The usability-security trade-off

Exploring employees' perceptions and preferences for technical security measures using choice modelling

Kirsten Meeuwisse

September 2016

Abstract

Companies implement technical security measures to let their employees behave in a secure manner. Employees however, can circumvent these measures. To solve this circumventing problem companies should know better what the preferences of their employees are. Employees' preferences with regards to technical security measures are based on the trade-off between perceived usability and security. With the help of choice modelling applied on a survey distributed among employees, this research aims to give insight into this trade-off. This research reveals that in general employees consider usability and security as equally important in their choices for technical security measures.

Keywords. Information security, usability, technical security measures, choice modelling, preferences, perceptions

1 Introduction

Common practice for companies in protecting themselves from data breaches and cyberattacks is the implementation of technical security measures. By these measures, the company tries to force employees to behave in a secure manner. However, despite the forcing character of these measures employees can circumvent them. For example, having strict password requirements forces the employee to choose a difficult password, but an employee can write this down severely decreasing the security level of that measure.

Herley [1] performed research on the reason behind people circumventing security measures. He proposed that people make a cost-benefit analysis of a technical security measure. Whereas benefits can be considered as the perceived security level of that measure and the costs as the effort it takes for employees to align with this measure. In other words costs can also be viewed as the usability of this measure: the more effort required for the employee to use this technical security measure, the less usable they will perceive this measure. The technical security measure with the greatest positive outcome of this cost-benefit analysis will be the preferred technical security measure. Implementing technical security measures that align with employees'preferences reduces the chance of employees circumventing the measures.

Having the technical security measure implemented which is the preferred one of the employee makes the chance of circumventing behaviour on this measure lower.

For companies it would be useful to get insights to their employees' preferences and perceptions of security and usability. In that way companies could adapt their technical security measures to the preferences of their employees, which could decrease the number of circumventions. However, there is little knowledge available about usability and security from the point of view of employees. This research project seeks to address this knowledge gap. The research applies perception-based choice modelling to usability and security of technical security measures. First, the perceived usability and security levels of multiple technical security measures will be measured. Second, the trade-off between perceived security and usability is made explicit by measuring the importance weights of perceived usability and security when employees make choices on technical security measures.

In section 2, related work in the field of usability and security of technical security measures is discussed. A conceptual framework for technical security measures in a company is created in section 3. Section 4 of this paper explains how these aspects will be measured. Section 5 discusses the design of the survey, which is used as a data collection method for this research. The results of the survey are discussed in section 6. Section 7 concludes this paper with the key findings and discusses implications of this study.

2 Related work

The relation between security and usability is an area that recently received attention in the information security research field. Despite the growing awareness that this relation is something to consider, limited research has been conducted in this field. Schultz [2] 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 research results on the relationship between usability and information security." The authors who have written about the topic claimed that security and usability are two conflicting goals: improving one will negatively affect the other [3, 4, 5]. The assumed relation in literature between usability and security is negatively correlated: 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 it is 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 users are likely unwilling to use this computer [6].

In addition to research performed on the high-level relation between security and usability, a small number of researchers conducted research from a more practical point of view: reviewing the usability aspects of multiple technical security measures [6]. These studies, however, faced two major limitations.

Firstly, the majority of these studies focuses on reviewing the usability aspect of technical security measures instead of making the connection with the security level of these particular security measures. In these research, the influence of usability on the security level of the measure is missing [7, 8, 9]. They did not empirically test whether a trade-off exists between both aspects. Is it in fact the case that security and usability cannot be fulfilled at the same time, or could usability and security smoothly go together in practice? New research could focus on the relation between security and usability, rather than reviewing the factors separately [10, 2].

Secondly, the majority of the studies looked into the factual level of usability; the average time it took to complete a task and the number of errors end-users make when using the technical security measure [11, 7, 12]. However, how users perceive usability could be different than the factual measured usability by researchers. In the end, users are the one that have to use the technology and not the researchers. Therefore, it would be interesting to determine the perceived level of usability by the end-users instead of the factual level of usability. The same argumentation holds for factual security. In the majority of the studies the security level of a technical security measure is defined in the number of vulnerabilities or possible successful cyber attacks [13, 14]. Although these things are not that easy to measure, they are the factual measurable metrics of security. However, when a user makes the decision for circumventing a measure or not, they will instead base decisions on what they perceive the security level to be and how they experience the usability level of that specific measure.

The two mentioned drawbacks of previously conducted research in the field of usability and security, support the relevance of this thesis research. On one hand, this thesis provide insights to how employees perceive the usability and security of different technical security measures. On the other hand, this thesis provides insight into the relation between both aspects by making the trade-off explicit that employees make between the importance of perceived security and usability, when choosing between technical security measures.

3 Conceptual framework

A company wanting to improve security has a broad range of options for security methods. Typically, the security department would start with setting up a security strategy. A security strategy entails the direction and focus of the desired security implementations of the company. If a company has a chief information security officer (CISO), then the strategy is developed by the CISO together with the business. Otherwise the security strategy is made by the security or risk department. With the security strategy as starting point, a translation is then made into two types of practical implementations: the code-of-conduct and technical security measures. A code-of-conduct contains guidelines on security behaviour, and are often developed by the CISO together with the HR department. An example of such a guideline is 'make sure you do not leave any confidential information unattended on your desk'. A technical security measure, however, is implemented by the CISO together with the office automation/workplace department. As the name implies, technical security measures are technical measures implemented on the IT systems of the company. An example of such a technical security measure is the installation of a spam filter on the mailbox, so that employees open fewer infected e-mails. An important difference between the two is that codes-of-conduct serve as a guide to employees, whereas technical security measures are forced onto employees. Figure 1 shows the different security methods and their relevant actors in a company.

From all the three security methods (security strategy, code-of-conduct and technical security measures), this research focuses on the third. Employees are using technical security measures on a daily basis and this is not the case for a security strategy or the code-of-conduct. Every time employees use their computer they will be confronted with these technical security measures: they need to authenticate themselves via a password for example. Since employees are regularly making use of

these technical security measures, the impact these technical security measures, have on the daily work of employees is significant. The impact and the forcing character of technical security measures make technical security measures an interesting topic to perform research on.

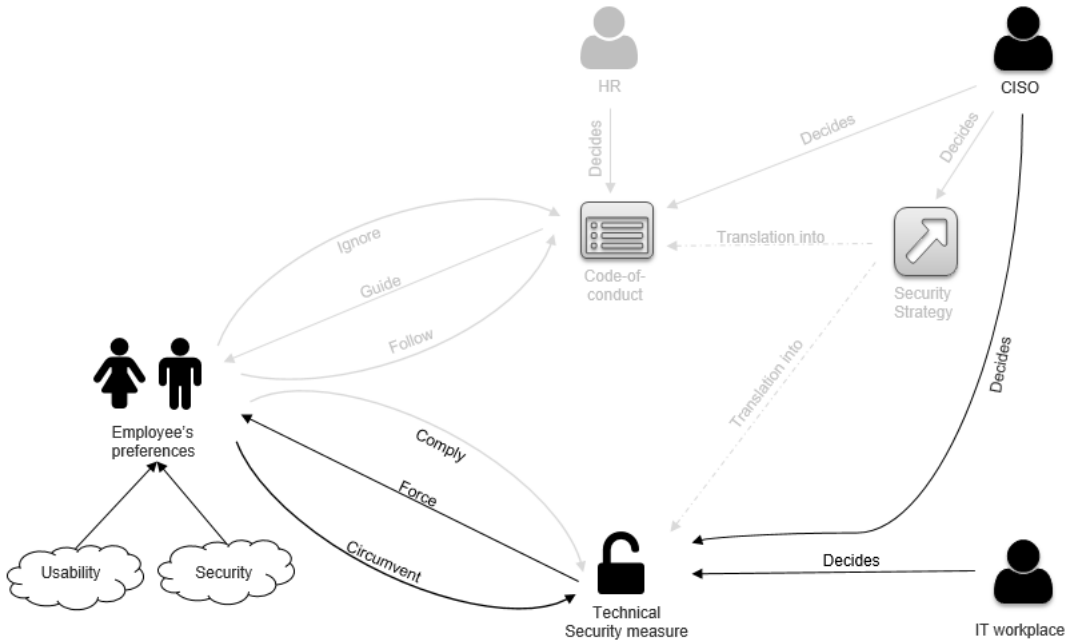

Figure 1: Conceptual framework of security methods in a company

Freedom of choice
Employees normally do not have the choice for which technical security measure to implement. Why would it than be useful to get insight on the preferences of employees for technical security measures? A reason is that this could give companies insights to how their employees would like to see the information security organized. Another option besides ask employees about their preferences for technical security measures, is to ask employees directly about their circumvention of security measures. However, employees could give socially desirable answers on these questions, by pretending as if they would never circumvent technical security measures. Therefore the choice is made to focus on the preferences of employees for technical security measures, as a proxy for their compliancy behaviour.

Technical security measures
No clear definition exists of what a technical security measure entails. The following definition is created by the researcher that will be used in this research: a technical security measure is an electronic security method that protects information on a computer. For this research two parts of the definition are especially important. A security method is only considered a technical security measure when it is an electronic security method. This condition keeps a security code-of-conduct out of the scope. In addition, the security method should be applied on a computer. This removes physical security, such as badges to get into the office, from the scope as well. Since this research

focuses on employees, the technical security measures can be delimited further to measures applied inside a company. This choice is made in order to leave measures employees take at their computer at home outside of the scope.

Literature is reviewed and insights from practice are gathered to see which technical security measures exist and which are suitable to use in this research. As a starting point security measure classes are reviewed to get a broad overview of the technical security measures field. First, it is decided which of these classes fit into the definition used for this research. Secondly, out of these classes a selection is made on which classes this research will focus. Selection criteria used are: interaction with users, suitability for choice modelling, contemporary relevance and comprehensibility for employees. Thirdly, in every selected class, specific technical security measures are placed. Since these technical security measures were still quite broad, specific implementations of these measures were selected for the survey. This selection process resulted in the following list of technical security measures (see table 1).

Table 1: Selected technical security measure implementations

Technical security measure class	**Technical security measure**	**Implementation A**	**Implementation B**	**Implementation C**
Authentication	Password length	Password length no restriction	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
Browsing security	Browsing restrictions	Every browser is allowed	Obligatory browser	
Data loss prevention	File sharing inside company	No restrictions	Via corporate shared drive	
	E-mail to someone outside the company	No e-mail restrictions	Warning message with e-mail	Pop-up message with e-mail which contains confidential words

4 Methodology

To determine usability/security perceptions of employees and to determine the trade-off between perceived security and usability that employees make, input from employees is collected through a survey. In this survey employees were asked to rate the perceived usability and security level of multiple technical security measures. Thereafter employees were asked to choose between combinations of technical security measures. This section discusses the methodologies used in this research to use the data from the survey to calculate perceptions and preferences of employees.

Methods

To analyse the answers of employees on perception related questions in the survey linear regression analysis is used. With linear regression analysis the effect of technical security measures on perceived usability and security is estimated (see line 1 in figure 2). Linear regression can only be applied when the dependent variable(s) are of continuous level. However, the dependent variables in this research are security and usability which are of categorical scale. Violating the assumption of not having a continuous dependent variable, can give problems in relation to the assumed granularity of the dependent variable. Carifio [15, 16] researched this granularity problem and showed empirical evidence that a variable measured on a Likert scale can actually be treated as a variable measured on an ordinal scale, suggesting that the assumption of usability and security as continues variables would not give major implications in this study.

To analyse the answers of employees on the choice related questions of the survey choice modelling is used. Choice modelling makes the decision process of people on a specific trade-off explicit [17]. In this research the choice for technical security measures is measured by estimating the trade-off between perceived usability and security (see line 2 in figure 2).

Figure 2: Overview of the research methods used in this paper

An analysis of the choice model (line 2 in figure 2) can only be done when a specific type of underlying model is assumed. Generally known and used model in this case, is the Random Utility Maximisation model (RUM) [17]. RUM has the assumption that people choose the option that gives them the highest utility [18]. Applied on this research this means that employees will choose the security measures that give them the highest utility. In addition to the RUM model there are a lot of different models which assume choice behaviour based on other concepts than utility maximization. One of these models is that is the Random Regret Minimisation Model (RRM) [19]. In the RRM model is assumed that people choose the option that gives them the least regret. Applied on this research this means that employees will choose the security measures that give them the least regret. To see which of these models fits the data best, a μRRM model will be estimated [20]. In the μRRM a μ will be estimated which determines if the model behave as a RUM model or as a RRM model. Since the μRRM is quite new, in most studies the μRRM model will be compared with the RUM model since this is the conventional widely used model within choice modelling. Therefore, also in this research both models will be compared: RUM and μRRM. This means that the choice model (represented by line 2 in figure 2) is estimated twice. If the underlying choice behaviour of employees is based on utility maximisation, the model fits of the RUM model and the μRRM model will be (almost) equal, since the μRRM model will behave as an RUM model. When the choice

behaviour is based on regret minimisation both models have another model fit, since the μRRM model will behave as an RRM model.

Pilot study
Before the survey was spread a pilot study was conducted among a small number of respondents (31 respondents). This pilot study is used to evaluate the design of the survey; do people understand the questions and do they have any suggestions for improvement? Moreover, the pilot study is used to calculate prior parameter estimates. Priors are estimates of the expected weights of the variables of the trade-off. These priors can be used to specify a more efficient design of the final survey. A more efficient design leads to a smaller number of required respondents for the same reliability (lower standard errors) or the same number of respondents leads to results with higher reliability [21]. Priors can be retrieved from literature or by conducting a pilot survey. Since there is no literature with priors applicable for this research, a pilot study is used to estimate these priors.

5 Survey design

In this research project, data is collected through a survey. The design of the survey should fulfil the goals of the survey: 1) measuring perceptions of employees and (2) measuring choices of employees. To be able to estimate a choice model, choices of respondents on different alternatives are required. Gathering choices on different alternatives in a survey is done by presenting respondents with choice sets containing multiple alternatives. For every choice set, the respondents are asked to choose the alternative they prefer. Furthermore, every respondent is asked about their perception of the usability and security level of these alternatives. Each alternative consists of every security measure from table 1, but with different implementations from table 1 per technical security measure. The technical security measure password expiry frequency for example could vary as follows: package A has a password expiry frequency of once a year, while package B has a password expiry frequency of never.

Between how many packages should the employee choose?
Employees have to choose between 3 different alternatives. Two different models will be tested in this research, as explained in section 2: the RUM model and the μRRM model. The RUM model requires at least two alternatives in a choice. The μRRM model requires at least 3 alternatives per choice. In this survey each choice will contain 3 alternatives, so that both models can be estimated.

How many choice questions should be asked?
Every respondent has to answer 3 choice questions (choice sets). Effect coding is used for the representation of the technical security measure implementations. For example the technical security measure password expiry frequency is coded with two indicator variables PEFOY and PEFOQ, see table 2. This is done in the same way for all the other technical security measures. In total 8 indicator variables are needed to represent 5 technical security measures.

The required number of choice sets for a survey with 3 alternatives per choice question is the number of indicator variables plus one divided by two. This leads to a number of choice sets of 5 (rounding up of (8+1)/2=4.5. To further reduce the number of choice sets per respondents, blocking is used. This means that the choice sets are grouped in multiple blocks. Every respondent is only presented

Table 2: Effect coding of password expiry frequency

Attribute	Attribute level	PEFOQ	PEFOY
Password expiry frequency	Once a quarter	1	0
	Once a year	0	1
	Never	-1	-1

with one of these blocks. Drawback of this blocking technique is that more respondents on the survey are required, since not everybody will answer all the choice sets. For the final survey with 5 choice sets, two blocks of each 3 choice sets are used (since an amount of 5/2=2.5 choice sets is not possible, the amount is rounded up to 3 per block). This results in a survey where every respondent has to answer 3 choice questions.

Which combination of alternatives in each choice question?
The choice sets for this survey are created by specifying an efficient design, which seeks to minimize the standard errors [22]. Creating an efficient design can be done with software called Ngene, based on the priors of the parameters. The priors have been estimated with the results of the pilot study. Together with the desired number of choice sets of 6 (every block gets 3 choice questions) Ngene specified which attribute levels should be in which alternative and which alternatives should be showed together in one choice question.

How to measure perceptions?
Employees are asked to rate their perceived usability and security for every package with technical security measures used in the choice part of the survey. The security and usability levels are measured by the use of a 5-point scale: very user-unfriendly, user-unfriendly, neutral, user-friendly, very user-friendly to measure usability and highly insecure, insecure, neutral, secure, and highly secure to measure security.

Target audience
The target audience of the survey are employees in general. Since this research tries to reveal a broad view on the perceptions and trade-off of employees, every type of employee was allowed to participate in the survey. The only prerequisite was that an employee has to make use of a computer at their work, since all the technical security measures named in the survey where measures applied on a computer.

Final survey
Due to blocking the survey has two different versions. Both versions of the surveys are designed in the survey tool Survey Monkey and every respondent is randomly assigned to one of the versions. The survey has been spread in two large Dutch companies and in personal networks via social media. Snowball sampling is used to reach a larger amount of people whereby people were asked to spread the survey on their social media and they were asked for 3 other people to fill in the survey. This all lead to a total number of 289 responses on the survey. However, 59 responses were partially filled in. Only the data of the 230 employees who fully completed the survey are used in this research.

6 Results

6.1 Perception

Linear regression

The influence of the technical security measures on the perceived level of usability can be determined by estimating the effect that every technical security measure implementation has on the perceived usability and security. These effects can be found in table 3. These estimated effects indicate to what extent the perceived usability/security levels of an alternative with multiple technical security measures change when this specific implementation is in place. The results of table 3 can be summarised as follows:

- The different types of browsing restrictions have the largest impact on the perceived usability level. Which means that the decision for which implementation of browsing restrictions to use will result in the highest change in the perceived usability level. A package with technical security measures which contains an obligatory browser has a way lower perceived usability level than a package where no browsing restrictions are in place. After browsing restrictions password expiry frequency and e-mail restrictions also have a relatively high impact on the perceived usability. For password expiry frequency the difference in perceived usability is large between a frequency of once a quarter and never or once a year. For e-mail restrictions the difference between a pop-up message with e-mails which contains confidential words is perceived as less usable than no e-mail restrictions. The different implementations of file sharing and password length only result in a small difference in perceived usability. Which means that for employees it does not really matter in terms of perceived usability whether a password length with no minimum length or complexity requirements, a password length with minimal 8 characters or a password length with minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character is implemented. The same holds for whether files have to be shared via a corporate drive or whether every application can be used to share files, the difference between both in terms of perceived usability is very small.
- For perceived security, the decision for which implementation of password length to use will result in the highest change. This is caused by the fact that a package with technical security measures which contains a password length with minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character has a much higher perceived security level than a package with a password length with no minimum length or complexity requirements. After the importance of password length on the perceived security comes the importance of password expiry frequency. The difference between a frequency of once a quarter and never in terms of perceived security is large. E-mail restrictions and file sharing are a bit less important for the perceived level of security. For e-mail restrictions this difference in perceived security is caused by the fact that a pop-up message with e-mails which contain confidential words is considered as more secure than no restrictions on e-mail. For file sharing the difference is caused by the fact that employees consider file sharing via a corporate shared drive as more secure than when it is allowed to use every type of application. Important to mention is that the size of the impact of e-mail restrictions and file sharing is only around 50% of the impact that password length has on the perceived security. Least important for the perceived security are browsing restrictions. A package with technical security measures which contains an obligatory browser will only have a small difference in perceived security than a package which contains no browsing restrictions.
- For most of the technical security measures implementations the effect on the perceived level of security is way larger (twice as large or more) than effect on the perceived level of usability. This

means that there is a larger difference of perceived level of security of the different implementations of a technical security measure than on the perceived level of usability. For example, when employees have to use a corporate shared drive for file sharing or when they are free to use any application they want to share their files differs in terms of usability not much, but in terms of security both implementations show a bigger difference.

Table 3: Effects of the technical security measures on perceived usability and security

Technical security measure	**Implementation**	**Effect on perceived usability**	**t-value of effect on perceived usability**	**Effect on perceived security**	**t-value of effect on perceived security**
	Regression constant	3.49	185.52	2.90	156.51
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	-0.05	-1.75	0.58	20.06
	Minimal 8 characters	0.06	1.91	0.02	0.73
	Password length no restriction	-0.01	*	-0.60	*
Password expiry frequency	Once a quarter	-0.24	-8.89	0.42	15.92
	Once a year	0.12	4.43	0.02	0.83
	Never	0.12	*	-0.44	*
Browsing restrictions	Obligatory browser	-0.27	-13.28	0.04	1.83
	Every browser is allowed	0.27	*	-0.04	*
E-mail restrictions	Pop-up message with e-mail which contains confidential words	-0.14	-4.88	0.21	7.42
	Warning message with e-mail	-0.06	-2.39	0.14	5.15
	No e-mail restrictions	0.20	*	-0.35	*
File sharing	Via corporate shared drive	-0.08	-3.76	0.27	13.40
	No restrictions	0.08	*	-0.27	*

R-square usability model = 0.16

R-square security model = 0.41

* For the effects which match with the estimated parameter value of the indicator variable, the t-value is given. The effects of the other technical security measure implementations are not estimated, but derived from the estimated parameter values of the indicator variable(s) of the same technical security measure. Therefore, for those it is not possible to show a t-value.

Correlation

To get a better understanding on how people perceive usability and security the relation between both aspects can be determined. The correlation between perceived usability and perceived security is calculated as -0.14. This negative correlation is a logical consequence of what most of the opposing signs of the effects on perceived security and usability of the different technical measures in table 18 suggests: when the perceived usability level increases by the implementation of the technical security measures the perceived security level decreases and the other way around. This means that this research shows that the correlation in the sample data is indeed negative as literature suggested, but the correlation is not strong (only -0.14).

6.2 Choices

To get insight in the trade-off between perceived usability and security choicemodelling is used. As section 4 explained two different choice models are tested in this research (the RUM model and the μRRM model). Table 4 shows that the RUM model (-472.82) and the μRRM model (-472.82) have an equal model fit. This is logical since the μRRM model can behave as a RUM model when the estimated μ by the μRRM model is very large (5 or larger). The estimated μ of 323 is indeed very large. This means that employees, who are choosing for an alternative with technical security measures, do this based on the principle of utility maximization. The alternative with the highest utility has the highest chance to get chosen by the employees.

Table 4: Model fits of RUM and μRRM

	RUM	**μRRM**
0 log likelihood	-758.04	-758.04
Final log likelihood	-472.82	-472.82
Rho square	0.38	0.38
Number of cases	690	690
μ		323

To get a more detailed insight into the RUM model the betas in the RUM model will be discussed in detail, see table 5. Important to mention is that the model fits shown in table 4 are the model fits of RUM model with only the linear components of perceived security and usability taken into account. However, research reveals that a model with the incorporation of quadratic components next to the linear components show to have a better model fit (-460.77). Therefore, for the remaining part of the paper this latter model will be discussed. Table 5 shows that model with the incorporation of quadratic components. The betas show the weights of the usability and security components when employees are making choices. The table shows that usability is seen as slightly more important than security. However, the 95% confidence intervals for both usability and security reveal that this difference in weights actually cannot be seen as a difference since they mainly overlap with each other. This is in line with the calculated t-ratio of 0.27 for the difference between the betas of linear security and usability, where a |t-ratio| of minimal 1.96 is needed for speaking of a significant difference between the betas (for a 5% significance level). What also can be seen from table 5 is that the betas of the quadratic components are negative, which means that a unit increase in perceived usability/security result in a less strong increase of utility per unit increase. So when the perceived usability and security level of a technical security measure is low one level increase in perceived usability or security has a strong effect on the total utility gained by this measure, whereas when the perceived security or usability level of a technical security measure is high, one level increase in perceived usability or security will have a less strong effect on the gained utility. Also for the quadratic components of usability and security holds that the 95% confidence interval reveals that both betas cannot be interpreted as different compared to each other (consistent with the calculated t-ratio of 0.55 for the difference). Figure 3 is a visual representation of table 5. The error bars show that the difference in contribution of security and usability to utility overlap with each other, which means that the contribution perceived usability and security give to utility is equal.

Table 5: The RUM model

Perceptions	**Beta**	**Std. error**	**t-value**	**Left side of 95% confidence interval**	**Right side of 95% confidence interval**
Security (linear)	2.51	0.40	5.97	1.73	3.29
Usability (linear)	2.68	0.48	5.26	1.74	3.62
Security (quadratic)	-0.19	0.06	-2.94	-0.31	-0.07
Usability (quadratic)	-0.24	0.07	-3.35	-0.38	-0.10

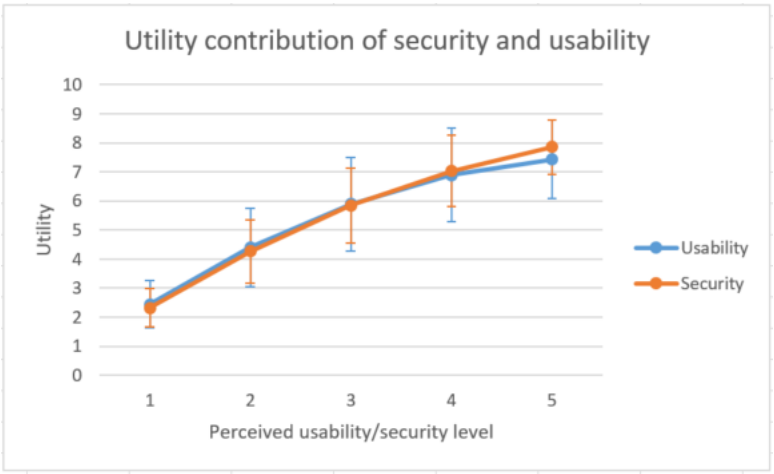

Figure 3: Visualization of the security and usability components in the utility function

Figure 3 is a generalised representation of the security-usability trade-off. However, the trade-off could differ between different kinds of employees, since one employee could make his/her choices based on different weights for perceived security and usability than another. To investigate this potential difference, the interaction effects of the usability and security weights with multiple personal characteristics are estimated. This interaction shows the increase or decrease of the importance of perceived usability or security to be incorporated when an employee with a specific characteristic makes a choice. Most of the researched characteristics are proven to be of insignificant influence.

The characteristic that did found to be of significant influence is 'current employment in the information/cyber security domain'. Employees who are working in the information/cyber security domain consider perceived usability as more important than perceived security. For employees not working in the information/cyber security domain, perceived security is more important than perceived usability in their overall preference towards technical security measures. More research is needed to give a better founded answer on the validity and reasons for this counter-intuitive effect.

7 Conclusions

Research was conducted to gain insight into (1) the way employees perceive usability and security and (2) what trade-off between perceived usability and security employees make. This study shows the perceived usability and security of the technical security measures: password length, password expiry frequency, browsing restrictions, e-mail restrictions and file sharing restrictions. Two technical security measures that have a large effect on either perceived security or perceived usability are: browsing restrictions and password length. Browsing restrictions show to have a large effect on the perceived usability, while having almost no effect on the perceived security. For password length the effect is opposite. Password length shows to have a large effect on the perceived security, while having almost no effect on the perceived usability. For most of the technical security measures holds that when implementation of that measure leads to an increase in perceived security, it leads to a decrease in security or the other way around.
The importance of the perceived usability and security is determined by the trade-off. Research shows that employees make a trade-off between usability and security based on utility maximisation behaviour. This means that the technical security measures which give employees the highest utility have the highest chance to be chosen. This highest utility is determined by the trade-off between perceived usability and security. In general employees consider perceived usability and security equally important. When the usability and security level of a technical security measure is perceived as low, one level increase in usability or security has a strong effect on the total utility gained by this measure, whereas when the security or usability level of a technical security measure is perceived as high, one level increase in usability or security will have a less strong effect on the gained utility.

The modelling approach used in this research warrants some discussion. A first remark is on the hypothetical setting of the survey, where employees had the choice of which technical security measures to implement at their work. This hypothetical choice has two major limitations. Firstly, their choice behaviour may not correspond with their real behaviour. Employees could pretend to be the perfect employee by choosing the alternative with a high level of security, whereas they would actually prefer the other alternative with a high level of usability. Secondly, providing employees with multiple alternatives gives the feeling that they have a choice. This could make them feel better about an alternative than they would feel about the same alternative when it is imposed on them by the company.

Second remark is about whether it was appropriate to compare the correlation between usability and security assumed by literature with the correlation found in this research. In this research, the security level of technical security measures is measured by how employees perceive security. This may not correspond to the factual security level of the technical security measures. Although in literature, it has not been explicitly mentioned that the assumed negative correlation is between factual levels of security and usability, it could be the implicit focus point of these studies. Therefore, the comparison of the correlation found between usability and security with the correlation assumed in literature done in section 6.1 could be not fully correct.

Third remark is on the small scope of this research. Firstly, this research only focused on five different technical security measures, out of the many options available to companies. Although these fives are selected with care (see section 3), this brings limitations in the applicability of this research results on other technical security measures. Secondly, these results are based on the answers of a specific group of respondents. The researcher tried to reach a diverse group of

respondents. However, it could also be argued that the sample has some bias, since the starting point of reaching respondents was the network of the researcher herself. Therefore, it should be stressed that the results of this study only holds in the specific type of environment used for this research. Recommended is to perform further research, for example distributing the same survey but with other technical security measures and among another group of respondents, to see if the results of this study are similar in other environments.

Last remark concerns the assumed effect on the outcomes of this study on the circumventing behaviour of employees. The trigger for this research were employees circumventing measures will lower the security level of the company. It is assumed that employees will circumvent less if a company implements the technical security measures of their preference. However, adapting to employees preferences is not a 100% certainty that employees will circumvent less. Besides the fact that it is good to know for a company what the preferences of their employees are, further research is required to understand if employees are more likely to comply fully with their preferred technical security measures, and the actual impact on the company's information security level.

References

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

[2] E. Schultz, "Research on usability in information security," *Computer Fraud & Security*, vol. 2007, no. 6, pp. 8–10, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1361372307700751

[3] D. Andersson, "Authentication with passwords & passphrases: Implication on usability and security," 2013. [Online]. Available: http://www.rlvision.com/blog/authentication-with-passwords-passphrases-implications-on-usability-and-security/

[4] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference*. IEEE, Conference Proceedings, pp. 275–282.

[5] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in *Cyberspace Safety and Security (CSS), 2011 Third International Workshop*. IEEE, Conference Proceedings, pp. 21–26.

[6] L. F. Cranor and S. Garfinkel, "Guest editors' introduction: Secure or usable?" *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 16–18, 2004.

[7] X. Cao and L. Iverson, "Intentional access management: Making access control usable for end-users," in *Proceedings of the second symposium on Usable privacy and security*. ACM, Conference Proceedings, pp. 20–31.

[8] A. Kobsa, R. Sonawalla, G. Tsudik, E. Uzun, and Y. Wang, "Serial hook-ups: a comparative usability study of secure device pairing methods," in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, Conference Proceedings, p. 10.

[9] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153–164, 2010.

[10] C. Braz, A. Seffah, and D. M'Raihi, *Designing a trade-off between usability and security: a metrics based-model*. Springer, 2007, pp. 114–126.

[11] S. Brostoff, M. A. Sasse, D. Chadwick, J. Cunningham, U. Mbanaso, and S. Otenko, "'r-what?'development of a role-based access control policy-writing tool for e-scientists," *Software: Practice and Experience*, vol. 35, no. 9, pp. 835–856, 2005.

[12] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0," in *Usenix Security*, vol. 1999, Conference Proceedings.

[13] S. L. Garfinkel and R. C. Miller, "Johnny 2: a user test of key continuity management with s/mime and outlook express," in *Proceedings of the 2005 symposium on Usable privacy and security*. ACM, Conference Proceedings, pp. 13–24.

[14] C. Kuo, S. Romanosky, and L. F. Cranor, "Human selection of mnemonic phrase-based passwords," in *Proceedings of the second symposium on Usable privacy and security*. ACM, Conference Proceedings, pp. 67–78.

[15] J. Carifio, "Assigning students to career exploration programs by preference," *Career Education Quarterly*, 1976.

[16] J. Carifio, "Measuring vocational preferences: Ranking versus categorical rating procedures," *Career Education Quarterly*, vol. 3, no. 2, pp. 17–28, 1978.

[17] D. McFadden, *Conditional Logit Analysis of Qualitative Choice Behavior*. New York: Academic Press, 1974, pp. 105–142.

[18] C. F. Manski, "The structure of random utility models," *Theory and decision*, vol. 8, no. 3, pp. 229–254, 1977.

[19] C. G. Chorus, T. A. Arentze, and H. J. Timmermans, "A random regret-minimization model of travel choice," *Transportation Research Part B: Methodological*, vol. 42, no. 1, pp. 1–18, 2008.

[20] S. van Cranenburgh, C. A. Guevara, and C. G. Chorus, "New insights on random regret minimization models," *Transportation Research Part A: Policy and Practice*, vol. 74, pp. 91–109, 2015. [Working Paper]. Available: http://www.sciencedirect.com/science/article/pii/S0965856415000166

[21] J. Rose and M. Bliemer, "Designing stated choice experiments: State-of-the-art," 2007. [Online]. Available: http://www.ivt.ethz.ch/vpl/publications/presentations/v205.pdf

[22] J. M. Rose and M. C. Bliemer, "Constructing efficient stated choice experimental designs," *Transport Reviews*, vol. 29, no. 5, pp. 587–617, 2009.