred sooner to later, whereas realization of an undesirable outcome is preferred later to sooner [6]" does not hold in this context. The vast majority of respondents preferred a SIL to a LDL. For DISCQ-G the sample showed greater variance, but the mean k score indicates that respondents were more likely to select an SIR instead of a LDR (higher impulsivity) when the questions are related to IS security controls compared to monetary outcomes.

The distribution of SA-6 scores (item-level and total) is presented in Fig 3. SA-6 demonstrated a high internal consistency as measured by Cronbach's alpha coefficient ($\alpha = .86$), similar to the value ($\alpha = .84$) reported in the questionnaire's validation study [12]. The overall mean score in the present sample cal-

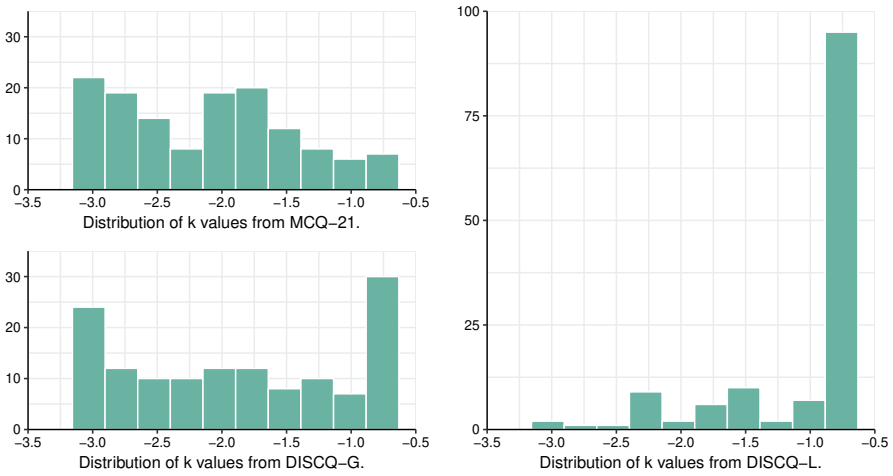

Fig. 2. Distribution of k parameter values from three instruments.

culated according to the original instructions ($M = 3.58$) falls within the range of reference scores (3.57-3.99) obtained in a U.S. sample [11].

The distribution of IS control-related behavior scores (item-level and total) is presented in Fig 4. Most IS control-related questions produced ceiling effects signifying that most of the respondents have already implemented the relevant control measures a long time ago. Screen locks on office equipment were implemented by nearly all respondents more than 2 years ago, whereas verifying a sender's e-mail address and the use of a password manager generated higher variances. Combining the item-level scores into an overall behavior metric resulted in greater variance but a negative skew was still remaining.

The existence of group differences across demographic nominal/ordinal variables and the rest of the variables were investigated with Kruskal-Wallis rank correlation test. It is a rank-based non-parametric test to assess whether there are statistically significant differences between two or more groups of an independent variable on a continuous or ordinal dependent variable.

In terms of the three variants of the log-transformed geomean k scores, no significant differences were detected across the various levels of the demographic variables (i.e. language of survey, age, gender, occupation or role).

With respect to total SA-6 scores, the following differences were identified: males ($M = 22.5$, $SD = 4.60$) had a significantly higher SA-6 total score, than females ($M = 20.1$, $SD = 4.49$) based on the Kruskal-Wallis test $\chi^2(2, N = 133) = 11.25$, $p < .05$. Another difference was detected $\chi^2(10, N = 108) = 33.50$, $p < .001$, such that employees in IT and information security ($M = 23.1$, $SD = 4.33$) had significantly higher SA-6 scores compared to employees in healthcare

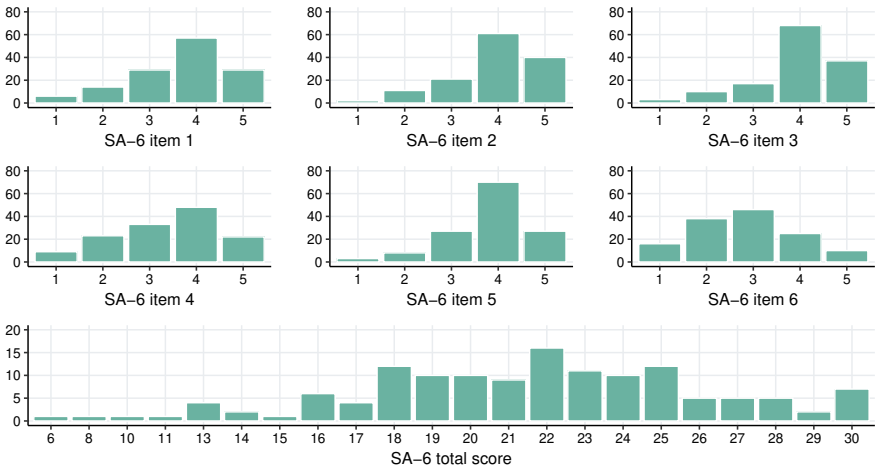

Fig. 3. Distribution of SA-6 item scores and overall SA-6 score.

($M = 19.5$, $SD = 4.47$), and employees in other functions ($M = 18.3$, $SD = 3.59$) as well.

A similar pattern was identified regarding overall behavior scores: there was a significant difference $\chi^2(2, N = 133) = 9.38$, $p < .05$ between males ($M = 20.9$, $SD = 3.96$) and females ($M = 18.2$, $SD = 5.25$). Furthermore, significant differences $\chi^2(10, N = 108) = 29.52$, $p < .05$ were found between IT and information security workers ($M = 21.5$, $SD = 3.80$), employees in healthcare ($M = 17.1$, $SD = 6.34$), and employees in other functions ($M = 16.1$, $SD = 3.14$).

All variables were tested with Shapiro-Wilk normality test and in all cases the variables were significantly different from a normal distribution, therefore Table 3 provides all the zero-order correlations among items and total scores using Spearman's ρ, which is a non-parametric measure of association between variables.

The K scores derived from the original MCQ-21 showed a positive correlation with the k scores from DISCQ-G (.38, $p < .01$). A weak negative correlation (-.25, $p < .01$) was detected between the MCQ-21-derived k scores and the implementation of screen locks. Only the k scores derived from DISCQ-L show correlation with SA-6 total scores (.29, $p < .01$), indicating that out of the three k variants, losses may be closest to capturing similar behavioral tendencies as the attitude-based measure. None of the correlations between the k variants and overall behavior scores were significant, whereas the correlation between overall behavior score and SA-6 total score is among the highest (.48, $p < .001$).

To answer each of the research questions a total of five linear regression models were constructed (four simple linear regression models and one multiple linear regression model). For each model, overall behavior score was entered as

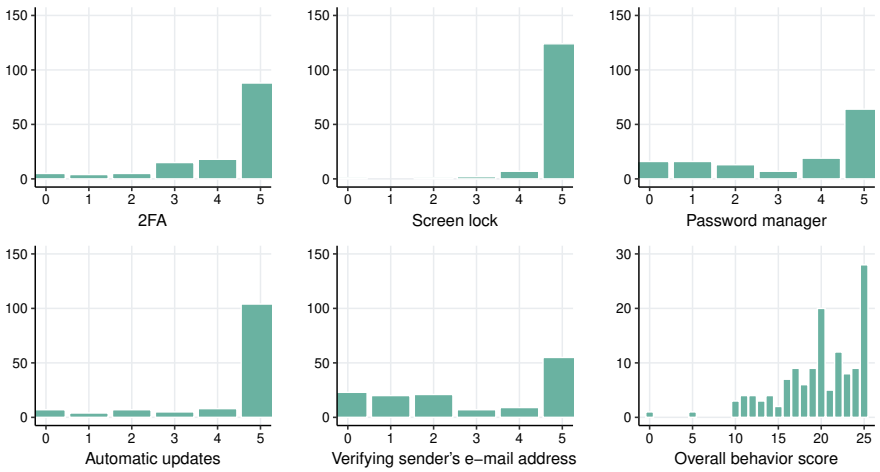

Fig. 4. Distribution of control-related behavior scores for each item and overall behavior score.

the dependent variable to assess the extent to which each independent variable is capable of predicting real-world behaviors individually and in combination. Thus, the first model used the discounting k parameters derived from the original MCQ-21 instrument as a single predictor variable (**RQ 1.**). The second and third models used the discounting k parameters derived from the DISCQ-L and DISCQ-G instruments adapted to an IS context as single predictor variables respectively (**RQ 2.**). The fourth model used SA-6 overall score as a single predictor, as attitudes provide the gold-standard for prediction of behavioral intentions and actual behavior, establishing a baseline for comparison (**RQ 3.**). The fifth model combined all independent variables derived from the instruments with demographic variables to assess the maximum predictive accuracy achievable using the available predictors (**RQ 4.**). The final model was constructed using a stepwise backward method for variable selection. The initial model contained all independent variables and in each step a predictor which did not significantly reduce the Akaike Information Criterion (AIC - a measure of prediction error) metric got removed [40]. The final model which reached the minimal overall prediction error (i.e. lowest AIC score) contained a total of three predictors (i.e. 2 levels of the role demographic variable and SA-6 overall score). Details of the five regression models are presented in Table 4 including the coefficients, error terms and the overall model performance metrics.

None of the simple linear regression models containing the k parameters as sole predictors performed better than an intercept-only model. Thus, the individual contribution of the DD k values for the prediction of real-world IS control-related behaviors in the present sample was zero. The same behaviors

Table 3. Correlations (Spearman's ρ) between instruments and items.

	Overall behavior score	**SA-6 total score**	**k_MCQ-21**	**k_DISQ-L**	**k_DISQ-G**
2FA	**.65*** **	**.35*** **	.01	.10	.13
SL	.16	-.01	**-.25** **	-.06	-.14
PM	**.70*** **	**.32*** **	.09	.09	.05
AU	**.53*** **	**.18***	-.03	.07	.09
VE	**.77*** **	**.40*** **	.02	.11	.10
SA-6_item 1	**.43*** **	**.79*** **	.03	**.25** **	.00
SA-6_item 2	**.36*** **	**.71*** **	.07	**.27** **	.06
SA-6_item 3	**.32*** **	**.70*** **	.07	**.22***	**.21***
SA-6_item 4	**.35*** **	**.84*** **	.08	.12	.02
SA-6_item 5	**.20***	**.62*** **	.06	**.27** **	.12
SA-6_item 6	**.46*** **	**.78*** **	.04	.14	.12
SA-6 total score	**.48*** **	-	-	-	-
k_MCQ-21	.04	.05	-	-	-
k_DISQ-L	.13	**.29** **	-.05	-	-
k_DISQ-G	.09	.08	**.38*** **	.08	-

*$p < .05$, **$p < .01$, ***$p < .001$.
Abbreviations: 2FA: two-factor authentication, SL: screen lock, PM: password manager, AU: automatic updates, VE: verifying e-mail sender, SA-6: Security Attitudes questionnaire, k_MCQ-21, k_DISQ-L, k_DISQ-G: geomean of log-transformed k parameters from MCQ-21, DISCQ-L and DISCQ-G.

were predicted by security-related attitudes (i.e. overall SA-6 score) significantly better, reaching an overall of 0.22 in terms of the adjusted R^2 metric. Adjusted R^2 is a more appropriate metric for model fit than R^2 as it penalizes a model with more predictors, whereas R^2 automatically increases by the inclusion of more predictor variables [34]. The final combined predictive model achieved an adjusted R^2 score of 0.25, which represents a small significant improvement compared to the fourth model by the inclusion of the role variable. Specifically, respondents with/without managerial responsibilities are significantly different from the reference group (prefer not to say). The independent variables collectively account for 25% of the variance in the dependent variable without any significant contribution from any of the DD k parameters.

5 Discussion

The present study aimed at exploring the effects of DD on end-users' IS control-related behaviors in real-world organizational settings in order to contribute to knowledge within the field of IS. The study used a validated psychometric instrument, MCQ-21, to first derive each participant's gold-standard discounting factors. Evidence from the literature indicates that DD has a high degree of context-dependence (i.e. instead of using a single discounting parameter for

Table 4. Summary of five regression models for predicting overall behavior scores.

DV: Behavior score		Regression			Residuals			Overall model performance		
	IVs	β	*S.E.* β	t	*df*	*S.E.*	*df*	F	R^2	Adj. R^2
Model 1	constant	20.22	1.35	**15.02*** **	1	4.77	133	0.14	0.00	-0.01
	k_MCQ-21	0.22	0.60	0.37						
Model 2	constant	20.56	0.99	**20.84*** **	1	4.76	133	0.84	0.01	-0.00
	k_DISQ-L	0.71	0.77	0.92						
Model 3	constant	20.71	1.04	**19.98*** **	1	4.76	133	1.04	0.01	0.00
	k_DISQ-G	0.51	0.49	1.02						
Model 4	constant	9.45	1.72	**5.50*** **	1	4.22	133	**37.63*** **	**0.22**	**0.22**
	sa-6	0.48	0.08	**6.13*** **						
Model 5	constant	3.19	2.89	1.10	3	4.13	131	**15.49*** **	**0.26**	**0.25**
	role 1	6.21	2.48	**2.51***						
	role 2	6.55	2.42	**2.70** **						
	sa-6	0.48	0.08	**6.22*** **						

$^*p < .05$, $^{**}p < .01$, $^{***}p < .001$.
Abbreviations: DV: dependent variable, IVs: independent variables, S. E.: standard error, k_MCQ-21, k_DISQ-L, k_DISQ-G: geomean of log-transformed k parameters from MCQ-21, DISCQ-L and DISCQ-G, SA-6: total score from Security Attitudes questionnaire.

temporal decisions across all contexts, people tend to evaluate future gains and losses differently across contexts), necessitating the development of instruments capturing the objective trade-offs unique within the IS domain. Thus, two new instruments have been developed, taking the validated psychometric instrument as a starting point for the development. The work focused on addressing certain limitations related to the original MCQ-21 (i.e. lack of transferability between various contexts), while aiming to maintain its desirable properties (e.g. precision of parameter estimation, construct validity, wide-range adoption). Another limitation of MCQ-21 is that it focuses only on gains (i.e. rewards), thus quantifying the discounted present value of potential losses is not achievable with the original instrument. The development of the new instruments aimed at specifying objective gains and focusing on objectively quantifiable losses, based on the literature of user perceptions related to IS control implementation. As a baseline measure for predictive performance, additional data was collected by SA-6, an instrument for capturing attitudes which are assumed to be the strongest predictors of behavioral intentions and subsequent behaviors according to state-of-the-art knowledge from the wider domain of psychology of behavior prediction [23, 36]. Behavioral data was collected by eliciting previous experience / implementation intentions regarding five basic IS controls through self-reports in organizational settings.

Results show that employees of three Norwegian SMEs have a great degree of patience demonstrated by overall low discounting scores as measured by the MCQ-21. The implementation of five fundamental IS controls were investigated based on expert advice and recommended best practices. The results show that the sample had a high average overall behavior score signifying that almost all of the participants implemented most of the controls a long time ago in

their organizations. The overall low average discounting score and high overall behavior scores are consistent with expectations based on the theory of DD: people with low discounting scores tend to make more optimal choices [25, 26].

Analyses of MCQ-21, and the two novel adapted versions (i.e. DISCQ-L, and DISCQ-G) indicate differences in discounting rates among the three versions suggesting the degree of convergent validity (the extent to which instruments measure the same concept) and discriminant validity (the extent to which instrument measure different concepts) [7]. Specifically, the results from DISCQ-L reveal that individuals tend to favor smaller immediate losses over larger delayed losses. Respondents showed a preference for minimizing the time lost due to the implementation of IS controls. These findings contradict the assumptions that people typically prefer an undesirable outcome later to sooner [6], and that people delay implementing security controls [13, 31, 38], when IS controls are framed as potential losses. Spearman's correlation analyses revealed an insignificant negative correlation between MCQ-21 and DISCQ-L suggesting that there was no meaningful linear relationship between these two instruments. DISCQ-G showed a positive correlation with MCQ-21 (.38, $p < .01$), which could indicate the trait-like characteristic of the DD concept (i.e. people who discount at a high rate in one context, discount at a high rate also in other contexts) [29]. Additionally, with respect to attitudes, DISCQ-L showed a weak positive correlation (.29, $p < .01$) with SA-6, indicating that avoidance of losses (in terms of time and productivity) is more strongly associated with behaviors and attitudes than the prospect of gains (in terms of security). Thus, it may be meaningful to focus on losses (of time and productivity) due to the implementation of IS controls when trying to motivate behaviors with desirable outcomes.

Regarding the research questions, results are as follows: the analyses related to RQ 1. and RQ 2. indicate that none of the DD parameters derived from the three instruments (MCQ-21, DISCQ-L, DISCQ-G) turned out to be useful predictors of self-reported IS-related real-world behavior in the present sample. This is demonstrated by the fact that none of the simple linear regression models using discounting parameter ks performed better than an intercept-only model.

However, with respect to RQ 3., the attitude-based measure (SA-6) was found to be a significantly better predictor (0.22 in terms of Adjusted R^2) of self-reported IS-related real-world behavior compared to discounting parameters.

Finally, with respect to RQ 4. the combination of all independent variables resulted in a predictive model in which the attitude-based measure (SA-6) and two fixed values of one demographic variable in combination improved the overall predictive accuracy from 0.22 to 0.25 according to the Adjusted R^2 metric. It is important to acknowledge that feature selection without adequate testing for overfitting can introduce risks and potentially yield spurious results. Such scenarios may necessitate further validation.

As some of the results contradict expectations based on existing results (i.e. lack of association of discounting parameters and real-world behaviors) while some of the results fulfill expectations (i.e. attitudes are strongly associated

with with real-world behaviors), it is important to investigate limitations of the present study and to provide suggestions for further work.

5.1 Limitations

A main limitation of the present study is related to data quality. Due to the highly skewed control-related behavior scores, a follow-up questionnaire was sent to the three contact persons at the organizations to gain a better understanding of the existing IS policies and regulations. Response was received months after the initial data collection from two organizations. Based on the responses, it became evident that most of the IS controls were set up as default settings for all employees in the organizations. Two controls were exceptions to this (i.e. password manager and verifying the sender's e-mail address) which generated the highest variances among control-related behaviors. These pieces of information explain the highly skewed IS control variables and may explain the DD concept's lack of predictive utility. In addition, it should be noted that a significant proportion of respondents (53.3%) belonged to the IT and IS professions. Consequently, caution is warranted when generalizing the findings of this study to the broader population of employees within SMEs due to the potential selection bias inherent in the sampled population.

It is worth noting that the concept of DD has generated a variety of research results, often with mixed or contradicting findings. Several instruments have been developed to derive discounting factors, which often make comparisons between studies problematic [26]. It is important to have standardized, collectively established criteria for the evaluation of instruments operationalizing the constructs. This study used MCQ-21 which is regarded a state-of-the-art instrument developed for research purposes in a clinical setting. However, as the instruments developed and presented in this study relied on MCQ-21, they could have inherited some of the weaknesses of the original instrument. Respondent groups in a study providing external validity of MCQ-21 were substance abusers and healthy controls [22]. The requirements in terms of sensitivity and specificity for an instrument which aims to distinguish between people with substance abuse disorders and healthy controls may be different than the sensitivity and specificity requirements of an instrument which aims to distinguish between high and low discounters in an IS context from the healthy general population. Thus, the novel instruments presented in this paper may require further improvements in terms of their sensitivity and specificity.

5.2 Future Work

In order to overcome the limitations in the present study and to better disentangle the DD construct's utility for predicting real-world IS control-related behaviors, various possibilities may be considered.

A replication study in a private context using the instruments presented here could provide evidence whether DD has more relevance when people have more freedom to act according to their own preferences. Thus, it would be important

to investigate whether DD has stronger association with real-world behavior in settings where organization-wide default settings related to IS controls are lacking. However, such a study also needs to consider various default settings and policies existing at service providers which people interact with frequently.

A probabilistic sampling method needs to be implemented to generate representative samples in order to improve the generalizability of the findings to all SMEs and other organizations.

The use of non-reactive (i.e. not relying on self-reports and direct interaction with participants), observational measures represents a crucial task for future studies. Such measures could rely on logs at the organizations or on private devices but would require a careful assessment of privacy implications and its impact on respondents' willingness to provide access to such data.

Finally, due to the highly dynamic nature of the IS field (i.e. evolving threats, novel vulnerabilities, new controls, etc.) it is highly unlikely that the same controls (which were investigated in the present study) will be regarded as best practice in a few years. To achieve reliable predictions about adaptive human behavior in a dynamic environment it is crucial to identify invariant features of the entire system. At the conceptual level of constructs, attitudes and DD may represent potential invariant constructs depending on their level of cross-cultural applicability. When invariant constructs are identified at the conceptual level, the task of accurately assessing the local parameters associated with the constructs (i.e. at the level of individuals or organizations) still remains. Therefore, further studies are needed to 1.) discover other invariant constructs at the conceptual level and 2.) develop instruments that can reliably assess parameters of the constructs.

6 Conclusion

The main purpose of this paper was to explore how the construct of DD can be utilized to predict end-users' IS control-related behavior in organizational settings. The DD concept has been used successfully to explain individual differences related to temporal trade-off decisions with various outcomes (e.g. monetary health, addiction, exercise, etc.), but there are also inconsistencies and mixed findings in the literature. Furthermore, there is a scarcity of investigations related to the links between DD and real-world IS control-related decisions. Therefore, this study provided a general overview about the concept of DD, its use in various contexts, existing results about its use in explaining IS-related behaviors.

The study measured individual's discounting factors by a validated psychometric instrument and developed two novel variants to capture context-specific details relevant in the field of IS. The predictive performance of the three instruments were assessed against an attitude-based measure, which represents the most useful construct for behavior prediction based on the literature.

Several findings are in line with expectations based on existing literature, such as attitudes being the best performing predictors of behaviors; low aver-

age discounting scores detected in the sample concurrently with high levels of compliance with IS security best practices - signifying that the results are not self-contradictory as people who have low DD k parameters tend to make more optimal choices in general, thus they might make more optimal IS-related decisions as well, compared to high discounters. However, some important results challenge prevailing views about DD, such as lack of detectable predictive power. DD seems to be a useful explanatory variable, but its predictive utility in organizational contexts (where default IS settings are enforced) is negligible. The results suggests that employees highly value their time, particularly concerning potential losses in workflow or productivity at work, as evidenced by their predominant preference for the smaller immediate loss options. The avoidance of losses (i.e. avoiding spending more time later on implementing a security control, but not in terms of losses due to potential data breaches) appears to be a more compelling motivator than the pursuit of gain (in terms of improved security).

7 Appendix

7.1 Delay discounting in an information security context (Survey)

7.1.1 Introduction

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 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. You are also welcome to distribute the survey to colleagues or people working in other organizations.

7.1.2 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.

1. **What is your age range?**
   - 18-29
   - 30-39
   - 40-49
   - 50-59
   - 60 or older
   - I prefer not to say
2. **What is your gender?**
   - Male
   - Female
   - Other
   - I prefer not to say
3. **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). Please specify your current occupation here:
   - I prefer not to say
4. **Which of the following best describes your role in the organization you currently work in?**
   - Manager
   - No managerial responsibilities
   - I prefer not to say

7.1.3 Monetary Choice Questionnaire (MCQ-21)

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?

1. **Would you prefer 317 NOK tonight, or 899 NOK in 14 days?**
   – 317 NOK tonight
   – 899 NOK in 14 days
2. **Would you prefer 423 NOK tonight, or 582 NOK in 25 days?**
   – 423 NOK tonight
   – 582 NOK in 25 days
3. **Would you prefer 709 NOK tonight, or 899 NOK in 35 days?**
   – 709 NOK tonight
   – 899 NOK in 35 days
4. **Would you prefer 360 NOK tonight, or 370 NOK in 43 days?**
   – 360 NOK tonight
   – 370 NOK in 43 days
5. **Would you prefer 159 NOK tonight, or 370 NOK in 10 days?**
   – 159 NOK tonight
   – 370 NOK in 10 days
6. **Would you prefer 338 NOK tonight, or 582 NOK in 20 days?**
   – 338 NOK tonight
   – 582 NOK in 20 days
7. **Would you prefer 878 NOK tonight, or 899 NOK in 35 days?**
   – 878 NOK tonight
   – 899 NOK in 35 days
8. **Would you prefer 222 NOK tonight, or 317 NOK in 75 days?**
   – 222 NOK tonight
   – 317 NOK in 75 days
9. **Would you prefer 508 NOK tonight, or 582 NOK in 45 days?**
   – 508 NOK tonight
   – 582 NOK in 45 days
10. **Would you prefer 423 NOK tonight, or 687 NOK in 70 days?**
    – 423 NOK tonight
    – 687 NOK in 70 days
11. **Would you prefer 264 NOK tonight, or 370 NOK in 25 days?**
    – 264 NOK tonight
    – 370 NOK in 25 days
12. **Would you prefer 687 NOK tonight, or 793 NOK in 50 days?**
    – 687 NOK tonight
    – 793 NOK in 50 days
13. **Would you prefer 254 NOK tonight, or 582 NOK in 10 days?**
    – 254 NOK tonight
    – 582 NOK in 10 days
14. **Would you prefer 317 NOK tonight, or 370 NOK in 20 days?**
    – 317 NOK tonight
    – 370 NOK in 20 days
15. **Would you prefer 561 NOK tonight, or 582 NOK in 55 days?**
    – 561 NOK tonight
    – 582 NOK in 55 days
16. **Would you prefer 497 NOK tonight, or 635 NOK in 50 days?**
    – 497 NOK tonight

   - 635 NOK in 50 days
17. **Would you prefer 423 NOK tonight, or 740 NOK in 20 days?**
   - 423 NOK tonight
   - 740 NOK in 20 days
18. **Would you prefer 529 NOK tonight, or 846 NOK in 70 days?**
   - 529 NOK tonight
   - 846 NOK in 70 days
19. **Would you prefer 476 NOK tonight, or 740 NOK in 35 days?**
   - 476 NOK tonight
   - 740 NOK in 35 days
20. **Would you prefer 286 NOK tonight, or 317 NOK in 35 days?**
   - 286 NOK tonight
   - 317 NOK in 35 days
21. **Would you prefer 169 NOK tonight, or 317 NOK in 35 days?**
   - 169 NOK tonight
   - 317 NOK in 35 days

7.1.4 The implementation of security controls (Information Security Control-Related Behaviors)

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.

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.

7.1.5 Security controls and loss of productivity or workflow (DISCQ-L)

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?

1. **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
2. **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
3. **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
4. **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
5. **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
6. **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
7. **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

8. **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
9. **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
10. **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
11. **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
12. **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
13. **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
14. **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
15. **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
16. **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

17. **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
18. **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
19. **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
20. **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
21. **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

7.1.6 Security attitudes questionnaire (SA-6)

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

1. **I seek out opportunities to learn about security measures that are relevant to me.**
    - Strongly disagree
    - Disagree
    - Neither agree nor disagree
    - Agree
    - Strongly agree
2. **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
3. **Generally, I diligently follow a routine about security practices.**
    - Strongly disagree

   - Disagree
   - Neither agree nor disagree
   - Agree
   - Strongly agree
4. **I often am interested in articles about security threats.**
   - Strongly disagree
   - Disagree
   - Neither agree nor disagree
   - Agree
   - Strongly agree
5. **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
6. **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

7.1.7 Security controls and protection against cyber attacks (DISCQ-G)

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?

1. **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

2. **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
3. **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
4. **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
5. **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
6. **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
7. **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
8. **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
9. **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
10. **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

11. **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
12. **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
13. **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
14. **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
15. **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
16. **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
17. **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
18. **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
19. **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

20. **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
21. **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

7.1.8 Closure

Thank you for your time and answers! Click Send 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.***

References

1. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proc. of the 5th ACM conf. on Electronic commerce. pp. 21–29 (2004)
2. Acquisti, A., Grossklags, J.: Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In: 2nd Annual WEIS. vol. 3, pp. 1–27. Citeseer (2003)
3. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE security & privacy **3**(1), 26–33 (2005)
4. Ahmed, M., Sharif, L., Kabir, M., Al-Maimani, M.: Human errors in information security. International Journal **1**(3), 82–87 (2012)
5. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Proceedings of the 2008 new security paradigms workshop. pp. 47–58 (2008)
6. Benzion, U., Rapoport, A., Yagil, J.: Discount rates inferred from decisions: An experimental study. Management science **35**(3), 270–284 (1989)
7. Campbell, D.T., Fiske, D.W.: Convergent and discriminant validation by the multitrait-multimethod matrix. Psychological bulletin **56**(2), 81 (1959)
8. Carifio, J., Perla, R.J.: Ten common misunderstandings, misconceptions, persistent myths and urban legends about likert scales and likert response formats and their antidotes. Journal of social sciences **3**(3), 106–116 (2007)
9. DNB: Annual report 2022 (2023), https://www.dnb.no/portalfront/nedlast/no/om-oss/samfunnsansvar/2022/2022-CDC_Annual_Report_v1.0.pdf, last accessed 20 March 2023
10. European Commission: Europeans' attitudes towards cyber security (2020), https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1, last accessed 23 August 2023
11. Faklaris, C., Dabbish, L., Hong, J.I.: SA-6 handout (2019), https://socialcybersecurity.org/files/SA6handout.pdf, last accessed 23 August 2023

12. Faklaris, C., Dabbish, L., Hong, J.I.: A self-report measure of end-user security attitudes (SA-6). In: Proc. of the 15th Symp. on Usable Privacy and Security (SOUPS). pp. 61–77. USENIX Association, Berkeley, CA. (2019)
13. Frik, A., Egelman, S., Harbach, M., Malkin, N., Peer, E.: Better late (r) than never: increasing cyber-security compliance by reducing present bias. In: Symposium on Usable Privacy and Security. pp. 12–14 (2018)
14. Google: Amerikansk dollar til norsk krone (2023), https://www.google.com/finance/quote/USD-NOK?sa=X&sqi=2&ved=2ahUKEwjE2I_C9aH-AhVP6CoKHZQtDh0QmY0JegQICBAd&window=1M, last accessed 11 April 2023
15. Green, L., Myerson, J.: A discounting framework for choice with delayed and probabilistic rewards. Psychological bulletin **130**(5), 769 (2004)
16. Grossklags, J., Barradale, N.J.: Social status and the demand for security and privacy. In: PETs: 14th Int. Symp., Amsterdam. pp. 83–101. Springer (2014)
17. Herley, C.: 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. pp. 133–144 (2009)
18. Hughes-Lartey, K., Li, M., Botchey, F.E., Qin, Z.: Human factor, a critical weak point in the information security of an organization's internet of things. Heliyon **7**(3), e06522 (2021)
19. Kaplan, B.A., Amlung, M., Reed, D.D., Jarmolowicz, D.P., McKerchar, T.L., Lemley, S.M.: Automating scoring of delay discounting for the 21-and 27-item monetary choice questionnaires. The Behavior Analyst **39**(2), 293–304 (2016)
20. Kirby, K.N., Herrnstein, R.J.: Preference reversals due to myopic discounting of delayed reward. Psychological science **6**(2), 83–89 (1995)
21. Kirby, K.N., Maraković, N.N.: Delay-discounting probabilistic rewards: Rates decrease as amounts increase. Psychonomic bulletin & review **3**(1), 100–104 (1996)
22. Kirby, K.N., Petry, N.M., Bickel, W.K.: Heroin addicts have higher discount rates for delayed rewards than non-drug-using controls. Journal of Experimental psychology: general **128**(1), 78 (1999)
23. Kraus, S.J.: Attitudes and the prediction of behavior: A meta-analysis of the empirical literature. Personality and social psychology bulletin **21**(1), 58–75 (1995)
24. Kurz, C.F., König, A.N.: Predicting time preference from social media behavior. Future Generation Computer Systems **130**, 155–163 (2022)
25. Loewenstein, G.F.: Frames of mind in intertemporal choice. Management science **34**(2), 200–214 (1988)
26. Matta, A.d., Gonçalves, F.L., Bizarro, L.: Delay discounting: Concepts and measures. Psychology & Neuroscience **5**, 135–146 (2012)
27. Mishra, S., Lalumière, M.L.: Associations between delay discounting and risk-related behaviors, traits, attitudes, and outcomes. Journal of Behavioral Decision Making **30**(3), 769–781 (2017)
28. NTB: Oljefondet utsettes for tre alvorlige dataangrep daglig (2022), https://www.digi.no/artikler/oljefondet-utsettes-for-tre-alvorlige-dataangrep-daglig/521643, last accessed 23 August 2023
29. Odum, A.L., Becker, R.J., Haynes, J.M., Galizio, A., Frye, C.C., Downey, H., Friedel, J.E., Perez, D.: Delay discounting of different outcomes: Review and theory. Journal of the experimental analysis of behavior **113**(3), 657–679 (2020)
30. Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R., Jerram, C.: The influence of organizational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making **9**(2), 117–129 (2015)

31. Rajivan, P., Aharonov-Majar, E., Gonzalez, C.: Update now or later? effects of experience, cost, and risk preference on update decisions. Journal of Cybersecurity **6**(1) (2020)
32. Reynolds, B., Schiffbauer, R.: Measuring state changes in human delay discounting: an experiential discounting task. Behavioural processes **67**(3), 343–356 (2004)
33. Schlienger, T., Teufel, S.: Information security culture. In: Security in the Information Society, pp. 191–201. Springer (2002)
34. Shieh, G.: Improved shrinkage estimation of squared multiple correlation coefficient and squared cross-validity coefficient. Organizational Research Methods **11**(2), 387–407 (2008)
35. Snape, G.: People being proactive about their personal cyber risks, but poor behaviors remain – survey (2022), https://www.insurancebusinessmag.com/us/news/cyber/people-being-proactive-about-their-personal-cyber-risks-but-poor-behaviors-remain--survey-427250.aspx, last accessed 20 March 2023
36. Sutton, S.: Predicting and explaining intentions and behavior: How well are we doing? Journal of applied social psychology **28**(15), 1317–1338 (1998)
37. Szekeres, A., Snekkenes, E.A.: Inferring delay discounting factors from public observables: Applications in risk analysis and the design of adaptive incentives. In: Proc. of the 5th CHIRA conference. SciTePress (2021)
38. Vaniea, K., Rashidi, Y.: Tales of software updates: The process of updating software. In: Proceedings of the 2016 chi conference on human factors in computing systems. pp. 3215–3226 (2016)
39. Wood, C.C., Banks Jr, W.W.: Human error: an overlooked but significant information security problem. Computers & Security **12**(1), 51–60 (1993)
40. Zhang, Z.: Variable selection with stepwise and best subset approaches. Annals of translational medicine **4**(7) (2016)