Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment

Molin, Eric; Meeuwisse, Kirsten; Pieters, Wolter; Chorus, Caspar

DOI
10.1016/j.cose.2018.03.003

Publication date
2018

Document Version
Final published version

Published in
Computers and Security

Citation (APA)
Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers and Security*, *77*, 65-78. https://doi.org/10.1016/j.cose.2018.03.003

COMPUTERS & SECURITY 77 (2018) 65–78

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment

Eric Molin[a,*], *Kirsten Meeuwisse*[b], *Wolter Pieters*[c], *Caspar Chorus*[d]

[a] *Engineering Systems and Services Department, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands*
[b] *Cyber Security, Deloitte, Amsterdam, The Netherlands*
[c] *Values, Technology and Innovation Department, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands*
[d] *Engineering Systems and Services Department, Faculty of Technology, Policy and Management, Delft University of Technolog, Delft, The Netherlands*

ARTICLE INFO

Article history:
Received 28 May 2017
Revised 16 February 2018
Accepted 18 March 2018
Available online 6 April 2018

Keywords:
Information security
Security measures
Security perception
Usability perception
Discrete choice experiments
Discrete choice models
Employees' preferences

ABSTRACT

It is often suggested in the literature that employees regard technical security measures (TSMs) as user-unfriendly, indicating a trade-off between security and usability. However, there is little empirical evidence of such a trade-off, nor about the strength of the associated negative correlation and the importance employees attach to both properties. This paper intends to fill these knowledge gaps by studying employees' trade-offs concerning the usability and security of TSMs within a discrete choice experiment (DCE) framework. In our DCE, employees are asked to indicate the most preferred security packages that describe combinations of TSMs. In addition, security and usability perceptions of the security packages are explicitly measured and modelled. The models estimated from these observed responses indicate how each TSM affects perceived security, perceived usability and preference. The paper further illustrates how the modelling results can be applied to design highly secure packages that are still preferred by employees. The paper also makes a methodological contribution to the literature by introducing discrete choice experiments to the field of information security.

1. Introduction

More than 40 million cybersecurity incidents are reported every year, and the damage done by cybercrime to the private sector is estimated to amount to hundreds of billions of euros every year (ISACA and RSA Conference, 2015; Gandal, 2015). These numbers indicate that information security is of utmost importance for companies. Companies protect themselves from data breaches and cyberattacks by implementing a range of technical security measures (TSMs). If employees use these measures as intended, more stringent security measures would by design result in higher levels of security, although they may have a negative impact on productivity. However, if employees perceive those measures as less usable they may find ways to circumvent them, which potentially makes them less or even counter-effective (Dinev et al., 2006; Kirlappos et al., 2015; Post and Kagan, 2007). For example, if employees are forced to change their password every week, they may write down their passwords on post-its attached to their desk. Although it is usually the companies' Chief Information Secu-

* Corresponding author.
E-mail address: e.j.e.molin@tudelft.nl (E. Molin).
https://doi.org/10.1016/j.cose.2018.03.003

rity Officer (CISO) who makes the decisions on technical security measures, it is the compliance behaviour of the employees that largely determines the resulting level of the company's cyber- or information security.

CISO's thus have to make complicated decisions, involving not only security, but also cost (limited budget), usability, and impact on productivity, and the success of their decisions partly depends on the preferences and behaviour of the employees. It is often suggested (see literature review in the next section) that the most secure measures are perceived by employees as particularly user-unfriendly, suggesting that CISO's have to make a trade-off in this regard. But there is in fact little empirical evidence about whether such a trade-off exists, nor about the strength of this correlation. Furthermore, it is unknown what importance employees attach to (perceived) security and (perceived) usability of information security measures. This makes it hard for CISOs to select those technical measures that provide a high level of security but still are considered sufficiently usable, enabling effective security deployment. Therefore, it is important to study the employees' behaviour, in particular in relation to the supposed trade-off between the security of such measures and their usability. This can be done within the framework of discrete choice theory (DCT) and discrete choice experiments (DCE), which is particularly suitable to study trade-offs. To this best of our knowledge, this method of data collection (DCE) and analysis (DCT) has not been used before in the context of cyber- or information security.

This paper intends to fill the above described knowledge gap by empirically studying employees' trade-offs concerning the usability and security of information security measures within a DCE framework. In our DCE employees are asked to provide responses to hypothetical security packages describing combinations of technical security measures. Our approach is more sophisticated than the usual experimental set up used for choice analysis, in the sense that – in addition to observing choices among those security packages – we also explicitly measure and model perceptions concerning the security packages in terms of security and usability. Data are collected using an on-line experiment which was completed by a sample of 230 employees. The insights the application of this methodology reveals can be used by system administrators to choose security measures that are perceived to be usable and may increase compliance behaviour.

The next section discusses related work; after that, we provide a conceptual framework and derive research questions. Subsequently, the construction of the experiment, the data collection and the model estimation procedures are explained. This is followed by a presentation and discussion of the results of the estimated models, including implications for practice. Finally, the results are discussed in light of the literature and avenues for further research are discussed.

2. Related work

Information security research started out with devising technical solutions to protect information. Such solutions would not always take usability into account. Instead, the main focus was on making the technology "work", and on making users comply with the technology-imposed usage requirements. In a sense, there was an adversarial relation with the user, who had to be "changed" in order to fit with the technological design. In a seminal paper, Adams and Sasse (1999) pointed out that "users are not the enemy": designs would need to take the user experience into account (user-centred design) in order to be effective.

Still, the relation between security and usability remained unclear. Schultz (2007) already stated that "although numerous authors have argued for the need to pay more attention to usability considerations in information security, relatively few papers present empirical results on the relationship between usability and information security." It is often claimed that security and usability are two conflicting goals: improving one will negatively affect the other (Andersson, 2013; Kainda et al., 2010; Nurse et al., 2011). The assumed relation is a negative correlation: if security goes up, usability goes down and if usability goes up security goes down. Consider a computer without password protection. It is clearly usable, but not secure. On the other hand, a computer on which you have to authenticate yourself every five minutes by providing your password could be very secure, but not user-friendly at all; users are likely to be unwilling to use such a computer (Cranor and Garfinkel, 2004).

Herley (2009) analysed the motivation of employees to comply with security measures in terms of costs and benefits, a notion which is more broadly supported by the well-known Technology Acceptance Model (Davis, 1986; Venkatesh and Davis, 2000). He argues that employees' perception of the benefits associated with (complying with) a cyber security measure depends on the extent to which they perceive it to actually contribute to security. He defines perceived costs in terms of the effort it takes employees to comply: the more effort it takes, the less a measure is perceived to be user friendly or 'usable'. Similarly, Beautement et al. (2009) describe a model in which employees make a cost-benefit analysis in relation to the (non-)encryption of USB sticks for data transfer, and associated confidentiality and availability risks. But the idea of a general trade-off between security and usability is disputed. For example, Caputo et al. (2016) use three case studies showing that a trade-off does not always exist.

In any case, there is a consensus on the need to consider usability when designing security solutions. In this line of research, many papers have argued for different approaches to taking usability into account in the design of security technology. In such approaches, the focus is on the design, thus what is required of design methods in order to lead to usable designs. Gutmann and Grigg (2005) discussed different possible options for how the two can be combined in the design process. Dhillon et al. (2016) used value-based objectives as a means to support decisions on balancing security and usability, whereas Mohamed et al. (2016) focused on mental models. Furnell (2016) concluded that usability has received more attention over the years, and that more choices between security mechanisms (with different levels of perceived usability for the individual user) are available to users.

To the extent that usability has been evaluated empirically, this mostly concerned the user-friendliness of a *single* security technology, as a way to point out problems in current approaches, or a means of validation of a better design

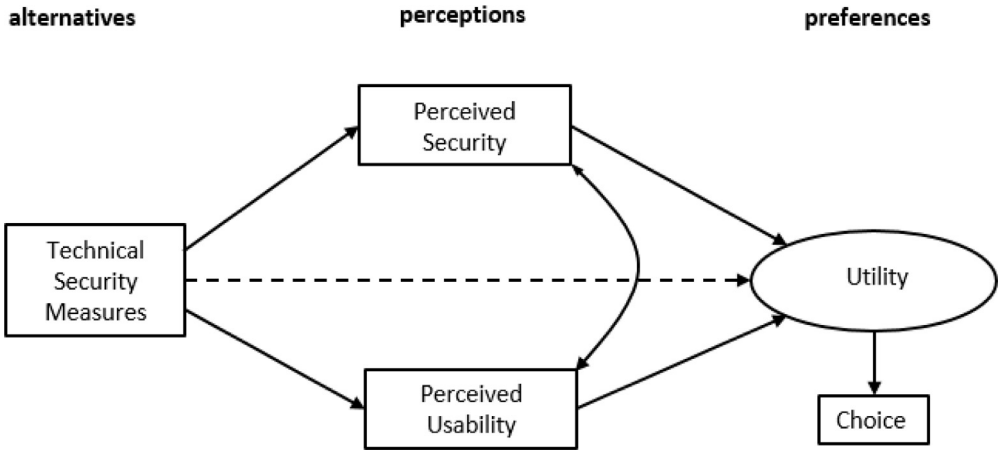


Fig. 1 – Conceptual framework.

(cf. Brostoff et al., 2010; Catuogno and Galdi, 2014; Sheng et al., 2006). This does not reveal the trade-offs that users make when having the opportunity to choose between different designs with different usability *and* security levels. The latter is particularly relevant in the context of concerns that employees may bypass company technology and use alternative (free but commercial) services instead, possibly with their own security add-ons – a notion which has been called "shadow security" (Kirlappos et al., 2015).

3. Conceptual framework and research questions

In order to understand how users make choices between different products/services with different usability and security characteristics, we need to investigate their preferences in the face of such different configurations. As discussed earlier, the company's CISO decides upon the security technology; hence, employees typically cannot freely choose the security packages of their preference. However, in this study we aim to study the process as if they could, so we are interested in the choices they make if they could freely choose their security packages and how they arrive at this choice; we assume that more preferred systems will result in higher compliance behaviour.

To study preferences, we leverage the paradigm of Discrete Choice Theory (e.g., Ben-Akiva and Lerman, 1985) and Discrete Choice Experiments (Louviere et al., 2000; Hensher et al., 2005). These are quantitative approaches that are usually employed in combination with the aim to empirically elicit the weights of different attributes in the preferences of users. More specifically, we conduct our research within the random utility framework (e.g. Manski, 1977; McFadden, 2001). This framework assumes that people choose that alternative from a set of available options from which they derive the highest utility; and that part of utility that can be related to observable factors (such as the attributes of alternatives) while another part is random, from the viewpoint of the analyst. The approach requires the observation of choices among alternatives that are described in several attributes. In this study, the attributes are technical security measures (TSMs) that can be taken by companies to protect information stored at computers. The alternatives describe combinations of attributes and thus represent packages of TSMs. The construction of these alternatives is discussed in the next section in full detail.

These constructed alternatives also allow us to study the trade-off between security and usability. At first sight, such a study would require establishing security and usability levels for different security designs. However, because it is complicated to assess security objectively (cf. Sanders, 2014) and because employees make choices among alternatives based on their perception of the alternatives (as opposed on their objective characteristics), we will explicitly measure these perceptions.

Fig. 1 summarizes the conceptual framework underlying our study. As will be explained in the following section, security packages are constructed that consist of different combinations of TSMs. These packages are evaluated by employees in terms of perceived security and perceived usability. The correlation between these observed evaluations indicates whether this relationship is negative as has been suggested in the literature. From the observed perception evaluations, models are estimated that indicate to what extent each of the TSMs affects perceived security and perceived usability of a security package. Furthermore, choices are observed between different security packages. From these observed choices, a choice model is estimated that indicates whether security or usability has a stronger effect on utility and as such on choices. Moreover, it is examined whether the effect of TSMs on choices (utility) is fully or partially mediated by security and usability perceptions. The solid lines represent the full mediation of the effect of the TSM's on utility by the two perception variables; the dashed line represents the direct effect of the TSM's on utility.

To summarize, this paper aims to answer to the following research questions:

- Do perceived usability and perceived security correlate negatively as suggested in the literature?
- Are more restrictive measures perceived as more secure and as less user-friendly?

Table 1 – Selected attributes (TSMs) and their levels.

Attribute	Level 1	Level 2	Level 3
Password length	No restrictions	Minimal 8 characters	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency	Never	Once a year	Once a quarter
Browser restrictions	Every browser is allowed	Obligatory browser	
File sharing inside company	No restrictions	Via corporate shared drive	
E-mail to someone outside the company	No restrictions	Warning message with e-mail	Pop-up message with e-mail which contains confidential word

- Does perceived usability or perceived security weigh stronger in employees' preferences for computer security?
- Are all effects of technical security measures on choice mediated by perceived usability and perceived security?

Next to these empirical questions, this study also aims to introduce the choice modelling paradigm in the information security community and evaluate possibilities for further research along these lines.

4. Methodology

In this section, the discrete choice experiment (DCE) is explained. First, we focus on how the technical security measures are selected. This is followed by a description of the way these are combined to arrive at choice alternatives. Next, the measurement tasks are explained. And finally, the model estimation and data collection procedures are discussed. For reasons of space limitations, we are unable to cover all nuances and subtleties that play a role in designing DCEs. Interested readers are referred to Hensher et al. (2005) for a full description.

4.1. *Technical security measures (TSMs)*

The alternatives presented to participants in the Discrete Choice Experiment involve combinations of TSMs. We define a TSM as an electronic security method that protects information on an office computer. Hence, this definition excludes measures that cannot be applied on a computer as well as measures that employees may take at home to protect their computer.

To arrive at a list of TSMs to be included in the experiment, a long list of different kinds of TSMs mentioned in the literature was made (e.g., Nurse, et al., 2011; Hagen et al., 2008; Kainda et al., 2010). The measures that did not fit the definition were removed from the list and the measures that are fairly similar to each other were grouped together. The resulting list was discussed with two experts of a major consultant in the field of information security, who have ample of experience with advising various clients in that regard. Finally, the most commonly used TSMs were selected to ensure that these are familiar to all respondents. The resulting seven attributes were tested in a pilot research, after which two more attributes were excluded because their content partially overlapped and respondents reported having troubles understanding their meaning. The resulting five attributes (TSMs) and their levels, which represent the different values the attributes can take in our experiment, are listed in Table 1.

4.2. *Construction of alternatives*

To arrive at alternatives from which participants are asked to choose during the DCE, the attribute levels (TSM-specifications) are combined according to an experimental design. Because respondents, in addition to being asked to choose among alternatives (security packages which consist of combinations of TSMs), are also asked to explicitly evaluate each alternative in terms of its perceived usability and security, the total number of alternatives to be constructed had to be limited. This way we avoid constructing a measurement task that is too demanding for respondents, which might trigger work overload and respondent fatigue, which in turn could lead to unreliable responses. With this constraint in mind, we constructed choice sets of three alternatives each, knowing that a choice from a set of three alternatives provides more preference-information than a choice from a set with only two alternatives. This approach reduces the number of choice tasks having to be attended to by participants.

Constructing a limited number of choice sets while still being able to estimate reliable parameters, can be accomplished by basing the construction of the choices alternatives on an efficient experimental design (e.g. Rose and Bliemer, 2009). Efficient experimental designs maximize information about the preferences and trade-offs obtained from each observed choice observation. This is achieved by, for example, avoiding a choice task which contains an alternative that dominates all other choice alternatives (i.e. outperforms it on every attribute). More generally, efficient experimental designs involve balancing the utilities of the alternatives in each choice set. To create such a balance, insight is needed in the utilities of alternatives, which requires prior parameter values, that is, the best estimates of the real parameter values by the analyst.

As this is the first stated preference experiment conducted on this topic, no prior parameter values were available from previous research. Therefore, a pilot research is conducted. The choice sets for this pilot study, each consisting three alternatives, are constructed from a so-called near orthogonal design resulting in 8 choice sets. This pilot experiment was filled out by 31 respondents recruited from the personal net-

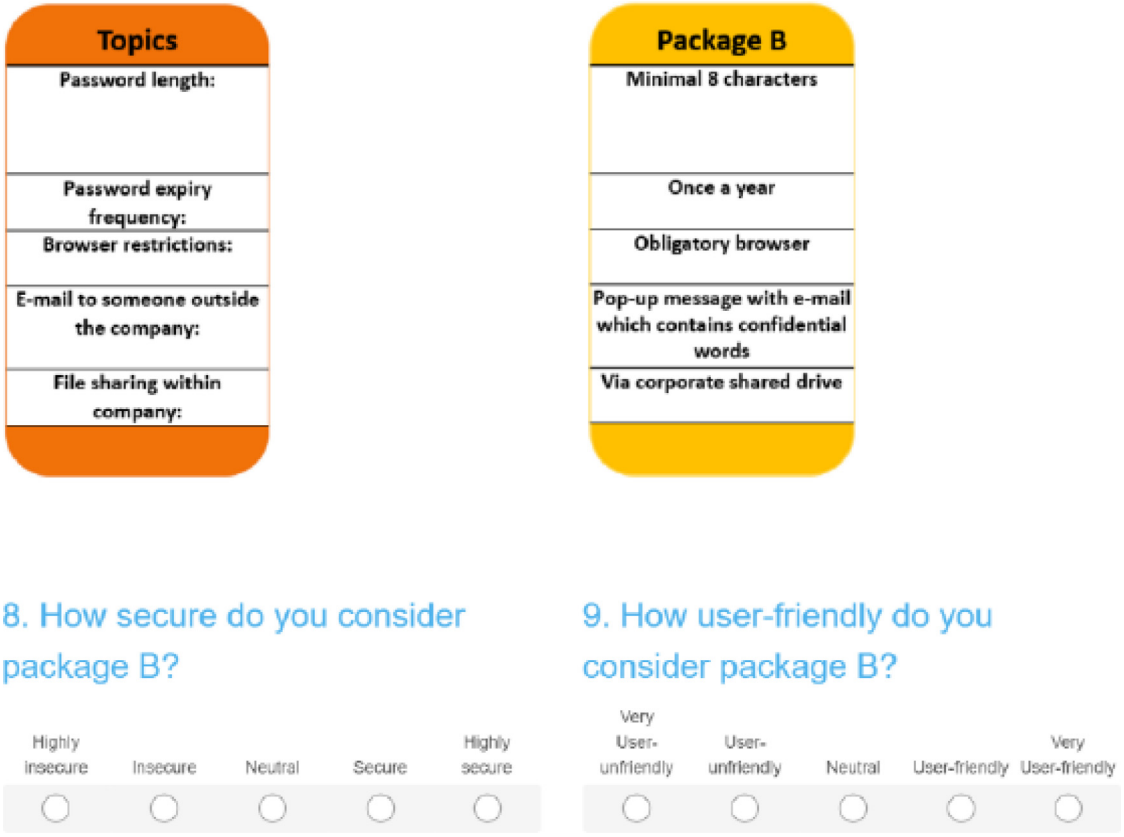


Fig. 2 – Example of the perception rating task.

work of one of the authors. A multinomial logit model is estimated from these observed choices and the estimated parameters were selected as the priors for constructing the efficient design for the main experiment. This resulted in the construction of 6 choice sets of three alternatives each, in the final design.

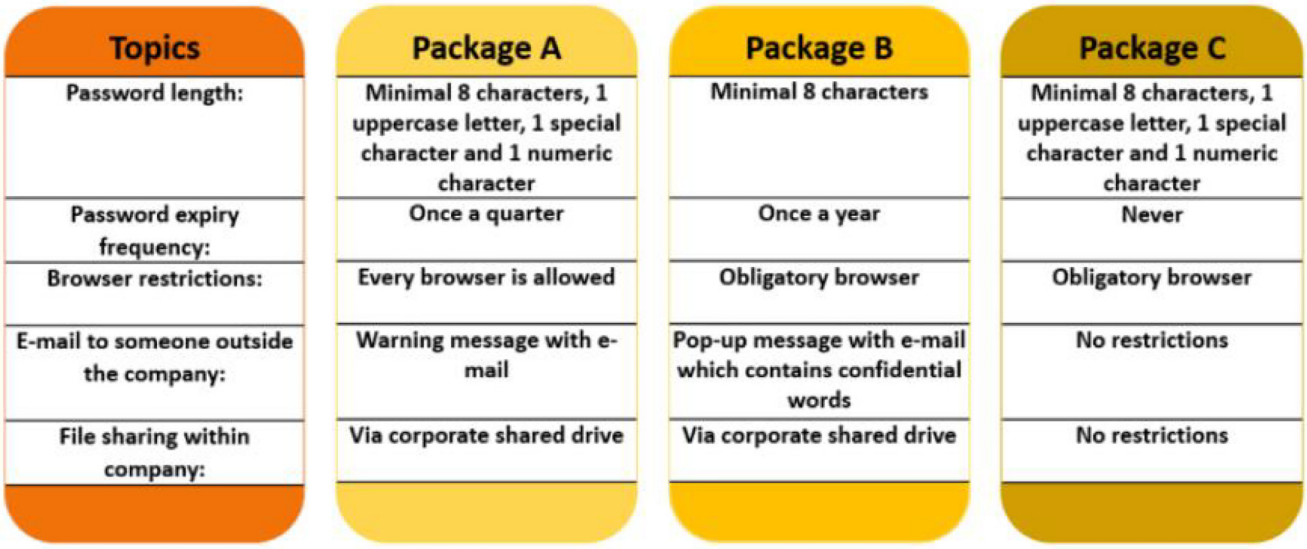
4.3. *Measurement task*

With respect to each of the choice sets, we requested respondents to perform two different tasks. First, they were asked to evaluate each alternative (security package) in terms of usability and security. To that effect, each single alternative is shown on the participant's computer screen, one by one. The respondent then evaluated the security and usability of the alternative by means of five-point rating scales, running from (1) highly insecure to (5) highly secure and from (1) very user-unfriendly to (5) very user-friendly, respectively. After providing the responses to package A, the second alternative, package B, of the same choice set appears on the computer screen. After providing the ratings for this package, the third and final package C of a choice set is shown. Fig. 2 presents a screenshot of the perception rating task. Note that package B is placed in the middle. This location corresponds with the location of that alternative in the choice task (see Fig. 3), which is discussed next.

After all the three alternatives are rated one by one in terms of perceived security and perceived usability, the entire choice set is presented on the screen, which thus consists of the same three packages the respondents rated just before. Respondents are then requested to indicate which of the three packages they would prefer at work. An example of this choice task is presented in Fig. 3. Note that the perceived security and perceived usability ratings which the respondents provided to each of the three packages are not visible at the moment they make the choice. The reason for this is that we wanted to stimulate respondents to once again consider the technical measures so they would not only base their choices on the ratings they just provided. However, respondents could consult the ratings by scrolling back to the rating questions and the ratings they provided.

To further limit the effort expected from respondents, the constructed 6 choice sets were blocked into two blocks of three choice sets each. A respondent was randomly assigned to only one of the two blocks. Thus, in total each respondent made three choices, and provided 18 perceptions ratings: nine security and nine usability perception ratings.

As was explained at the beginning of Section 3, the DCE in this study was constructed because the employees' choices among security packages cannot be observed in real life. As a consequence, so called stated behaviour is observed, hence, what the respondents say they will do when the presented hypothetical choice situation becomes a reality. Although responses observed in DCEs are often criticized for the possibility that stated responses do not necessarily reflect what people actually will do in real life, validation studies gener-



Topics	Package A	Package B	Package C
Password length:	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	Minimal 8 characters	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Once a quarter	Once a year	Never
Browser restrictions:	Every browser is allowed	Obligatory browser	Obligatory browser
E-mail to someone outside the company:	Warning message with e-mail	Pop-up message with e-mail which contains confidential words	No restrictions
File sharing within company:	Via corporate shared drive	Via corporate shared drive	No restrictions

Fig. 3 – Example of the choice task.

ally show high levels of accuracy in predicting actual choice behaviour by means of models estimated from responses observed in DCEs (e.g. Wlömert and Eggers, 2016).

4.4. *Model estimation*

Random utility theory assumes that decision makers, in our case employees, choose that alternative from a set of alternatives from which they derive the highest utility. It is further assumed that they derive a certain utility from each attribute level, in our case, a TSM level. This utility-component is called a part-worth utility. Finally, it is assumed that these part-worth utilities are combined to arrive at an overall utility for an alternative. Although other utility specifications are possible, it is typically assumed that this process can be approximated by the following linear additive utility function:

$$U_j = V_j + \varepsilon_j = \sum_i \beta_i X_{ij} + \varepsilon_j$$

where, U_j is the utility derived from an alternative j, V_j is the structural or systematic part of utility, which can be predicted by the model, ε_j is the random part utility, which is the part of utility that cannot be predicted by the model (e.g. covering idiosyncrasies from the side of the decision maker), X_{ij} denote the attribute levels of attribute i for alternative j; and β_i are the weights of the attributes i, hence, the parameters that are estimated. The product $\beta_i X_{ij}$ involves the part-worth utility of an attribute level, i.e., the contribution made by that attribute level to the utility of an alternative. By assuming that the error term ε_j is independently and identically distributed according to the so-called Extreme Value Type I distribution, choice probabilities take the following Multinomial Logit form:

$$p_j = \frac{e^{V_j}}{\sum_k e^{V_k}}$$

where p is the probability of choosing alternative j among a set of alternatives k, and e is the base of the natural logarithm. Parameter estimates are obtained using Maximum Likelihood Estimation routines. For a more detailed introduction into choice modeling we refer to Ben-Akiva and Lerman (1985).

Because all attributes in this study are categorical, they need to be coded first in order to be included in models. For this we applied a so-called effects coding scheme, which is presented in Table 2 (Bech and Gyrd-Hansen, 2005). This coding scheme involves that the L levels of an attribute are coded by L−1 indicator variables. The first L−1 levels are coded 1 on

Table 2 – Effects coded attribute levels.

Attributes	Levels	Parameters	
		PLMM	PLM
Password length (PL)	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	1	0
	Minimal 8 characters	0	1
	No restrictions	−1	−1
		PEFOQ	**PEFOY**
Password expiry frequency (PEF)	Once a quarter	1	0
	Once a year	0	1
	Never	−1	−1
		BR	
Browser restrictions (BR)	Obligatory browser	1	
	Every browser is allowed	−1	
		ERPM	**ERWM**
E-mail restriction (ER)	Pop-up message with e-mail which contains confidential words	1	0
	Warning message with e-mail	0	1
	No restrictions	−1	−1
		FS	
File sharing (FS)	Via corporate shared drive	1	
	No restrictions	−1	

each respective indicator variable and 0 on all other indicator variables, while the *L*th level is coded −1 on all indicator variables. If all attributes are effects coded, then an estimated constant can be interpreted as the mean score on the dependent variables derived from all evaluated alternatives. Estimated coefficients for the L−1 indicator variables then indicate to what extent the corresponding levels affect the dependent variable. By definition, the contributions to the dependent variable of the levels that belong to the same attribute summate to zero. In utility models, the parameters estimated for the L−1 indictor variables express the marginal utility of the corresponding level. The marginal utility of the *L*th level is the negative sum of the marginal utilities of the other L−1 levels

The structural utility *V* derived from alternative *j* can be specified as follows:

$$\begin{aligned} V_j = {} & \beta^V_{PLMM} \cdot PLMM_j + \beta^V_{PLM} \cdot PLM_j + \beta^V_{PEFOQ} \cdot PEFOQ_j \\ & + \beta^V_{PEFOY} \cdot PEFOY_j + \beta^V_{BR} \cdot BR_j + \beta^V_{ERPM} \cdot ERPM_j \\ & + \beta^V_{ERWM} \cdot ERWM_j + \beta^V_{FS} \cdot FS_j + \beta^V_{PS} \cdot PS_j \\ & + \beta^V_{PSQ} \cdot PS^2_j + \beta^V_{PU} \cdot PU_j + \beta^V_{PUQ} \cdot PU^2_j \end{aligned}$$

where β are the parameters to be estimated and the other terms are as explained in Table 2, except for the PS and PU, which denote the observed perceived security and perceived usability ratings resepectively (note: these were obtained per individual based on the outcomes of the rating task described above). Because we expect that the marginal increase in utility diminishes with higher initial perception levels, we add quadratic terms for PS and PU. Note that because we conducted an unlabeled experiment, no constant is included in the utility function as there is no reason to expect that respondents would systematically prefer the first, second or third alternative in a choice set.

In addition to the choice model, we estimate separate models for the security and usability ratings that are observed for every alternative. These ratings are assumed to be of interval measurement level, hence, regression models are estimated to examine to what extent each indicator variable affects the perceived security and perceived usability, respectively. More specifically, the following function is estimated to predict the perceived security PS^P of an alternative j:

$$\begin{aligned} PS^P_j = {} & C + \beta^{PS}_{PLMM} \cdot PLMM_j + \beta^{PS}_{PLM} \cdot PLM_j \\ & + \beta^{PS}_{PEFOQ} \cdot PEFOQ_j + \beta^{PS}_{PEFOY} \cdot PEFOY_j \\ & + \beta^{PS}_{BR} \cdot BR_j + \beta^{PS}_{ERPM} \cdot ERPM_j \\ & + \beta^{PS}_{ERWM} \cdot ERWM_j + \beta^{PS}_{FS} \cdot FS_j \end{aligned}$$

C is the regression constant and β are the parameters to be estimated. A similar model is estimated to predict perceived usability PU^P(we leave out the corresponding function to avoid repetition). Because effects coding is applied and thus all attributes are expressed on the same scale (−1 to 1), the estimated parameters in the perceived security and perceived usability equations can be directly compared in terms of weight, i.e., the impact on the observed perception. Note that these parameters cannot be directly compared to the parameters of the choice models, because these are expressed on a different scale.

4.5. *Data collection*

The population of interest consists of all employees whose job involves working with computers on a regular basis. A sample is recruited from this population by applying snowball sampling, starting with the personal network of one of the authors. Each respondent was asked to send the questionnaire to three persons of their social network that belonged to the population. In total, 230 respondents completely filled out the questionnaire.

Table 3 presents a distribution of respondent characteristics. The table makes clear that more males than females responded. Furthermore, respondents are relatively young

Table 3 – Distribution or respondent characteristics (in percentages of N = 230).

Gender	Male	60.0
	Female	40.0
Age	< 25 years	20.9
	25–29 years	37.8
	30–39 years	19.1
	40–49 years	10.0
	50 + years	12.2
Company size (number of employees)	< 10	6.5
	10–49	10.0
	50–249	10.9
	250–500	6.1
	500–999	5.2
	1000–9999	31.3
	10,000 +	30.0
Work experience	< 1 year	41.3
	1–4 years	34.4
	5–9 years	11.8
	10 + years	12.6
Share worktime on computer	0–25%	3.0
	26–50%	7.0
	51–75%	23.0
	76–100%	67.0

(average age is 32 years), which is also reflected in the relatively large share of respondent with relatively limited number of years of work experience. On the other hand, two thirds of the respondents spend most of their working time on a computer, so in that respect they are experienced. Finally, the results show that the far majority of the respondents works in big of very big companies.

Because of the non-random starting point of the snowball procedure, the questionnaire cannot be considered a random sample. So care should be taken to generalize the results from this sample to the wider population of employees.

5. Results

In this section, we present and discuss the results of the three estimated models. This section is organized by following the four earlier formulated research questions.

5.1. *Security and usability correlation*

We start by focussing on the first research question: Do perceived usability and perceived security correlate negatively, as suggested in the Literature? This expectation can indeed be confirmed by the empirical results: the correlation is negative, −0.143 ($p = 0.000$), albeit suggesting a relatively weak association. This finding on the one hand confirms notions from the literature that on an average higher (perceived) security is paired with lower (perceived) usability. On the other hand, the relatively low correlation also indicates that this is not necessarily always the case, as suggested in the literature as well. Hence, this suggests that it should in principle be possible to design technical security measures that are both perceived to be secure and usable (note that our results provide some options to do so, which we will discuss later).

Table 4 – Distributions of observed usability and security ratings and correlation (N = 2070).

Rating	Security	Usability
1	9.1%	2.1%
2	32.0%	13.3%
3	24.8%	29.3%
4	28.0%	44.0%
5	6.0%	11.2%
mean	2.90	3.49
median	3.00	4.00
stand. dev.	1.094	0.932
correlation	−0.143	

Table 4 presents the distributions for the observed security and usability perception ratings. The results indicate that for both security and usability the full range of the rating scale is used by respondents. Comparing the distributions reveals that on average the presented security packages score higher on perceived usability than on perceived security and that the spread in usability ratings is somewhat smaller.

5.2. *Security and usability perception of technical security measures*

To answer the second research question (Are more restrictive measures perceived as more secure and less user friendly?), we inspect the results of the two regression models estimated from the observed perceptions. These are presented in Table 5: in the first column the parameters of Perceived Security (β^{PS}), in the second column those of Perceived Usability (β^{PU}). Recall from Table 3 that we estimate L−1 parameters for the L attribute levels of each attribute. Absolute t-values > 1.96 denote a statistically significant parameter at the conventional 95% confidence level. In order to give a full picture and to ease interpretation of the levels of all varied security attributes, we added the effect of the Lth level to the table (in italics). The latter effects are not estimated but derived: because effects coding is applied, the contributions to the ratings of all levels of an attribute sum to zero by design. These effects are thus expressed in deviations from the average, which in both regression models is denoted by the estimated constant. Model fit of the Perception models is based on the well-known R-square measure which gives the percentage of variation in perception which is explained by the model. Model fit of the Choice models is measured based on McFadden's rho-squared (e.g. Ben-Akiva & Lerman, 1985), which gives the percentage of initial uncertainty – from the side of the analyst – concerning choice probabilities which is eliminated by the estimated model. Both range from 0 to 1, with higher values indicating a better model-fit. The Rho-squared values of the presented model (see Table 5) are 0.25 and 0.44 respectively, which many researchers interpret as a reasonable model fit and reasonably good model fit respectively (Hensher et al., 2005). Furthermore, both estimated choice models are statistically significant in the sense that they fit the data better than the null model: LL_Null-model = −758.04; LL_Model C (attributes only) = −565.66 (LRS = 384.76, df = 8, $p = 0.000$);

Table 5 – Estimated parameters and associated *t*-values ($t > 1.96$ implies significance at the 5% level).

	Perception				Choice			
	A Security		B Usability		C Attributes only		D Attributes+perceptions	
	β^{PS}	t	β^{PU}	t	β^{V}	t	β^{V}	t
Regression constant (C)	2.90	156.51	3.49	185.52				
Password length								
Min 8 ch., 1 uppercase, 1 special ch., 1 numeric ch. (PLMM)	0.58	20.06	−0.05	−1.75	0.89	11.28	−0.11	−1.14
Minimal 8 characters (PLM)	0.02	0.73	0.06	1.91	−0.02	0.23	0.57	5.89
No restrictions	*−0.60*		*−0.01*		*−0.87*		*−0.46*	
Password expiry frequency								
Once a quarter (PEFOQ)	0.42	15.92	−0.24	−8.89	0.31	4.78	−0.03	−0.30
Once a year (PEFOY)	0.02	0.83	0.12	4.43	0.11	1.46	0.28	3.46
Never	*−0.44*		*0.12*		*−0.42*		*−0.25*	
Browser restrictions								
Obligatory browser (BR)	0.04	1.83	−0.27	−13.28	−0.35	7.23	−0.22	−3.98
Every browser is allowed	*−0.04*		*0.27*		*0.35*		*0.22*	
E-mail restriction								
Pop-up message with e-mail which contains confidential word (ERPM)	0.21	7.42	−0.14	−4.88	0.02	0.21	0.03	0.43
Warning mess. with e-mail (ERWM)	0.14	5.15	−0.06	−2.39	0.09	1.35	−0.07	−0.73
No restrictions	*−0.35*		*0.20*		*−0.11*		*0.04*	
File sharing								
Via corporate shared drive (FS)	0.27	13.40	−0.08	−3.76	0.19	3.86	0.05	0.78
No restrictions	*−0.27*		*0.08*		*−0.19*		*−0.05*	
Perceived security (PS)							2.51	5.74
Perceived security^2 (PSQ)							−0.24	−3.62
Perceived usability (PU)							2.33	4.37
Perceived usability^2 (PUQ)							−0.19	−2.57
Model fit:	$R^2 = 0.41$		$R^2 = 0.16$		$Rho^2 = 0.25$		$Rho^2 = 0.44$	

LL_Model D (attributes + perceptions) = −425.37 (LRS = 665.34, df = 12, $p = 0.000$).

Based on our discussion of previous research, we expect that increased restrictions are perceived as more secure but as less usable (less user-friendly), hence, their effects are expected to have opposite signs. Indeed, the results suggest that this is the case:

- Having more restrictions on passwords is clearly perceived to increase security (see col. A) and this effect is relatively large. On the other hand, its effect on usability (see col. B) is not statistically significant.
- Obligatory change of password every 3 months is perceived to improve security (see col. A), whereas it is perceived as less usable (see Col. B).
- Obligatory browser is perceived to improve security (col. A), although its effects is rather small, and is perceived to be less usable (col. B).
- Also obligatory file sharing via a corporate drive is perceived to improve security (col. A), but is perceived as less usable (col. B). The impact on security is much larger than on usability.
- Finally, with respect to E-mail restrictions, both warning messages are perceived to increase security (col. A) and to decrease usability (col. B).

Some further results of the regression models are noteworthy mentioning. Comparing the R^2's of the two models indicates that the proportion explained variance of the Perceived Security Model (col. A) is much higher than of the Perceived Usability Model (col. B). Hence, security perception can be predicted with more precision than usability perception. Possibly, interactions between attributes play a bigger role in the usability model and/or employees are much more heterogeneous in their usability perceptions of security measures than in their security perceptions. Furthermore, as reported earlier and also denoted by the higher regression constant, the average perceived usability level of the presented technical security packages is higher than their average perceived security level.

5.3. *Impact of security and usability on choice*

We now focus on the third research question: does perceived usability or perceived security weigh stronger in employees'

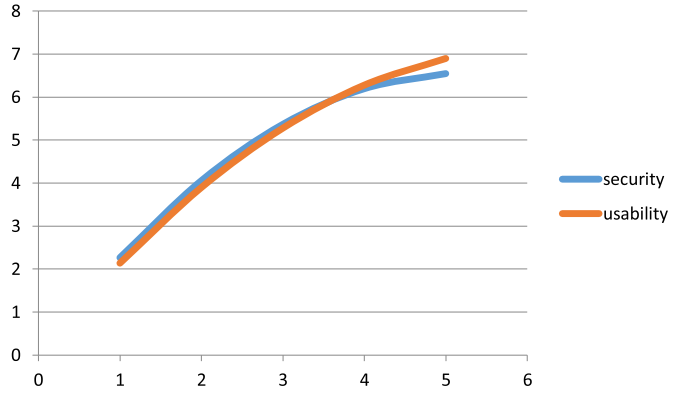


Fig. 4 – Utility contribution for security and usability perception.

preferences for computer security? To answer this question, we inspect the parameters for perceived security and perceived usability as estimated by the multinomial logit model, which are presented in col. D of Table 5. As expected, both (linear) parameters have a positive sign, which indicates that the more the security measures are perceived to be secure and the more they are perceived to be usable, the more utility is derived from the package containing these measures, and thus the more likely that package is chosen (ceteris paribus). In addition to the parameters for the linear effects, also the parameters for the quadratic components of the perception ratings are statistically significant. These parameters are negative, which suggests that for higher initial values of perceived security and perceived usability, further marginal increase in utility is diminished. This is a plausible outcome: the higher the evaluation of a package of technical security measures already is, the less additional utility is derived from a further increase. This effect is illustrated in Fig. 4, which presents the utility contribution for predicted security and usability ratings, as a function of the initial levels.

Fig. 4 also demonstrates that the impact of perceived security and perceived perception on utility is about the same. The figure suggests that at lower values, the impact of perceived security is little stronger, while at higher values the impact of perceived usability is a little stronger. This suggests that once security is at a high level, thus the package is considered safe, usability becomes more important. However, the differences found in the sample are very small and the estimated parameters do not differ in a statistically significant way. Thus, we conclude that perceived security and perceived usability affect choice of security packages to a similar extent.

Comparing Rho-square values of the MNL with and without the perception ratings as explanatory variables (col. C with col. D in Table 5) indicates to what extent the ratings themselves affect choice, beyond the effects of the factors that influence these ratings (i.e., the TSMs). By adding the perception ratings, the Rho-square value significantly increases from 0.25 to 0.40, indicating a substantial improvement of model fit. Hence, the observed perceptions play a substantial role in the choice of the preferred security package. As expected, parameters and t-ratios in col. D are mostly smaller than those in col. C, indicating that part of their effect is mediated by the security and usability perceptions.

5.4. *Direct versus indirect effects of security measures*

This last result raised the fourth research question: Are all effects of technical security measures on choice mediated by perceived usability and perceived security? If the effects of the security attributes would all be mediated by the two perceptions, their parameters would not be statistically significance once the observed perceptions were included in the model. Hence, non-significant parameters suggest that the direct effects of TSMs on choices are non-existent and all effects are mediated in an indirect process, i.e., through the effects of TSMs on perceptions and the effects of perceptions on choice. As the results presented in the col. D of Table 5 indicate, this is not the case: even when controlled for security and usability perception, the following parameters of the technical security measures on utility are found to be statistically significant:

- The level *minimal 8 characters* password length, is preferred above more restricted levels, thus the less restricted password requirement is preferred.
- The level *once a year* of password change frequency is more preferred than *once a month*, thus the less frequent change is preferred.
- *Every browser allowed* is more preferred than *obligatory browser,* thus the less restricted level is preferred.

What may be considered remarkable, is that these significant levels all concern less restrictive measures. Moreover, they all concern levels of which we found earlier that they positively influence perceived *usability* ratings. On the other hand, most of the levels of which we earlier found that they increased the perceived *security* ratings lose their statistical significance. In contrast, these levels all significantly increase utility in the attributes-only MNL model (see col. C of Table 5), i.e. the model which does not include the perceptions. These results suggest that perceived security mediates security related aspects of the technical security measures, whereas perceived usability does not fully mediate usability aspects of these TSMs.

The question is then what the three significant direct effects represent; in other words, could these for example represent another (perception) dimension in addition to security and usability? We can only speculate about this, because we

do not have additional measurements. A possibility is that the three significant levels represent current security levels many employees currently experience at work. Such a third dimension that might play a role in preferences of security packages in addition to security and usability could be labelled as *familiarity* with the security measures at work. Another possible dimension may be related to a TSM's impact on the business at large rather than (individual) usability. For example, employees may prefer measures that are known to secure highly important business resources, or they may prefer measures with limited impact on overall productivity.

5.5. *An illustration*

In this section, an illustration of the results is provided to demonstrate how the estimated models can be applied to predict employees' perceptions and preferences concerning different security packages (i.e., combinations of TSMs). This application shows how the model can be used by CISOs in the design of security packages, for example, to design an optimal security package. We first apply the model to predict the choice probabilities for a scenario in which employees can only choose between a usability optimal and a security optimal package: (1) the "usability optimal" package maximizes the user-friendliness and consists of those TSM levels that all contribute highest to perceived usability, which all involve less restrictive measures (see Table 5); (2) the "security optimal" package maximizes security and consists of the most restrictive levels of each TSM that all contributed highest to perceived security. Table 6 presents the levels of the packages and their contributions to perceived security, perceived usability and utility contribution based on the parameter estimates presented in Table 5.

To predict choice probabilities, we first need to predict the utilities of both packages that consist of direct and indirect effects of the technical security measures. To illustrate this, we calculate the utility of the first package. Completely in line with earlier presented equations, the contribution to utility of the direct effects is simply the sum of direct effects, which are presented in the last column of Table 6 (the direct effect of the first package is 1.06). To calculate the indirect effects, we first need to predict the security and the usability perceptions of the package, which can be found by summing the results in the first and second columns of Table 6, respectively. The utility contribution of perceived security and perceived usability to the overall utility of these packages is then calculated by weighing the predicted perception values with their parameters as estimated by the MNL model (the attributes plus perception model). The utility contribution of PS in the first package $= 2.51 * 2.28 - 0.24 * 2.28^2 = 4.48$; the utility contribution of PU $= 2.33 * 4.22 - 0.19 * 4.22^2 = 6.25$. These utility contributions represent the indirect effect of the TSMs mediated by the perceptions. The overall utility of the package is a summation of the two indirect effects and the direct effect (11.98).

In a similar fashion, the overall utility of the *security optimal* package can be calculated (11.04). For the scenario in which employees can only choose between the usability optimal and the security optimal packages, the MNL model predicts that $(\exp(11.98)/(\exp(11.98) + \exp(11.04)) =)$ 72% of the employees would choose the *usability optimal* package and, hence, 28% would choose the *security optimal* package. Hence, the large majority would not prefer the security optimal package.

Assume that the CISO wishes to design a highly secure package that is more preferred by the employees, for example, because she believes this would increase compliance and less counter-effective behaviour of employees. Hence, the CISO wishes to keep a high security packages and therefore only allows a minimal concession to user-friendliness. She assumes the following package: (3) "joint optimal", which has the same high security levels as the security optimal package, except that for browser restrictions the level *obligatory browser* is replaced by the more user-friendly level *every browser allowed*. The results indicate that this adaptation hardly affects the *security perception*, but it considerably increases the usability perception and results in a higher direct utility contribution. This results in an even higher overall utility (12.10) of this package than the *usability optimal* package. If employees could only choose between the *usability optimal* and the *joint optimal* package, the MNL model predicts that 53% would prefer the *joint optimal* package, and 47% would prefer the *usability optimal* package. Hence, instead of only 28% preferring the highly secure package, now 53% of the employees, thus the majority, prefers the highly secure package over the most user-friendly package, while only a single concession is made to user-friendliness.

This example suggests that CISOs can design and implement a highly security package that is still preferred by a majority of the employees. This package involves a maximum of password restrictions, frequent password changes, file sharing via a shared drive and email restrictions that involve warning messages. Obligatory browsers, on the other hand, are not supported by the employees, so they are not included in the package: this TSM is not perceived to contribute to security while it is regarded as less user-friendly. It goes without saying that the more concessions are made to user-friendliness, the more employees will prefer the resulting security packages. As is demonstrated here, CISOs can apply the model to ex ante evaluate different security package designs in terms of employees preferences and in this way design their optimal security package.

6. Conclusion and discussion

In this paper, employees' preferences for technical security measures that companies can take to protect information are studied within the empirical frameworks of discrete choice theory and discrete choice experiments. More specifically, an experiment is conducted, in which employees evaluate combinations of technical security measures in terms of security and usability perceptions and make choices among security packages. Regression models were estimated from the observed perception ratings, the parameters of which express to what extent security measures affect perceived security and perceived usability. In addition, a so-called MNL model (being the workhorse model for discrete choice analysis) was estimated from the observed choices, which revealed the relative impact of security and usability perceptions on choice. Our results provide insight into the trade-off made by users of

Table 6 – An illustration: predicted employee responses to three security packages.

		Contributions		
		PS	PU	V
Package 1	**"usability optimal"**			
Regression constant		2.90	3.49	
Password length	*Minimal 8 characters*	0.02	0.06	0.57
Password expiry	*Once a year*	0.02	0.12	0.28
Browser restrictions	*Every browser is allowed*	−0.04	0.27	0.22
E-mail restriction	*No restrictions*	−0.35	0.20	0.04
File sharing	*No restrictions*	−0.27	0.08	−0.05
	Predicted perceptions	2.28	4.22	
	Predicted utility contribution	4.48	6.45	1.06
	Overall utility	**11.98**		
Package 2	**"security optimal"**			
Regression constant		2.90	3.49	
Password length	*Min 8 ch., 1 upperc. 1 sp. ch.,*	0.58	−0.05	−0.11
Password expiry	*Once a quarter*	0.42	−0.24	−0.03
Browser restrictions	*Obligatory browser*	0.04	−0.27	−0.22
E-mail restriction	*Pop-up – confidential words*	0.21	−0.14	0.03
File sharing	*Via corporate shared drive*	0.27	−0.08	0.05
	Predicted perceptions	4.42	2.71	
	Predicted utility contribution	6.41	4.92	−0.28
	Overall utility	**11.04**		
Package 3	**"joint optimal"**			
Regression constant		2.90	3.49	
Password length	*Min 8 ch., 1 upperc. 1 sp. ch.,*	0.58	−0.05	−0.11
Password expiry	*Once a quarter*	0.42	−0.24	−0.03
Browser restrictions	***Every browser is allowed***	**−0.04**	**0.27**	**0.22**
E-mail restriction	*Pop-up – confidential words*	0.21	−0.14	0.03
File sharing	*Via corporate shared drive*	0.27	−0.08	0.05
	Predicted perceptions	4.34	3.25	
	Predicted utility contribution	6.37	5.57	0.16
	Overall utility	**12.10**		
Choice probability		**A**	**B**	
A = package 1	B = package 2	72%	28%	
A = package 1	B = package 3	47%	53%	

information technology, between security and user-friendliness aspects of technical security measures.

Based on the results of the estimated models, answers are formulated to four research questions, which can be summarized as follows. First, perceived usability and perceived security indeed correlate negatively as is suggested in the literature, although we find that the association is relatively weak (−0.14). Second, as expected, more restrictive security measures are perceived as more secure and as less usable. Third, perceived security and usability affect choice to the same extent; that is, both dimensions of technical security measures are considered equally important by users of information technology. As expected, higher security and usability perception scores increase the preference for security packages; however, and in line with intuition, the marginal increase diminishes with higher initial levels of security and usability perceptions. Fourth, perceived security fully mediates the effect of security related aspects of technical security measures, while perceived usability does not fully mediate the effects of user-friendliness related aspects of security measures. The results give rise to the possibility that other dimensions exists that mediate the effects of TSMs, such as for example familiarity. However, this possibility needs further research.

Our findings that (a) employees clearly recognize that more restrictive measures improve security, and (b) security is considered by them to be equally important as usability, may encourage CISOs of companies to adopt a more cooperative process in their security design process, in which perceptions and preferences of employees are taken into account. Investigating employee preferences, like in our study, may lead to the design and implementation of packages of security controls that are better tailored towards employee's needs, reducing circumvention activities that could be exploited in cyberattacks. We provided an illustration of how the models estimated in this study can be applied for this purpose. However, this will not be simply a matter of selecting the right controls; it will also involve properly managing commitment and awareness.

Interesting avenues for further research within the discrete choice framework include the following. First, the number of technical security measures included in our study was rather limited (for good reasons). Hence, it would be of interest to include more of those measures, such as for example, multi-factor authentication, and examine whether the strength of

the correlation between perceived security and usability as found in this study is robust. Second, in our study perceptions are measured first, and then choices are observed. The question is whether explicitly asking about usability and security first makes respondents more conscious of these aspects (i.e., increases their salience), so the issue is to what extent the presentation order affected the results. It would be of interest to study to what extent our results are robust under a different order of both measurement tasks. Third, the possibility of other dimensions in addition to security and usability, e.g. familiarity, could be further investigated. Fourth, the results presented in this paper were based on a convenience sample, and should therefore be treated with care. Hence, further research should include more representative samples. Fifth, heterogeneity in perceptions and preference could be examined. The discrete choice paradigm offers a range of methods to study heterogeneity (Greene & Hensher, 2003), of which the following three are probably most promising in the context of response to information security measures. First, traditional segmentation could be applied, which implies examining to what extent people with different sociodemographic characteristics differ in their perception of and preferences for TSMs. Second, it can be assumed that preference weights do not have crisp values but follow a certain distribution across employees, which can be examined by estimating more advanced choice models, such as mixed logit models. Third, latent classes may be assumed, which are groups in the population that are internally homogeneous in their preferences and which can be identified based on their observed choices. In these models, membership functions can be estimated that allow predicting the probability of belonging to a latent class based on observed individual characteristics.

Apart from extensions to the present study, it is hoped that this paper stimulates other choice modelling applications in this field, both extending the work on employee preferences as well as focusing on the choices of other actors in the cybersecurity playing field. In terms of employees, this may not only involve studying preferences for security controls, but also choices in terms of compliance or non-compliance with security policies. Choices for non-compliance may happen spontaneously, for example when official security is found too cumbersome, or in response to deceptive acts of attackers, such as in phishing (Finn and Jakobsson 2007) or social engineering (Bullée et al. 2015) attacks. How attributes of policies and situations contribute to preferences for (non-)compliance may help in improving organizational aspects of security. One possible application to other actors lies in analysing the choices security officers make when selecting controls to be implemented in their organization. Which attributes contribute to the utility of a possible control, and how does this affect the decision? Another possibility is to study choices of cyber-attackers, in terms of which targets to attack using which means, assuming that there are subjects willing to participate, either known offenders or white-hat (ethical) hackers. Better understanding of attacker choices may inform better representations of attacker behaviour in security models and risk analyses. In these ways, discrete choice theory and discrete choice experiments may become useful tools in the portfolio of techniques for improving security in cyberspace by considering the human factor.

As a final note, there is a debate around how much control should *actually* be given to employees regarding security choices. Much of the existing practices assume centralized control of security solutions (cf. Parkin, Kassab & Van Moorsel 2008), but one could imagine frameworks in which employees can decide how much security the data or applications they work with require. This so-called "laissez-faire security" (Johnson et al. 2009) requires investigation not just of the preferences of employees with respect to technical security measures, but also *regarding their preferred level of control over such measures*.

REFERENCES

Adams A, Sasse MA. Users are not the enemy. Commun ACM 1999;42(12):40–6.

Andersson, D. (2013). Authentication with passwords and passphrases: implication on usability and security. http://www.rlvision.com/blog/authentication-with-passwords-passphrases-implications-on-usability-and-security/

Beautement A, Coles R, Griffin J, Ioannidis C, Monahan B, Pym D, et al. Modelling the human and technological costs and benefits of USB memory stick security. Managing information risk and the economics of security. US.: Springer; 2009. p. 141–63.

Bech M, Gyrd-Hansen D. Effects coding in discrete choice experiments. Health Econ 2005;14(10):1079–83.

Ben-Akiva M, Lerman SR. Discrete choice analysis: theory and application to travel demand. Cambridge: MIT Press; 1985.

Brostoff S, Inglesant P, Sasse MA. Evaluating the usability and security of a graphical one-time PIN system. Proceedings of the 24th BCS interaction specialist group conference. British Computer Society; 2010. p. 88–97.

Bullée JWH, Montoya L, Pieters W, Junger M, Hartel PH. The persuasion and security awareness experiment: reducing the success of social engineering attacks. J Exp Criminol 2015;11(1):97–115.

Caputo DD, Pfleeger SL, Sasse MA, Ammann P, Offutt J, Deng L. Barriers to usable security? Three organizational case studies. IEEE Secur Priv 2016;14(5):22–32.

Catuogno L, Galdi C. Analysis of a two-factor graphical password scheme. Int J Inf Secur 2014;13(5):421–37.

Cranor LF, Garfinkel S. Guest Editors' Introduction: secure or usable? IEEE Secur Priv 2004;2(5):16–18.

Davis Jr FD. A technology acceptance model for empirically testing new end-user information systems. Massachusetts Institute of Technology, 1986.

Dhillon G, Oliveira T, Susarapu S, Caldeira M. Deciding between information security and usability: developing value based objectives. Comput Hum Behav 2016;61:656–66.

Dinev, T., J. Goo and K. Nam (2006), User behaviour toward preventive technologies – cultural differences between the United States and South Korea. In: Proceedings of the paper presented at the ECIS.

Finn P, Jakobsson M. Designing ethical phishing experiments. IEEE Technol Soc Mag 2007;26(1):46–58.

Furnell S. The usability of security-revisited. Comput Fraud Secur 2016;2016(9):5–11.

Gandal, S. (2015). Lloyd's CEO: cyber-attacks cost companies $400 billion every year, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds, (Accessed March, 15, 2017).

Greene WH, Hensher DA. A latent class model for discrete choice analysis: contrasts with mixed logit. Transp Res Part B Methodol 2003;37(8):681–98.
Gutmann P, Grigg I. Security usability. IEEE Secur Priv 2005;3(4):56–8.
Hagen JM, Albrechtsen E, Hovden J. Implementation and effectiveness of organizational information security measures. Inf Manag Comput Secur 2008;16(4):377–97.
Hensher DA, Rose JM, Greene WH. Applied choice analysis: a primer. Cambridge University Press; 2005.
Herley C. So long, and no thanks for the externalities: the rational rejection of security advice by users. Proceedings of the workshop on new security paradigms workshop, 2009.
ISACA and RSA Conference (2015), State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey, ISACA and RSA Conference. https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf (Accessed March, 15, 2017).
Johnson ML, Bellovin SM, Reeder RW, Schechter SE. Laissez-faire file sharing: access control designed for individuals at the endpoints. Proceedings of the new security paradigms workshop. ACM; 2009. p. 1–10.
Kainda R, Flechais I, Roscoe AW. Security and usability: analysis and evaluation. Proceedings of the ARES'10 international conference on availability, reliability, and security. IEEE; 2010. p. 275–82.
Kirlappos I, Parkin S, Sasse MA. Shadow security as a tool for the learning organization. ACM SIGCAS Comput Soc 2015;45(1):29–37.
Louviere JJ, Hensher DA, Swait JD. Stated choice methods: analysis and application. Cambridge: Cambridge University Press; 2000.
Manski CF. The structure of random utility models. Theory Decis 1977;8(3):229–54.
McFadden D. Economic choices. Am Econ Rev 2001;91(3):351–78.
Mohamed MA, Chakraborty J, Dehlinger J. Trading off usability and security in user interface design through mental models. Behav Inf Technol 2016:1–24.
Nurse JR, Creese S, Goldsmith M, Lamberts K. Guidelines for usable cybersecurity: Past and present. Proceedings of the third international workshop on cyberspace safety and security (CSS). IEEE; 2011. p. 21–6.
Parkin SE, Kassab RY, Van Moorsel A. The impact of unavailability on the effectiveness of enterprise information security technologies. Proceedings of the fifth international service availability symposium on service availability, ISAS 2008. Springer, 2008.
Post GV, Kagan A. Evaluation information security tradeoff: restricting access can interfere with user tasks. Comput Secur 2007;26(3):229–37.
Rose J, Bliemer M. Constructing efficient stated choice experimental designs. Transp Rev 2009;29(5):587–617.
Sanders WH. Quantitative security metrics: unattainable holy grail or a vital breakthrough within our reach? IEEE Secur Priv 2014;12(2):67–9.
Schultz EE. Research on usability in information security. Comput Fraud Secur 2007;2007(6):8–10.
Sheng S, Broderick L, Koranda CA, Hyland JJ. Why Johnny still can't encrypt: evaluating the usability of email encryption software. Proceedings of the symposium on usable privacy and security; 2006. p. 3–4.
Venkatesh V, Davis FD. A theoretical extension of the technology acceptance model: four longitudinal field studies. Manag Sci 2000;46(2):186–204.
Wlömert N, Eggers F. Predicting new service adoption with conjoint analysis: external validity of BDM-based incentive-aligned and dual-response choice designs. Market Lett 2016;27:195–210.

Eric Molin is an associate professor of Travel Behavior Research at the Engineering Systems and Services Department of the faculty Technology, Policy and Management, TU Delft. He conducts research that is on the crossing between applying cutting edge behavioral research methods and generating policy relevant insights for emergent policy topics. He is an expert in developing (advanced) stated choice experiments. Topics of research involve among others technology and policy acceptance mainly in the field of Transportation. He co-chairs the subcommittee on stated response travel survey methods of the Transportation Research Board, Washington DC.

Kirsten Meeuwisse is a consultant in Cyber Security working at Deloitte. She graduated from the TU Delft of the Master program in Systems, Engineering, Policy Analysis and Management. Her thesis research was about the trade-off between security and usability. Her aim is to make security controls user-friendly. In that way end-users are not annoyed by working with these controls and therefore will not circumvent these security measures, which leads to a more cyber secure world.

Wolter Pieters is an associate professor in cyber risk at Delft University of Technology, faculty of Technology, Policy and Management. He has MSc degrees in computer science and philosophy of science, technology and society from the University of Twente, and a Ph.D. in information security from Radboud University Nijmegen, focused on the controversy on electronic voting in elections. His research interests include cyber risk management, cyber security decision making, and cyber ethics. He was technical leader of the TREsPASS European project on socio-technical cyber risk management, and is currently part of the CYBECO project on behavioural models for cyber insurance.

Caspar Chorus is Professor of Choice behavior modeling at the Faculty of Technology, Policy and Management. His main research aim is to increase the behavioral realism of choice behavior models (mathematical models of decision making), by means of combining recent insights from the behavioral sciences and advances in econometric techniques. His work has received various international prizes, scholarships and personal research grants (including recently a 2 million euro Consolidator grant from the European Research Council). He has pioneered the Random Regret Minimization approach to discrete choice modeling, which has been incorporated in various econometrics software packages, courses, and textbooks worldwide.