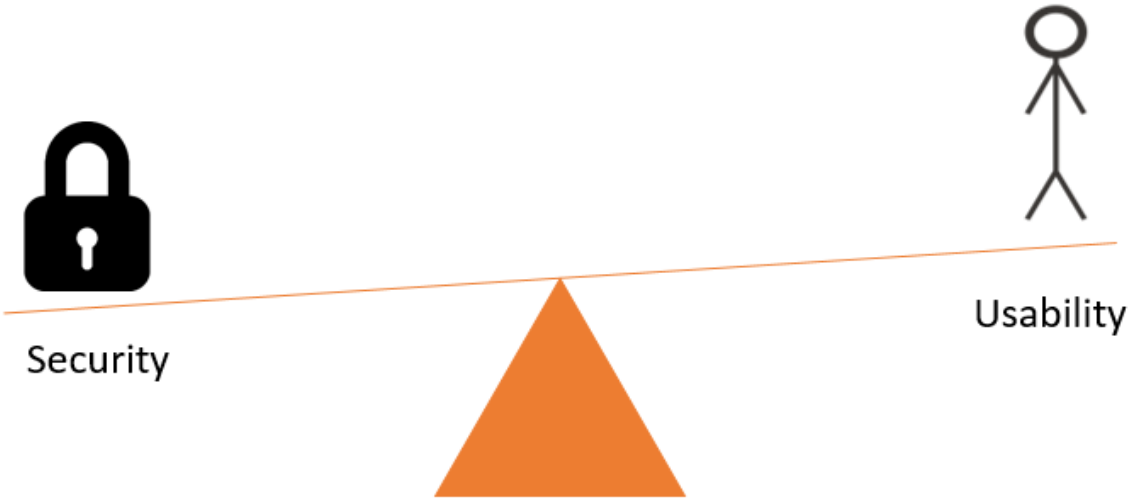
The usability-security trade-off

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

MSc thesis Kirsten Meeuwisse

The usability-security trade-off

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



MSc Thesis of Kirsten Vera Maria Meeuwisse

For the degree of Master of Science in Systems Engineering, Policy Analysis and Management – Information Architecture

Student number: 4079612
Project duration: May 2016 – October 2016

Graduation committee:	Prof. Dr. Ir. Caspar Chorus	chairman, Delft University of Technology
	Dr. Ir. Wolter Pieters	first supervisor, Delft University of Technology
	Dr. Eric Molin	second supervisor, Delft University of Technology
	Jelle Niemantsverdriet MSc MBA	external supervisor, Deloitte

TU Delft

Deloitte.

Preface

Dear reader,

Before you lies my thesis about the trade-off perceived usability and information security from the viewpoint of employees. With this thesis I hope to obtain my Master's degree in Systems Engineering, Policy Analysis and Management at the Delft University of Technology. The last five months I have spent all my time on writing this thesis. Since I am really interested in everything that is related to information security, I mostly enjoyed writing this thesis. I learnt a lot during the process of writing a thesis, especially about the structure and style of writing which is most understandable for the reader.

This thesis would not have been the way it is now, without the help of many people. Therefore, I would like to thank all of them. Firstly, I would like to thank my graduation committee, which supported me throughout the whole process of writing this thesis. Wolter, thank you very much that you have read and reviewed all concept versions I sent to you. Eric, thank you for teaching me how to apply choice modelling and how to design an understandable survey, which is not as easy as I had anticipated. Jelle, thank you that you always had time for me to discuss my thoughts about the direction of my thesis. Caspar, thank you for your enthusiastic interest in my topic and your explanations about regret based choice models. Furthermore, I would like to thank the people from Deloitte, where I did my graduation internship. Thank you for all your enthusiasm and for the interesting reading material and articles many of you have sent to me. Moreover, I would like to thank all my reviewers whom reviewed either the content of a chapter or corrected my English. Thank you for your refreshing ideas and tips. Last, but not least, I would like to thank my family and friends. They had much patience with me during the past five months, when I was sometimes a bit stressed about my thesis or when I had no time for them, because I was busy with this thesis project. Especially I would like to thank Bob for his faith and encouragements.

I enjoyed writing this thesis and I hope you will enjoy reading it.

Kirsten Vera Maria Meeuwisse
Amsterdam
September 2016

Summary

Companies implement technical security measures to ensure their employees behave in a secure manner. Employees however, can sometimes circumvent these measures when they prefer other technical security measures over the ones that are implemented by the company. In such cases, employees might have chosen other technical security measures if they were able to choose these themselves. The choice for technical security measures is determined by the perceived level of usability and security of that specific measure, and by the trade-off between the importance of perceived usability and security in their overall preference towards that measure. However, little knowledge is available about these perceptions and this trade-off. Firstly, it is unknown how employees perceive the usability and security of technical security measures. Secondly, it is unknown what the trade-off is that employees make between the importance of perceived usability and security when choosing for technical security measures. This research tries to fill these two knowledge gaps by answering the following research question: "How do employees perceive security & usability of technical security measures at their work and what is the trade-off they make between these aspects in their choices for technical security measures?"

This research focuses on technical security measures that fall in the category: electronic security methods that protect information on a computer. This results in the following list of technical security measures used in this research: minimum password length, password expiry frequency, browser restrictions, file sharing inside the company and e-mail restrictions on e-mails sent to someone outside the company.

Data for this research is collected via a survey distributed among different kinds of employees. The only prerequisite for participating is that employees should regularly use their computer at work, since the researched technical security measures are all measures applied on a computer. The survey consists of questions related to perceptions of usability and security, and choices for technical security measures. In the survey employees were confronted with multiple packages consisting of different technical security measures. For every package they had to specify their perceptions on usability and security. Thereafter they had to choose, out of multiple packages, which one they would prefer at work. In total 230 employees completed the survey.

The first part of the research question (perceptions of employees) is answered trough linear regression. With linear regression the effect of technical security measures on the perceived level of usability and security is estimated. The second part of the research question (the trade-off) is measured with choice modelling. With choice modelling the choice for technical security measures is measured by estimating the trade-off in weighing perceived usability and security. Applying choice modelling can only be done when a specific type of underlying choice behaviour is assumed. Two types of choice behaviour are reflected on within this research: utility maximisation and regret minimisation behaviour. This means that there is tested if technical security measures that gives employees the highest utility are the preference of employees or if technical security measures that gives employees the least regret are the preference of employees.

The first outcome of the survey is about the usability and security perceptions of employees. The most important technical security measure for the perception of usability is found to be restrictions in the choice of a web browser. When employees had to use an obligatory browser, their usability perception decreased compared to when employees would be free to choose the browser they want. Least important for the perceived level of usability were file sharing restrictions and password length. The different implementations of these technical security measures only result in a small change of perceived usability. The most important technical security measure for the perception of security is found to be password length. Requiring a password length containing a minimum of 8 characters, 1 uppercase letter, 1 special character and 1 numeric character highly increased the perceived level of security compared to a password length with no minimum length or complexity requirements. Also the password expiry frequency has a large effect on the perceived security. Employees perceive an expiry frequency of once a quarter as more secure than an expiry frequency once a year and even as way more secure than a password expiry frequency of never. Browsing restrictions is the technical security measure that has the least impact on perceived security level. Employees perceive an obligatory browser as almost same secure as when there are no browsing restrictions in place.

Important to mention is that for most of the technical security measures the effect on perceived security is twice as large (or even larger) as the effect on perceived usability.

The perceived usability and security levels of the technical security measures also reveals another result: the suspicion by literature that security and usability are contradictory aspects is confirmed by the empirical results of this research. For most technical security measures holds that when the perceived usability level increased by implementing this measure, the perceived security level decreased. This means that perceived security and usability are negatively correlated.

The second outcome of the survey is about the trade-off that employees make when choosing technical security measures between perceived security and usability. The analysis shows that when employees are choosing between packages with technical security measures, they do this based on utility maximisation behaviour rather than on regret minimisation behaviour. This means that the package which gives employees the highest utility has the highest chance to be chosen. The utility of each package is dependent on the levels of perceived usability and security (discussed before) and on the trade-off between the importance of perceived usability and security. This research shows that in general employees consider the following trade-off: employees consider perceived usability and security equally important, which means that when employees would choose which technical security measures to implement, they will consider the perceived usability and security level of these measures as equally important in their overall preference towards these measures.

Analysis on the trade-off also reveals that the importance of an improvement in perceived security or usability is dependent on the current perceived level of security and usability. When the perceived usability and security level of a technical security measure is low, one level of increase in perceived usability or security has a large effect on the total utility gained by this measure. However, 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.

In the analysis of the survey there was also accounted for the potential influence of personal characteristics of employees on the answers employees gave. This analysis reveals that most characteristics of the employees are not of significant influence on the perceptions or the trade-off between the importance of perceived usability and security. From the ones that were found to be of significant influence, the one that has the largest effect is 'current employment in the information/cyber security domain'. Employees who work in the information/cyber security domain consider perceived usability as more important than perceived security, whereas employees not employed in this area consider perceived security as more important than perceived usability. More research is needed to give a better understanding of the underlying reasons that cause this counterintuitive effect.

The outcomes of this research are food for thought. Firstly, recommended for companies is to implement technical security measures more in line with the preferences of their employees. Although this research reveals some insights in these preferences, reality should show if adapting to these preferences indeed will lower the circumvention rate. Secondly, the scope of this research was limited: only five technical security measures where researched. This has implications for the validity of the outcomes of this study for other technical security measures than the ones in scope for this study. More research is needed to see if the trade-off of employees between the importance of usability and security is the same for other technical security measures. Thirdly, it should be stressed that the observations are based on perceived usability and security. So in the outcomes of this research no claims are made about whether one measure is more secure than the other. Finally, it is important to mention that this research is one of the first where choice modelling is applied within the information security research field. Therefore, this study should not be seen as final stage, but as a launching pad for more studies within this research area.

Contents

List of figures and tables

1. Introduction

1.1 Background

The importance of information security has been highlighted by the increasing number of security incidents each year (Identity Theft Resource Centre, 2016; Statista, 2016; Symantec, 2016; Wei, 2016). Common practice for companies in protecting themselves from such security incidents (e.g. data breaches and cyberattacks), is the implementation of technical security measures. In an ideal situation these technical security measures force the employees to behave in a secure manner. However, reality shows that this is not common practice. Despite the forcing character of technical security measures, employees often find a way to circumvent these measures (Dinev, Goo, Hu, & Nam, 2006; Post & Kagan, 2007). For example, the use of the web browser Google Chrome is blocked by the system, but Google Chromium, which is a similar application, is not. Another example, when employees have to change their password on a weekly basis. This is a technical requirement and as an employee you cannot ignore it, otherwise you are not able to access the computer. What you can do as an employee is write down your password on a post-it every week, because you will forget your password otherwise. However, writing down your password decreases the effectiveness of this technical security measure (Brostoff & Sasse, 2000). Both examples reveal that although technical security measures try to force an employee to behave in a certain way, the employee still exhibits undesired behaviour.

Why circumventing?

Since circumventing technical security measures will result in a lower security level of the company, it is important to investigate why employees would circumvent. Herley (2009) made inquiries towards the motivation of people for not complying with technical security measures. He stated that employees make the decision circumventing or not based on a cost-benefit analysis of the technical security measures. In his research, he defined benefits as the "avoidance of the harm that the attack might bring" (Herley, 2009, p. 134). How much harm a technical security measure prevents depends on the information security quality of the technical security measures. Or in other words, the security level of the measure. He defined costs as the effort it takes for the employee to align with the measure. Effort needed on a technical security measure can also be viewed as the usability of this measure. The more effort it takes for employees to use this technical security measure, the less usable they perceive this measure.

Preference

If employees would have the choice between different technical security measures, they would make such a cost-benefit analysis for every technical security measure. The technical security measure that scores the best on the cost-benefit analysis would have the preference of the employee. According to the technology acceptance model (Davis, 1989) this preference towards a technical security measure determines the behaviour of the employee, which means that for the preferred technical security measure the chance that the employee would circumvent the measure would be low. Therefore, although in real life employees are not able to choose between technical security measures (since the company makes this decision), it would be interesting to know the preferences of the employees on technical security measures. When the preferences of employees are known companies could change their technical security measures to the ones preferred by their employees in order to lower the circumvention rate.

Perceptions and trade-off

When employees make a cost-benefit analysis of technical security measures, they do this based on two inputs. Firstly, on the height of the costs and benefits and secondly, on the weights of the costs and benefits. Applied on this research this means that this cost-benefits analysis consists of the security and usability level of the technical security measures (height of the costs and benefits) and on the trade-off between the importance of security and usability (weights of the costs and benefits).

The security and usability level of a technical security measure can be measured in two ways: actual usability and security (factual level) or perceived usability and security (subjective level). Actual security is how secure the technical security measure is according to security experts and security tests. Perceived security is how secure the user thinks the technical security measure is. Since this research focuses on employees, perceived usability and security level is interesting to look at. It could be that a

technical security measure is according to the specifications not secure, but end-users perceive it as very secure.

The weights of security and usability can be measured by an importance trade-off. Do employees see usability as more important aspect than security in their choices for technical security measures or do they see it the other way around?

Knowledge gap

To summarize, employees working in a company are confronted with technical security measures. Employees perceive a certain level of usability and security of these measures. Based on the trade-off between those perceived levels they have a certain preference towards a technical security measure. This (non-) preference is a reason for circumventing this measure or not. In this described situation there are two aspects still unknown. It is unknown how employees perceive the usability and security of technical security measures, and it is unknown what the trade-off is that employees make between the importance of usability and security. This research tries to fill these two knowledge gaps.

1.2 Theory

As explained above, this research is interested in the importance trade-off between perceived security and usability, because this determines the preference for a particular technical security measure. This preference could be tested by letting employees choose between different technical security measures. In offering this choice, the security and usability levels of the technical security measures can be varied to identify what trade-off employees make between weighing both aspects and how these affect their choice. Discrete choice modelling is a way to investigate a trade-off. Choice modelling makes the decision process of people on a specific trade-off explicit (McFadden, 1974). In choice modelling the choices people make between different alternatives are analysed by looking to the different characteristics of these alternatives. Each alternative has multiple characteristics. Humans make a trade-off between how important they find each characteristic, based on that they make a choice of which alternative they prefer. It is important to mention the difference between choice, preference and trade-off in this theory. People choose the alternative they prefer based on a trade-off. In case of this research: a choice for technical security measure A or B is made by determining which measure is most preferable, which is decided based on how the trade-off between the importance of the perceived usability level and the perceived security level is for each measure.

Choice modelling assumes that choices are a result of the cognitive decision-making process of an individual (Timmermans, 1982). "This assumes that choice alternatives can be described in terms of their physical, functional, and socioeconomic attributes" (Molin & Marchau, 2004, p. 120). These attributes are factual attributes e.g. price of an alternative. Normally in choice modelling, the trade-off between such factual system attributes would be determined. This research wants to determine the trade-off between perceived usability and security. However, perceived usability and security are no system attributes, but subjective attributes. Every person differs in the perception of these attributes. Normally choice modelling does not take attributes that are subjective in itself into account. This research wants to determine the trade-off between two subjective terms and therefore traditional choice modelling is not possible. This thesis will not be the first one who will try to catch perceptions in a choice modelling experiment. A possible way to do this is described in the paper of Molin and Marchau (2004). They let users make their perceptions explicit by asking them to rate, for example, their perceived safety, based on system attributes such as speed. This thesis uses the implementation of measuring perceptions performed by Molin and Marchau (2004) by letting people rate their experienced usability and security levels based on system attributes.

1.3 Research objective & research questions

The objective of this research is to provide companies with insights on how their employees perceive security and usability and what the most desirable balance is between both aspects for their employees. These insights can be translated into recommendations for companies that encourage a configuration of technical security measures that is more consistent with their employees' preferences. If companies can adjust their technical security measures to the preferences of their employees, employees would probably

circumvent these technical security measures less. This let companies become closer to the ideal situation where employees comply with technical security measures.

The main research question that will be answered in this thesis is:
"How do employees perceive security & usability of technical security measures at their work and what is the trade-off they make between these aspects in their choices for technical security measures?"

Different sub-questions need to be addressed in order to be able to answer the main question. The sub-questions are:

1. What technical security measures exist and which of these are suitable for researching the trade-off between usability and security?
2. How do employees perceive the usability and security level of the selected technical security measures?
3. What is for employees the trade-off in weighing perceived usability and security when choosing between different combinations of technical security measures?

1.4 Added value of the thesis

1.4.1 Added scientific value

Very little research has been conducted on the trade-off between usability and information security and thus this thesis could be one of the first expanding into this research field. In addition, as far as the author knows, there never has been made a link between the choice modelling theory and information security. Also in this case this thesis could be a first trial. Schultz (2005) underlined the need for more papers on the human factor in information security. Applying choice modelling in the field of information security will provide the information security research area with more insights about the human factor in information security. Lastly, this research tries to capture perceptions into a choice model, which is not new, but not that often performed in choice modelling.

1.4.2 Added value to practice

The deliverable of this research will be empirical results about (1) how employees perceive security and usability of technical security measures and (2) about the trade-off employees make between security and usability when preferring technical security measures. These empirical insights could enable companies to create a better design of implemented technical security measures by striking the right balance and height (according to their employees) of usability and security. This could improve the security level of companies, since employees would comply better with the technical security measures when they are better adjusted with their wishes. Helping companies by improving their security will help the society by better protecting confidential data that the company owns. This will help in protecting IT systems in general and thereby making the society a bit more secure.

1.5 Thesis outline

The second chapter of this thesis will discuss background information of important variables of this research. In the third chapter the methodology that is used in this research will be explained. More detailed information on how choice modelling is applied in this research will be discussed here. The fourth chapter describes which technical security measures will be used in this research. The fifth chapter explains the chosen design for the experiment used in this research. This is followed by the results of the experiment in chapter six. Thereafter answers to the sub-questions and the main research question will be given in chapter seven. This chapter also provides recommendations for future research and for companies, the relative position of this research in literature and discusses the limitation of this research.

2. Relevant variables

In this research, three aspects are very important: usability, security and technical security measure. To get a better understanding of these variables, this chapter will review literature and use practical experience to gain more background knowledge about these variables. Furthermore, this knowledge will provide reasons on why these aspects are relevant to research.

2.1 Usability and security

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 (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 research results on the relationship between usability and information security." The authors that did research the topic claimed that security and usability are two conflicting goals: improving one will negatively affect the other. Andersson (2013) for example stated that techniques which increase security tend to decrease usability. Kainda, Flechais, and Roscoe (2010) supported that statement by saying that security and usability are at odds. Nurse, Creese, Goldsmith, and Lamberts (2011) even asked themselves if usable security actually is an oxymoron.

Figure 1 makes the assumed relation in literature between usability and security explicit. Usability and security seems to be negatively correlated: if security goes up, usability goes down and if usability goes up security goes down. Consider a computer without a password. It is clearly very 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 (Cranor & Garfinkel, 2004).

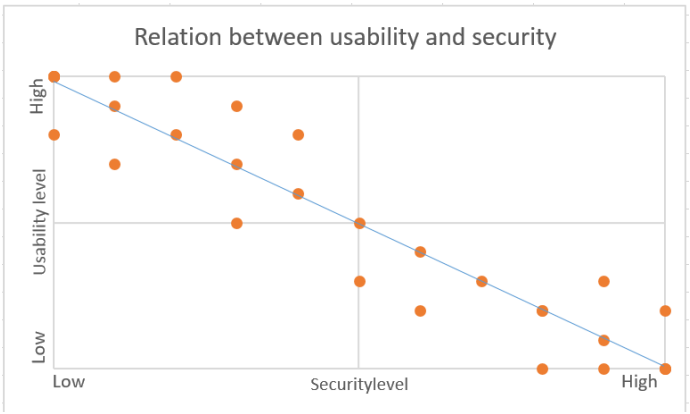


Figure 1 - Assumed security usability relation

In addition to research performed on the high-level relation between security and usability, such as figure 1, a small number of researchers conducted research from a more practical point of view: reviewing the usability and security aspects of multiple technical security measures (Cranor & Garfinkel, 2004). These studies, however, faced two major limitations.

Firstly, the majority of these studies focused on reviewing the usability aspect of technical security measures instead of making the connection with the security level of these particular technical security measures. Kobsa, Sonawalla, Tsudik, Uzun, and Wang (2009) conducted an experiment to test the usability of different forms of secure device pairing. Although they performed an extensive user experiment on usability, they barely mention the security level of each secure device pairing method. Cao and Iverson (2006) conducted research on the usability of access control mechanisms. Also in this research, the focus was fully on the usability aspects of the technical security measure rather than reviewing the implications this have on the security level of the measure. Weir, Douglas, Richardson, and Jack (2010) studied the usability of different authentication methods in online banking. They fully focused on the usability experience of the end-user but did not mention the difference in security level of the evaluated authentication methods. In all of the mentioned studies the influence of usability on the security

level of the measure is missing. 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 (as figure 1 suggest), 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 (Braz, Seffah, & M'Raihi, 2007; Schultz, 2007).

Secondly, the majority of the studies looked into the factual level of usability, rather asking people about how they perceive the usability. Brostoff et al. (2005) measured the usability of an authentication mechanism. They measured usability by the number of failed log-ins and the time it took for every user to get logged in. Cao and Iverson (2006) researched the usability of access control mechanisms by measuring speed and accuracy of the users actions with the access control mechanism. Whitten and Tygar (1999) perform a usability study of an encryption mechanism. They measured usability by given participants of their study specific tasks they had to perform and then measuring the time it took to complete the tasks, measuring how many errors the participants made and measuring how many tasks the participants were able to complete at all. The studies are examples of how usability can be measured with measurable facts. However, how users perceive usability could be different than the factual measured usability by researchers. Researchers could measure for example, a short task performance time and thereby assuming that the measure is usable, while end-users (although they were able to complete their task fast) perceive the measure as unusable since they did not like the user interface. Kainda et al. (2010, p. 277) supported this by saying that "while objective analysis of usability analysis of systems is common, users' subjective assessment is crucial to a systems success". 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. Garfinkel and Miller (2005) measured the security of a specific type of e-mail protection by measuring the robustness of the measure against certain attacks. Kuo, Romanosky, and Cranor (2006) measured the security of specific password types by measuring the crackability of these passwords. Both studies shows that security is measured with factual measurable metrics of security. However, when a user makes the decision for circumventing a measure or not, they will 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.

2.2 Employees

An important part of the scope of this research are the employees. The main focus of this research is to generate conclusions on how employees generally perceive usability and security and which trade-off they make between these aspects. However, not every employee is the same and every individual could perceive usability and security differently, as well as make alternative trade-offs between usability and security. Therefore, generalisation is likely to inaccurately represent the opinions and behaviour of the employees. A solution to this problem is to incorporate work related factors of employees into this research. This would make it possible to distinguish the perception of usability and security among specific types of employees, as well as to distinguish in the trade-of they make in weighing both aspects. Literature is reviewed to see which work related factors could be of influence.

Literature

Multiple studies mention the importance of the size of a company for security (Baker & Wallace, 2007; Ernest Chang & Ho, 2006; Kankanhalli, Teo, Tan, & Wei, 2003; Post & Kagan, 2007). They assume that bigger companies have more money, thus more money to spend on security. Consequently, it is assumed that more attention will be paid to information security in bigger companies via security awareness. Translating this assumption to this research results in the following hypothesis: employees working in bigger companies will find security more important than employees working in a smaller company.

Another important factor for security in a company could be the business segment of the company (Baker & Wallace, 2007; Ernest Chang & Ho, 2006; Kankanhalli et al., 2003; Post & Kagan, 2007; Stanton, Stam, Mastrangelo, & Jolton, 2005). Every sector implements information security in a different way. If a company operates in a riskier environment, it is likely to put more resources on information security. Therefore, it is expected that employees working in different sectors will weight the importance of security differently. No specific hypothesis can be formulated about the direction of the influence of this type of sector, since literature does not provide suggestions as to which sectors would put more resources on information security than others.

Another possibly determining factor could be security related job. Post and Kagan (2007) stated in their research that for jobs concerned with information/cyber security, employees will estimate the effectiveness of technical security measures lower. Translating this assumed relation to this research results in the following hypothesis: Employees working in the information/cyber security domain will perceive the security level of technical security measures lower than employees not working in the information/cyber security domain.

Practice

Besides the factors identified by the literature, there are various other work related factors that could be of influence on the research. Brainstorming together with a professional security advisor resulted in the following additional factors, which could also be tested with the survey of this research: years working for the company, job type of the employee, percentage of computer use at work, perception of sensitivity level of information at work, and whether security awareness training has been followed. The first work related factor is years working for the company. The longer an employee works for a company, the more he/she is used to the norms and values and habits of the company. These norms, values and habits could concern the usability and security importance. The number of years working for a company could influence the trade-off and perceptions of employees. The second possible factor that could be of influence is the job type of the employee. Depending on the type of work employees perform, employees could think differently about security and usability. Literature assumed that the sector in which the company operates is the factor of influence, but it could be that job type explains the difference between employees. An example could be that secretary A and manager B have a different opinion about security and usability, although they both work for a company in the same sector. The third factor is the perceived level of sensitivity of information at work. Sensitive information requires a higher level of security. A hypothesis for this research is: employees who perceive the sensitivity of the information they work with as low, would perceive security as less important. Lastly, a work related factor is whether employees have followed a security awareness training or not. Security awareness training is a widely used measure to make employees more aware of information security. The hypothesis is that employees who have followed a security awareness training perceive security as more important than employees who have not.

2.3 Technical security measures

The introduction chapter already explained that this research focuses on technical security measures inside a company. However, technical security measures are not the only security methods that a company can implement to be better secured. To see the relative position of technical security measures within these security methods possible and to get a broader view on how companies implement security methods and which different actors are involved, a conceptual framework is made. Since this is a rather practical implementation, this framework is not based on literature, but on conversations with two security professionals who have implemented security strategies and security transformations in multiple different companies. Important is to keep in mind that this picture is not the only way how security can be organised in a company. The picture sketched here is a generalisation of what is most commonly seen by these experts.

Security methods

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 2 shows the different security methods and their relevant actors in a company.

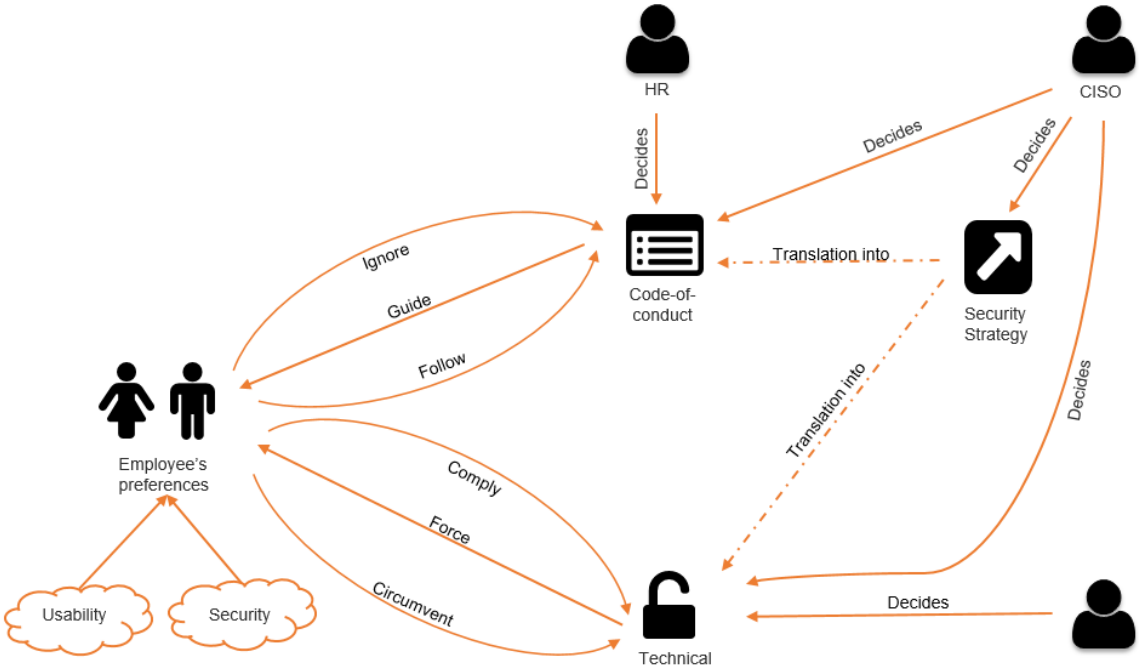


Figure 2 - Conceptual framework of security methods in a company

Power deviation

Important to mention about security methods inside a company is that there exists a power deviation. The CISO has decision power on which security methods to implement. However, employees have influencing power by ignoring or circumventing these security methods. This power deviation is an important aspect, because the decision power could give the company the idea that he/she can guide and force the behaviour of the employees by deciding which security methods to implement. However, the power of employees in this situation should not be forgotten. Although they are not able to decide which security methods to implement, they can influence the effectiveness of the security methods, by their (circumventing) behaviour.

Scope

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 are 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.

2.4 Conclusion

The literature review revealed the importance of this research on the relation between security and usability. Literature also supports the viewpoint of this research, which is the viewpoint of employees. Therefore, this research is not about (the trade-off between) usability and security, but rather about (the trade-off between) perceived usability and security. By focusing on employees, it is important that they are not generalized and are focussed on individually. Practical experience is used to create a conceptual framework around technical security measures; the relation it has with actors and other security methods. Figure 3 shows the scope of this research inside the conceptual framework.

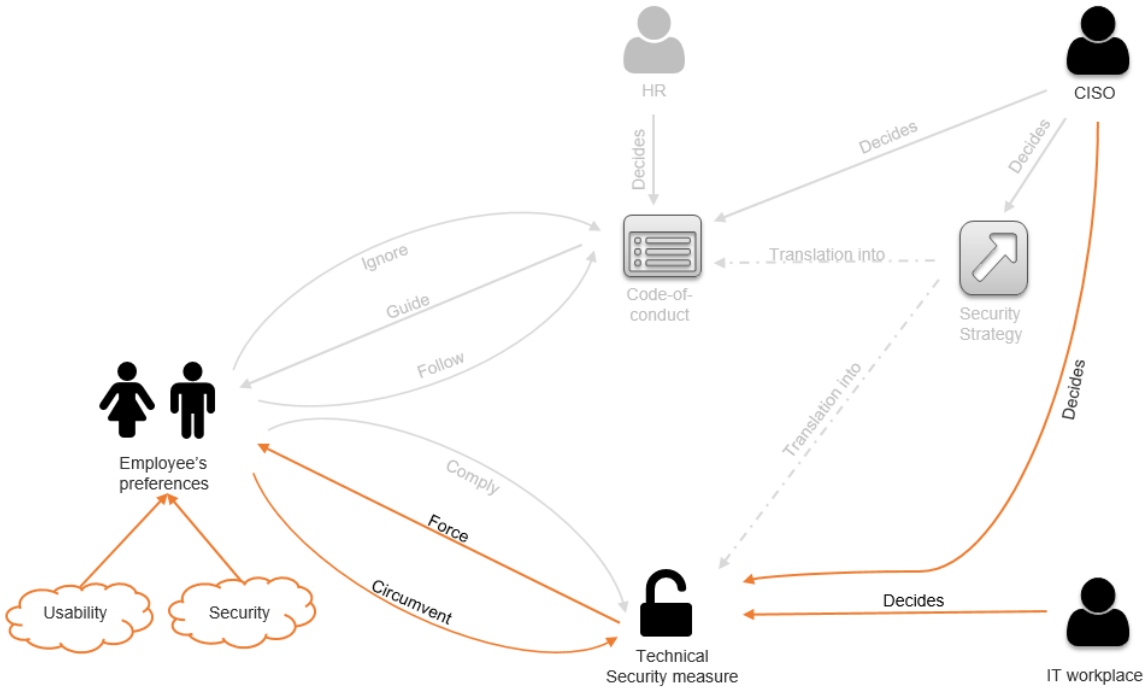


Figure 3 - Scope of this research

3. Methodology

3.1 Introduction

The introduction already reveals that choice modelling is the main method used in this research. However, choice modelling is a rather broad concept and it should be specified in which manner choice modelling should be applied in this research. This and other methods that will be used in this study will be discussed in this chapter. This chapter only contains explanations about how the research is going to be conducted. The research itself will be performed in chapters four through six.

3.2 Selecting technical security measures

The first step in this research is to determine the scope of the technical security measures. Which technical security measures should be taken into account and which are left out of this research? This demarcation starts with providing a definition of what is perceived as a technical security measure. No clear definition exists in literature and therefore the definition that will be used in this research should be constructed.

Second step is creating an overview of existing technical security measures. Literature review is the method that is used for this purpose. For this literature review synonyms of a technical security measure are used to find information. These synonyms are security controls, technological security measures, technical security solutions and technical security tools. Databases used for this search are Google Scholar and Scopus. However, since a technical security measure is rather a practical concept, non-academic websites are used as an information source as well. For this purpose, the search engine of Google is used.

Technical security measures are practical implementations of a security strategy. A practical view on the list of technical security measures created by the literature review, would be a useful additional method. For information from practice, professional security advisors are asked to review the list of technical security measures.

When the list of technical security measures is finalised, the next step is selecting some of these measures. Selection criteria that are used, are the influence on the employee, suitability for choice modelling and contemporary relevance. More information on the selection of these criteria can be found in chapter four. The result of the used methods is a short list with technical security measures that will be used in the choice modelling experiment.

3.3 Survey

3.3.1 Security and usability trade-off

In order to analyse choices that are based on a trade-off, data is required. When applying choice modelling there are two ways of data gathering. One possible way is to make use of revealed preferences. Revealed preferences are real-life choices made by the users. The data gathering is conducted by observing these actual choices. However, observing the choice behaviour of employees is not possible in this research. As figure 2 from chapter two already revealed, choosing which technical security measures should be implemented in companies, is made by the CISO and not by the employees themselves. Since employees do not make these choices, observing employees will not result in observing choices for technical security measures. What observing employees can reveal is some of the circumvention behaviour of employees. For example, employees writing down their password on a post-it is observable. However, not every circumventing behaviour is publically observable. Some circumvention behaviour is only visible on the computer of the employees. For example, an employee uses Google Chromium although Google Chrome is blocked by the system. Problem with this circumvention behaviour is that can result in some privacy restrictions. An employee does not want that their computer use and circumvention behaviour is monitored. Due to these privacy concerns and not being possible to observe choices of employees, revealed preferences is not a suitable way of data gathering for this research.

A second option for collecting data in choice modelling is called stated choices. In this option people are asked what choices they would make, when choosing between different options. The difference with revealed preference is that employees are confronted with a hypothetical question in stated choice (what

would they choose if), while real choices are observed in case of revealed preference. Ideally, research is conducted on real choices instead of hypothetical choices, but since observing revealed preferences is not possible, hypothetical choices are a good alternative. Advantage of choosing stated preference as data gathering method is that data can be collected with the help of a survey which is easily distributed. Instead of asking people about their preferences for technical security measures, another option would be to ask people about their circumvention behaviour. However, employees could give socially desirable answers by saying that they do not circumvent technical security measures. To prevent this, asking people about their preferences for technical security measures is used as a proxy for circumvention behaviour.

Design

The design of a choice modelling survey consists of multiple elements: attributes, alternatives and the choice question. The choice question in a choicemodelling survey is: 'which alternative would you prefer?' The attributes are the selected technical security measures and alternatives are combinations of these attributes. For this research multiple alternatives (packages) are presented which contain multiple technical security measures. An employee is asked which alternative he/she prefers. Figure 4 shows three possible alternatives and the choice between them. Next step is to decide which combinations of technical security measure implementations are packed together in each alternative and to determine the number of choice questions. This is done with the help of an efficient design.

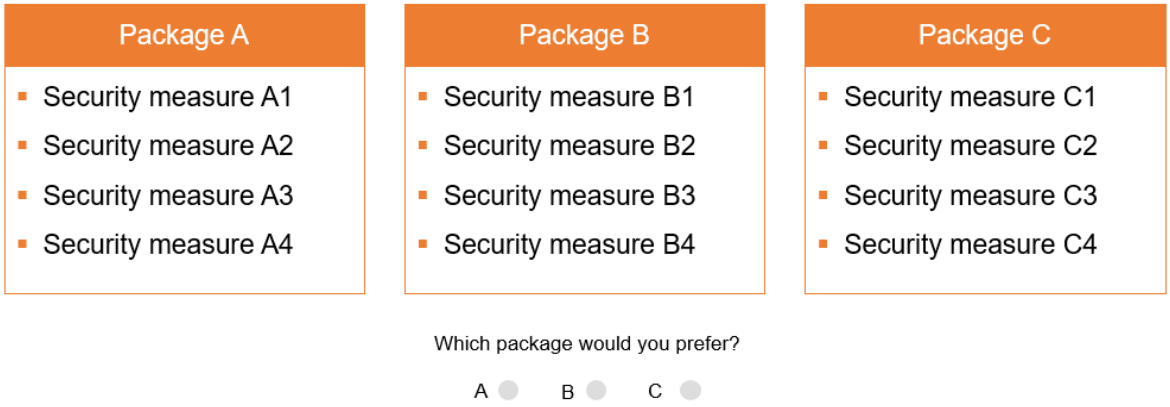


Figure 4 - Example of possible choice question in the survey

Efficient design

The goal of an efficient design is to have maximum information extraction: extract as much information as possible from the choice questions. This can be achieved by balancing the utilities of the alternatives in each question (Molin, 2016). This means that dominance of an alternative should be avoided. For example, one alternative has an estimated probability of 95% to be chosen, will probably not reveal new information about a trade-off. A situation where one alternative has 60% probability to be chosen will add a lot of new information about the trade-off. The result of this efficient design is that the survey will be shorter and more efficient, because useless choice situations (e.g. given three alternatives, one alternative has a probability of 95% being chosen) are deleted from the survey by the efficient design. Required input for an efficient design are prior estimates. Priors are estimates of the expected parameter values of the variables of the trade-off. The prior estimated will be used to create a survey design that result in the lowest possible standard errors. This leads to a smaller number of required respondents for same reliability or the same number of respondents lead to results with higher reliability (Rose & Bliemer, 2007). Priors can be retrieved from literature or by conducting a pilot survey. Since there exist no literature with priors applicable for this research, a pilot study will be used to estimate these priors. This pilot study will be conducted among a small number of respondents (approximately 20/30 respondents).

Freedom of choice

In choice modelling, the choice question (see figure 4) is normally asked to respondents when respondents of the survey actually have the freedom of choice on the presented alternatives. In this research this is not the case, since in reality the decision power is in the hands of the CISO (see section 2.3). The employees only have influencing power by their circumventing behaviour. Even without the

actual freedom of choice it is still useful to ask employees about a hypothetical choice situation, because this could give companies insights to how their employees would like to see the information security organized. Important to mention is that employees are not asked in the survey which choice they would make in case they were the CISO, but which choice they would make when they would have choice freedom in the same role they currently have. This is an important distinction, because asking employees about their choices when they would be CISO would results in different answers. Employees would understand the responsibility for information security that comes with being CISO and that could make security more important to them than it is to them now in their current employee's role.

3.3.2 Perceptions

In addition to the fact that this research tries to determine the trade-off employees make between the importance of security and usability, the aim of this research is to also give insight in the perceived usability and security level of technical security measures. Measuring perceptions can be done in a survey with the help of rates. Possible rates for security are for example highly insecure, insecure, neutral, secure, and highly secure.

Employees are asked to make their usability and security perceptions explicit by rating the security and usability level on this predefined scale. This can be analysed with regression analysis. With regression analysis the influence of different independent variables on the dependent variables can be estimated (de Vocht, 2009). In this research, the dependent variables are usability and security. The technical security measures are the independent variables in this research. So through regression this research estimates the influence of different technical security measures on the perceived level of security and usability.

Sequence of questions

When implementing questions about the perceived usability and security levels in the choice modelling survey there are two options: first asking respondents to value security and usability, before letting them choose the most preferable alternative or first asking respondents to make choices and thereafter let them make their perceptions explicit. It is decided to use the last option in the survey of this research, since the other option has a big drawback. When the other sequence would be used, first asking choices and thereafter asking perceptions, employees will try to explain their earlier made choice for an alternative by giving usability and security levels which can logically be derived from the made choice. In literature this problem is referred to as cognitive dissonance. Cognitive dissonance relates to a situation where perceptions of people are not in line with their behaviour (L. Festinger, 1962). When people are confronted with such dissonance they want to disestablish this dissonance. People will try to change their perceptions to let it correspond with their behaviour (Leon Festinger & Carlsmith, 1959). Since changing perceptions is easier than changing behaviour. In the sequence of questions chosen for this research changing perceptions based on the made choices would be harder, since people are first being asked to make their perceptions explicit before let them make choices. Figure 5 shows an example of how the sequence of questions will look like by using the chosen sequence.

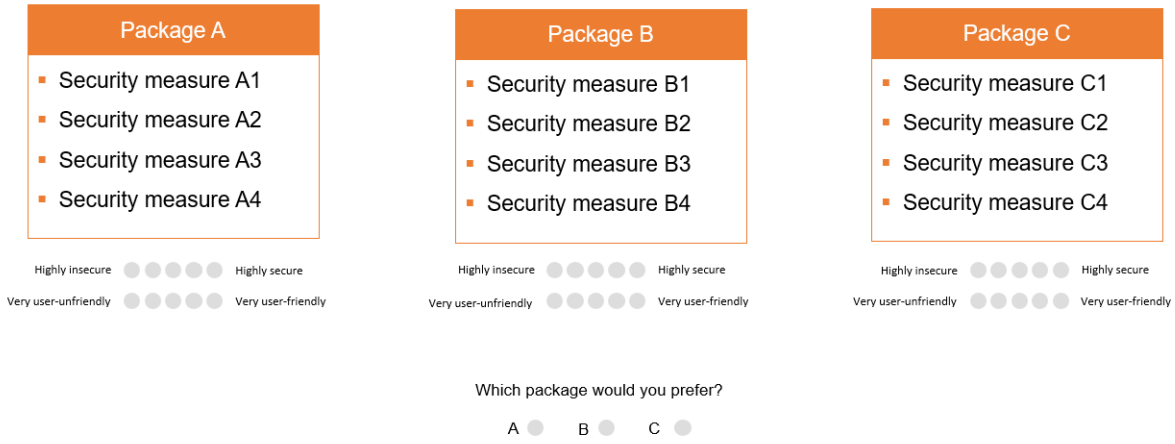


Figure 5 - Possible combined question in the survey

3.4 Analysis of the data

Perceptions and trade-off combined

A result of the choice for the design in figure 5 is that three different models can be estimated. The first model is a regression analysis on the influence of the technical security measures on the perceived usability and security level (see line 1 in figure 6). The second model is a choice model which assumes that employees choose an alternative with technical security measures based on the usability and security levels of this alternative (see line 2 in figure 6). It could be argued that employees do not consider usability and security at all when making a choice for a specific alternative. They could choose based on other concepts than security and usability. This possibility is the third model (see line 3 in figure 6). It is difficult to decide in advance which model of the two choice models (line 2 and 3) applies best, because no prior knowledge exist on the trade-off of employees between usability and security. Therefore, both of these choice models are tested to see which one fits best to the data.

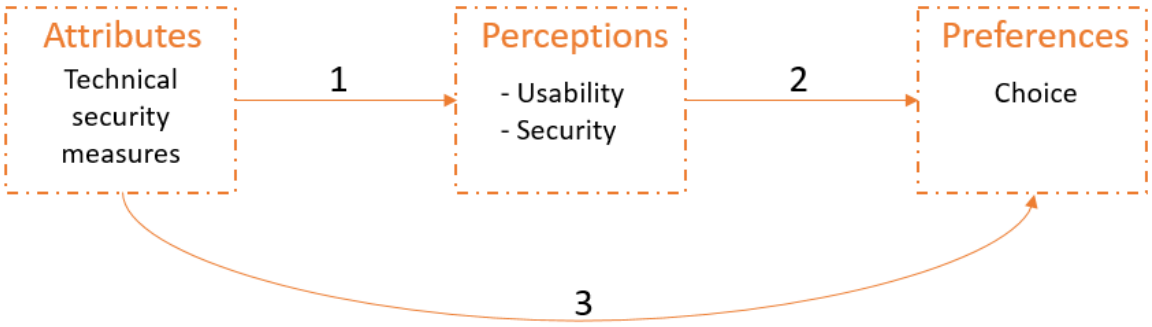


Figure 6 - The models that will be applied in this research

Linear regression

To calculate the impact of technical security measures on perceived usability and security a specific type of regression analysis will be used. One of the most straightforward and easy to interpreted forms of regression analysis is linear regression. Before linear regression can be applied, an important assumption of this method has to be met: dependent variable(s) should be of continuous level (Laerd Statistics, 2013). However, the dependent variables in this research are security and usability which are not measured on a continuous scale, but rather on a categorical scale (e.g. highly insecure up to highly secure). Violating the assumption of not having a continuous dependent variable, gives problems in relation to the assumed granularity of the dependent variable. In linear regression it is assumed that the distance between every unit of the dependent variable has the same size. However, in case of this research it is doubtful if the distance between highly insecure and insecure is the same as the distance between insecure and neutral secure for example. Carifio (1976, 1978) researched this difference in granularity 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.

Utility maximisation and regret minimisation model

Analysing the choice models, visualised in figure 6 by line 2 and 3, can only be done when a specific type of the underlying model is assumed. In choice modelling theory there are a lot of different underlying models. Generally known and used model is the Random Utility Maximisation model (RUM) (McFadden, 1974). RUM has the assumption that people choose the option that gives them the highest utility (Manski, 1977). Applied on this research this means that employees will choose the technical 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 concepts other than utility maximisation. One of these models is the Random Regret Minimisation model (RRM). RRM assumes that people choose the option that gives them the least regret (Chorus, Arentze, & Timmermans, 2008). "Regret is the emotion that we experience when realizing or imagining that our current situation would have been better, if only we had decided differently" (Zeelenberg & Pieters, 2007, p. 3). Zeelenberg and Pieters (2007) support the assumption of RRM that people are regret averse. In the area of information security, technical security measures are designed to prevent regret. Technical security measures try to protect

companies from data breaches. In case the company has implemented no technical security measures or not the right one to block a cyber-attack, the company feels regret that they did not invest enough in their security. Due to the logical connection to security, the RRM model is interesting to look at. Recently an expansion to the RRM model was made: the μRRM model (van Cranenburgh, Guevara, & Chorus, 2015). Difference with the RRM model is that the μRRM model makes it possible to estimate the shape of the regret function, whereas in the RRM one fixed shape is assumed. Another advantage of the μRRM model is that it also can approach RUM model behaviour. Within the μRRM model a μ will be estimated which determines if the model behave as a RUM model or as a RRM model. This property makes it logical to only use a μRRM model, since this can estimate both a RUM and a RRM model depending on the μ. However, since the μRRM is quite new, in the majority of the studies the μRRM model will be compared with the RUM model because this is the conventional widely used model within choice modelling. Therefore, also in this research both models will be compared: RUM and μRRM. If the μRRM model behaves as a utility maximisation based choice model, the model fits of RUM and μRRM will be the same. But if the μRRM model behaves as a regret minimisation choice model, the model fits of RUM and μRRM will be different. This means that the choice models represented by line 2 and 3 in figure 6 are both estimated twice. The first time assumed that people make choices based on utility maximisation (RUM), the second time assuming that people make choices based on either regret minimisation or utility maximisation dependent on the estimated μ by the model (μRRM).

To explain the two models more in detail formulas (1) and (2) show the different models applied on the assumption that employees choose based on perceived usability and security (represented by line 2 in figure 6). The formulas in which people choose based on the technical security measures (represented by line 3 in figure 6) follows the same principles only perceived security and usability would then be replaced by the technical security measures.

RUM model

$$Ui = \beta_{usability} * Usability + \beta_{security} * Security + \epsilon \quad (1)$$

Where

$U_i = Utility\ of\ alternative\ i$

$\beta i = Weight\ of\ perceived\ usability\ or\ security$

$Usability = Perceived\ usability\ level$

$Security = Perceived\ security\ level$

$\epsilon = randomness$

In a RUM model for each alternative a utility is calculated. The utility of an alternative consist of the perceived security and usability level and a corresponding beta. This beta represents the weight of perceived usability and security. When for example perceived usability is considered very important to employees when choosing an alternative, the beta of perceived usability will be high. The last component of the RUM formula is a randomness factor. This randomness factor represents the utility that cannot be explained by perceived usability or security, so the utility of the alternative that is gathered via something else than perceived usability or security.

μRRM model

$$RR_i^{\mu RRM} = \mu*(-ln(1 + exp[(\beta_{security}/\mu) * (Security_j - Security_i)]) - ln(1 + exp[(\beta_{security}/\mu) * (Security_k - Security_i)]) - ln(1 + exp[(\beta_{usability}/\mu) * (Usability_j - Usability_i)]) - ln(1 + exp[(\beta_{usability}/\mu) * (Usability_k - Usability_i)])) + \epsilon \quad (2)$$

Where

$RR_i = Regret\ of\ alternative\ i$

$\mu = Scaleparameter$

$\beta i = Weight\ of\ perceived\ usability\ or\ security$

$Usability_i = Perceived\ usabilitylevel\ of\ alternative\ i$

$Usability_j = Perceived\ usabilitylevel\ of\ alternative\ j$

$Usability_k = Perceived\ usabilitylevel\ of\ alternative\ k$

$Security_i = Perceived\ security\ level\ of\ attribute\ i$

$Security_j = Perceived\ security\ level\ of\ attribute\ j$

$Security_k = Perceived\ security\ level\ of\ attribute\ k$

$\epsilon = Randomness$

In the µRRM model for each alternative a regret is calculated. Regret exists when another alternative than the chosen one, would actually have been a better choice. Therefore, in the µRRM formula the levels of security and usability are compared with the levels of the other possible alternatives continuously. In case of formula (2) the perceived security of alternative i is compared with the perceived security of alternative j and of alternative k (same holds for perceived usability of alternative i, j and k). In the µRRM also a µ component is estimated. The µ represents the scale parameter of the regret function. The estimated µ tells what kind of function the estimated regret follows (see Figure 7 (van Cranenburgh, 2015)). As said a µRRM model can also approximate a RUM model. This is the case if a µ of ∞ is estimated. In reality a µ larger than 5 already correspond to a RUM model behaviour. In formula (2) also a randomness term exists, to gather the regret that cannot be explained by usability and security.

Figure 7 - Possible µ in the µRRM model

Socio demographic & work related factors

In the survey employees will also be asked about their personal characteristics. Firstly, social demographic questions will be asked, such as age and gender. Secondly, work related questions will be asked as well, such as company size and company sector. These questions are added to get an understanding of the type of employees that have participated in the survey. In addition, these extra questions could give insight if different type of employees have a different perception of usability and security and if they make different choices. This can be done by adding interaction effects to the utility/regret function. The significance of these interaction effects will be tested. If these effects don't prove to be significant, it can be concluded that in the population there exists no difference in the choices, given a specific social demographic or work related factor.

3.5 Conclusion

In order to answer the formulated sub questions in the introduction, a few steps have to be followed. First the scope of this research, which technical security measures will be taken into account, should be determined. This will be done by a combination of literature review and practical experience. The selected technical security measures will be used as attributes of alternatives in the survey. Then a pilot study will be performed. This pilot study will be conducted among a small number of respondents. This pilot study will test how people evaluate the survey: do they have tips/tricks how it can be improved? This pilot study can already give an insight in priors as well. This small insight can be used to make the final survey more efficient. The design of the final survey will be adapted to all the insights and gathered knowledge from the pilot study. After the final survey is conducted, the analysis of the data can start. In the analysis part three models will be estimated: a linear regression model and two choice models. Which choice model will fit best to the data will be determined afterwards. These models will be tested under two different conditions: people make choices based on utility maximisation and people make choices based on regret minimisation. These assumptions are tested, to see which one fits the data best. Last step of the analysis is the analysis of the influence of personal characteristics of the respondents. When all these steps are performed, the sub questions and subsequently the main research question can be answered.

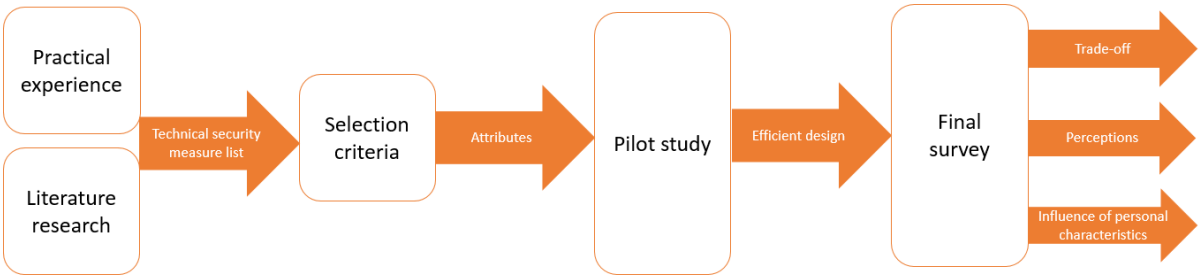


Figure 8 - Methodology overview

4. Selecting technical security measures

4.1 Introduction

The first step in answering the main question of this research is deciding what technical security measures to take into account. Before this decision can be made, a definition of a technical security measure should be given. Thereafter, a list can be made containing different technical security measures. However, since a technical security measure is such a high-level term, a top-down approach will be used to create such a list with technical security measures. The first step in this top-down approach is determining different classes within the area of technical security measures. This will be done in twofold: by (1) reviewing literature and (2) discussing the results of this review with professional security advisors. Second step is making a selection from which of these classes will be used in this research. This demarcation will be done with the help of multiple selection criteria. The last step is selecting the specific technical security measure from each class that will be used in the survey. This chapter will follow all these steps.

4.2 Definition of technical security measure

No clear definition exists of what a technical security measure entails. To clarify what is meant by a technical security measure the following explanation will be used in this research: a technical security measure is an electronic security method that protects information on a computer. For this research the two underlined 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.

4.3 Technical security measure classes from literature

Literature research on technical security measures resulted in four different papers discussing possible technical security measure classes. Every paper makes its own differentiation in classes of technical security measures. The one paper does this more extensively than the other. However, every paper that mentions technical security measure classes, no matter to what extent, is taken into account for this research. Reason is that most reviewed papers in the field of technical security measures are only focusing on one specific technical security measure, rather than on the classification of these measures. Therefore, the four papers that (even slightly) mention classification are used in this research.

Nurse et al. (2011) mention six different areas of technical security measures: authentication, encryption, firewalls, secure device pairing, access control, and secure interaction. Merete Hagen, Albrechtsen, and Hovden (2008) indicate five types of technical security measures: personal passwords, anti-virus software, redundancy of critical systems, intruder detection systems, and firewalls. Kainda et al. (2010) divide technical security measures in six different categories: authentication, encryption, device pairing, public key infrastructure, security tools, and secure systems. In the United Kingdom a document was published with ten critical areas where and how to reduce cyber risk (Communications-Electronics Security Group, Department for Business Innovation & Skills, Centre for Protection of National Infrastructure, & Cabinet Office, 2012). The areas described are information risk management regime, secure configuration, network security, manage user privileges, user education and awareness, incident management, malware prevention, monitoring, removable media controls, home and mobile working. An overview of the different classes identified by the four different papers can be found in table 1.

Table 1 - Overview of technical security measure classes in literature

Nurse et al. (2011)	Merete Hagen et al. (2008)	Kainda, Flechais et al. (2010)	Communications-Electronics Security Group et al. (2012)
Authentication	Personal passwords	Authentication	Information risk management regime
Encryption	Anti-virus software	Encryption	Secure configuration
Firewalls	Redundancy of critical systems	Device pairing	Network security
Secure device pairing	Intruder detection systems	Public key infrastructure	Manage user privileges
Access control	Firewalls	Security tools	User education and awareness
Secure interaction		Secure systems	Incident management
			Malware prevention
			Monitoring
			Removable media controls
			Home and mobile working

4.3.1 Fit the definition

Due to the fact that multiple definitions of a technical security measure exist, it could be that the classes identified by these papers do not fit to the definition of a technical security measure as used in this research. This paragraph filters these classes out of the overview.

The first class that does not fit in the definition used in this study is the class 'secure interaction' in the paper of Nurse et al. (2011). 'Secure interaction' is the general interaction between the computer and the end-user. This can be seen as the user-interface the end-user sees when using his/her computer. A widely used term within the information security society for the user-interface of security methods is HCIsec: Human computer interaction security (Fidas, Voyiatzis, & Avouris, 2010). This cannot be seen as a specific technical security measure class according to the definition used for this study, because it is a general principle that applies to each technical security measure. Each measure should have an easy-to-use user interface. Therefore, this described class by Nurse et al. (2011) is not used as a separate class in this research.

Another class that is eliminated from the list for this research is the class 'secure systems' as Kainda et al. (2010) propose. The authors use this class to capture all remaining technical security measures that do not fit in one of the other classes they defined. By definition such a leftover class is not very specific and is therefore undesirable in this research.

The cyber risk publication of the Communications-Electronics Security Group et al. (2012) does not mention technical security measures, but addresses ten critical areas where to reduce risk. Although they do not mention the term technical security measure specially, the areas they discuss could be useful input for classifying technical security measures. Logical consequence is that the classified areas contain multiple areas that do not fit to the definition of a technical security measure used in this study. The first area is the area 'information risk management regime'. This area contains themes such as creating a governance framework and making information security part of the board's agenda. This area cannot be considered as a technical security measure, because it contains no technical component. The same holds for the area 'user education and awareness'. This category focuses on creating security awareness among users via trainings and campaigns. The third area that does not fit in the definition of a technical security measure is 'incident management'. This area focuses on how to act when an accident happens. An example of a

measure inside this category is an incident response plan. Also for this category holds that it does not contain a technical component and therefore this class is not used in this research.

Having filtered out the classes that do not fit the definition of a technical security measure as used in this study, the following overview of classes remains.

Table 2 - Classes in literature that fit the definition of technical security measures

Nurse et al. (2011)	Merete Hagen et al. (2008)	Kainda, Flechais et al. (2010)	Communications-Electronics Security Group et al. (2012)
Authentication	Personal passwords	Authentication	Secure configuration
Encryption	Anti-virus software	Encryption	Network security
Firewalls	Redundancy of critical systems	Device pairing	Manage user privileges
Secure device pairing	Intruder detection systems	Public key infrastructure	Malware prevention
Access control	Firewalls	Security tools	Monitoring
			Removable media controls
			Home and mobile working

4.3.2 Overlap

The four papers define their own classification of technical security measures. These classifications can be compared with each other to reveal similarities. In this paragraph an analysis will be performed to identify classes that cover approximately the same topic and can thus be clustered together.

Authentication

Authentication is defined by Wiedenbeck, Waters, Birget, Brodskiy, and Memon (2005, p. 1) as "the process of determining whether a user should be allowed access to a particular system or resource". The purpose of an authentication mechanism is to avoid access to people which are not allowed to get into the system. Nurse et al. (2011) and Kainda et al. (2010) both identify the class authentication. Merete Hagen et al. (2008) address the class personal passwords. Which is a generally known example of a specific technical security measure in the authentication class. The three classes are thus clustered in the class 'authentication'.

Encryption

According to Rouse (2014b, para. 1) encryption is "the conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties". In other words: if person A sends a message to person B, encryption transforms the message in such a way that person C is not able to gain significant information about the content of that message (Bellare, Desai, Jokipii, & Rogaway, 1997). An example of a technical security measure in the encryption class is encryption on an e-mail message sent to others. The papers of Nurse et al. (2011) and Kainda et al. (2010) both mention the class 'encryption'. Since they both used the same class name, the class used in this study will also be named 'encryption'.

Network security

The Communications-Electronics Security Group et al. (2012) propose the class 'network security'. Network security protects the business network from connecting to untrusted networks. A related class to network security is the class 'intrusion detection systems' (IDS) identified by Merete Hagen et al. (2008). "An IDS inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system" (Parekh, Madan, & Tugnayat, 2012, p. 84). Another technical security measure related to network security is the class 'firewalls' proposed by Merete Hagen et al. (2008) and Nurse et al. (2011). A firewall is

"security software that checks the traffic flowing between a personal computer and the network(s)" (Raja, Hawkey, Jaferian, Beznosov, & Booth, 2010, p. 53). The purpose of a firewall is to block all harmful software trying to get into the computer. Since IDS and firewalls are also concerned with network security, these classes are clustered with the class 'network security'. Kainda et al. (2010) identify the class 'security tools'. Security tools "are systems that help users manage their security" (Kainda et al., 2010, p. 276). These tools include, for example, password managers and firewalls. This means that 'security tools' can be split into two and can be clustered with respectively the 'authentication' and 'network security' clusters.

Secure device pairing
A proposed class by both Nurse et al. (2011) and Kainda et al. (2010) is 'secure device pairing'. 'Secure device pairing' is referred to as setting up a security association between two devices (Uzun et al., 2007). An example of a device pairing measure is making use of a Bluetooth connection to connect a mobile phone with a computer. 'Secure device pairing' will as well be used as a technical security measure class for this study.

Access control
'Access control' is a technical security measure class proposed by Nurse et al. (2011). Access control mechanisms put limits on who can see or use a (shared) resource (Whalen, Smetters, & Churchill, 2006). The purpose of access control is to avoid people who are, for example, not allowed to write to a file, changing the content of a file. A similar topic is addressed in the publication of the Communications-Electronics Security Group et al. (2012): 'managing user privileges'. This class stresses that the right accounts with specific privileges should belong to the right user. Since access control is a more general name, this name will be used as an overall name for both proposed classes.

Anti-virus software
Merete Hagen et al. (2008) propose the class 'anti-virus software'. An anti-virus program scans your computer on viruses and thereafter removes them (Sharpened Productions, 2010). The goal of an anti-virus program is to protect the computer from harmful programs, which are already installed or are about to be installed. The Communications-Electronics Security Group et al. (2012) suggest the area 'malware prevention' . Malware is "software that is specifically designed to gain access or damage a computer without the knowledge of the owner" (Symantec, 2010, para. 1). A common way to prevent a computer from infection by malware is to install an anti-virus program. Malware will not be seen as a separate class, but will be part of the anti-virus class.

4.3.3 Non-overlapping classes

In addition to classes identified by multiple authors which (partly) overlaps, there are also classes identified by only one of the authors. For each class will be discussed how the authors describe these classes to gain a better understanding of how these can be used as classes for this study.

Redundancy of critical systems
Merete Hagen et al. (2008) propose the class 'redundancy of critical systems'. In case a critical system is damaged or does not work (properly), a back-up system must be in place that can take over all tasks of that particular critical system (Belden & Hirschmann, 2011). 'Redundancy of critical systems' will be used as a class for this study as well.

Browsing security
Kainda et al. (2010) suggest the class 'public key infrastructure'. "Public Key Infrastructure is the combination of software, encryption technologies, and services that enables a company to secure its communications and business transactions on the Internet" (Khosrow-Pour, 2006, p. 553). Kainda et al. (2010) state that inside the field of technical security measures PKI mostly focuses on secure web browsing behaviour of users. To stay in line with their suggested scope, and since encryption is already part of another class, a new technical security measure is added to the list of classes: 'browsing security'.

Secure configuration
Communications-Electronics Security Group et al. (2012) propose the class 'secure configuration'. This class copes with maintaining your software up-to-date and have the latest patches installed. This in order to prevent hackers to exploit vulnerabilities discovered in the software. This class is added to the list with classes used for this research.

Monitoring
Monitoring is another class that Communications-Electronics Security Group et al. (2012) propose. Security monitoring consist of tools that monitor all the traffic on the network and host systems. Objective is to indicate an attack by continuously monitoring unusual activities or trend. Also 'security monitoring' is used as a class for this study.

Removable media controls
Another area proposed by the Communications-Electronics Security Group et al. (2012) is 'removable media controls'. Removable media controls prevent theft of information and the introduction of malware. Possible technical security measures in this area can be blocking all removable media or scanning every removable media before it can be used. 'Removable media controls' are also used as a technical security measure class in this study.

Secure remote working
The last category Communications-Electronics Security Group et al. (2012) suggest is home and mobile working. Technical security measures within this category are encryption, for example encrypting the data on a laptop in case of theft, and making secure connections with the corporate network when working from a location outside the company. Since encryption is already covered by another class, this category will only focus on the secure connection when working remotely. Therefore, this class will be called 'secure remote working'.

Conclusion
After combing and discussing all the classes extracted from the four found papers, a final list with technical security measure classes is composed. Table 3 shows an overview of this list.

Table 3 - Selected technical security measure classes from literature

Technical security measure class definitions	
Authentication	"The process of determining whether a user should be allowed access to a particular system or resource" (Wiedenbeck et al., 2005, p. 1).
Encryption	"The conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties"(Rouse, 2014b, para. 1).
Network security	Protect the business network from connecting to untrusted networks (Communications-Electronics Security Group et al., 2012).
Secure device paring	Setting up a security association between two devices (Uzun et al., 2007).
Access control	"Set limits on who can (or cannot) see or use a shared resource" inside a company (Whalen et al., 2006, pp. 1517-1518).
Anti-virus software	Protect the computer from harmful programs which are already installed or about to be installed.
Redundancy of critical systems	In case a critical system is damaged or does not work (properly), a back-up system is in place which can take over all tasks of that particular critical system (Belden & Hirschmann, 2011).
Secure configuration	"Proactively and continuously hardening the security configurations of operating systems, applications and network devices" (Piper, 2013, p. 1)
Browsing security	Restrictions put in place on the browsing behaviour of the user.
Security Monitoring	"The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions" (Bejtlich, 2004, para. 1).

Removable media controls	Prevent theft of information and the introduction of malware by removable media
Secure remote working	"Provide remote workers with a secure access to the corporate network" (Richmond, 2012, para. 4).

4.4 Security measure classes from practice

Since technical security measures are practical in nature, it is useful to improve the list extracted from literature with practical knowledge. Together with two security advisors who have performed security improvement projects for multiple companies, the list in table 3 was reviewed. In this validation process the classes identified from the literature are discussed to identify possible gaps. This paragraph discusses the improvements proposed by the security advisors. The security advisors suggest adding the following technical security measure classes: end-point protection and data loss prevention (DLP).

The first suggestion is to extend the anti-virus class to a class called end-point protection. End-point protection is more than only anti-virus, it also involves for example anti-spyware (Kassner, 2011). This suggestion for broader scope of the anti-virus class will be implemented in the technical security class list.

The other category that is suggested by the security advisors is data loss prevention (DLP). "DLP is a strategy for making sure that end-users do not send sensitive or critical information outside the corporate network" (Rouse, 2014a, para. 1). The difference with access control is that DLP focuses on information sharing with parties outside the company, whereas access control focuses on information sharing within a company. By introducing the concept of DLP the earlier defined class 'removable media controls' will no longer be a separate class. On one side removable media controls focuses on preventing viruses, which is now covered in end-point protection. On the other side it focuses on securing confidential information from being spread outside the company. This last part is now covered inside the DLP class.

After combining literature with practical experience a final list of technical security measure classes is composed that will be used in this research. Table 4 provide an overview of the final list of classes.

Table 4 - List of technical security measures from literature and practice

Technical security measure class	definition
Authentication	"The process of determining whether a user should be allowed access to a particular system or resource" (Wiedenbeck et al., 2005, p. 1).
Encryption	"The conversion of electronic data into another form, which cannot be easily understood by anyone except authorized parties"(Rouse, 2014b, para. 1).
Network security	Protect the business network from connecting to untrusted Networks (Communications-Electronics Security Group et al., 2012).
Secure device paring	Setting up a security association between two devices (Uzun et al., 2007).
Access control	"Set limits on who can (or cannot) see or use a shared resource" inside a company (Whalen et al., 2006, pp. 1517-1518).
Endpoint protection	Protection of each device in the corporate network from different types of viruses.
Redundancy of critical systems	In case a critical system is damaged or does not work (properly), a back-up system is in place which can take over all tasks of that particular critical system (Belden & Hirschmann, 2011) .
Secure configuration	"Proactively and continuously hardening the security configurations of operating systems, applications and network devices" (Piper, 2013, p. 1).
Browsing security	Restrictions put in place on the browsing behaviour of the user.

Security monitoring	The collection, analysis, and escalation of indications and warnings to detect and respond to intrusions on the network (Bejtlich, 2004, para. 1).
Data loss prevention	"A strategy for making sure that end-users do not send sensitive or critical information outside the corporate network" (Rouse, 2014a, para. 1).
Secure remote working	"Provide remote workers with a secure access to the corporate network" (Richmond, 2012, para. 4).

4.5 Selecting technical security measure classes

The list from table 4 is too extensive and long to perform a detailed research on every technical security measure class. Therefore, only a selection of technical security measure classes will be used in this research. This selection is performed with the help of three selection criteria. The first selection criterion is the interaction with the users. This research is interested in the perceived levels of security and usability of technical security measures. In order for employees to give a judgement about the usability of a technical security measure they should experience a kind of interaction with the specific technical security measure. Otherwise, for example, in case the technical security measure is just running on the background without the employee noticing it, no usability component is visible for the employees. The second selection criterion is suitability for choice modelling. This choice modelling experiment will be distributed among all different kind of employees. No requirements are specified on the type of employees participating in the survey, besides that they sometimes should make use of a computer at work. Because no pre-knowledge of an employee can be assumed, it is important that every employee is familiar with the technical security measure class. In the survey one can give a brief explanation of the technical security measure, but if an employee is not familiar with the technical security measure, judging and making a choice would be difficult. The third criterion is contemporary relevance. With contemporary relevance is meant that the technical security measures used for this research should not be outdated, but are actually used nowadays. Otherwise the relevance of the results and recommendations of this research is limited. This paragraph discusses the suitability of each technical security measure class on the three selection criteria. If a technical security measure class do not satisfy one of these selection criteria the class will be out of the scope of this research.

Authentication

The class 'authentication' is based on letting end-users perform an action before they can get access to the system. It does not matter what kind of authentication is used, fingerprint scanning or logging in with a password, in any case the employee has to interact with the system. Also every employee is probably confronted with authentication at their work, or otherwise at their home computer or at their mobile phone. Therefore, authentication is suitable for choice modelling.

Encryption

On 'encryption' it is more difficult to give a general judgement whether an interaction is taking place with an employee or not. Frequently used applications of encryption are data encryption of a laptop and e-mail encryption. Data encryption on a laptop mostly requires a numeric encryption key. From the point of view of end-users, remembering and inserting this key can be seen as a password measure. This is already dealt with in the authentication class. Another type of encryption is e-mail encryption. When encrypting an e-mail the end-users have to perform certain steps before encryption is successful. Whitten and Tygar (1999) study the usability of these steps. They found that the tool they tested, PGP, does not contain a sufficient user interface. The problem with e-mail encryption in case of this research is the fact that it is tool-dependent how the usability is classified. The tested program of Whitten and Tygar (1999) is just one of the possible programs possible for encrypting e-mail messages. Therefore, it is not possible to implement encryption in the choice modelling survey.

Network security

Network security mostly does not involve any operation of the user. Firewalls and IDS are running in the background of the company's computer and the employees are not confronted with the firewall. Consequently, network security will be outside the scope of this research.

Secure device pairing
Secure device pairing requires an action of employees: they have to type in a code on one or two devices. Sometimes the action contains typing on one device the code displayed on the other device, or it could be typing the same code into two devices. Although multiple options exist for connecting two devices with each other, basic methods such as typing in codes for establishing a Bluetooth connection can be easily explained in a choice modelling survey. The problem with this category is that manually connecting two devices with each other is outdated. Nowadays users can login with their own account on both devices and see and add their files and settings to this account on both devices. So although secure device pairing methods could be used inside a choice modelling experiment, the class will not be included in the research, because of the outdated character of this technical security measure.

Access control
The class 'access control' is about which employee has access to which file. Although in most cases this is predefined by the system, as a user you still are confronted with drawbacks of this technical security measure. For example, you want to have access to a file, but you are not in the department of the person who published this file. The technical security measure in place only allows you to access files of your department. Although you did not perform an action to make this technical security measure work, you experience the drawback of not having access. So there exists an interaction between the technical security measure and the end-user. For employees it would still be possible to value the usability of this technical security measure. Access control is therefore suitable for this research.

Endpoint protection
The class 'endpoint protection' will not be in scope for this research. Anti-virus software runs on the background of a laptop without the user noticing it is running. It would be impossible for employees to give a judgement about the usability of anti-virus software or other background running endpoint protection mechanisms.

Redundancy of critical systems
Redundancy of critical systems is also not a technical security measure that an average employee is confronted with. Making critical systems redundant is something the IT department does. Even in case of a breakdown of the critical system and the back-up server taking over, the employees probably will not notice this. Redundancy of critical systems will thus not be in scope for this research.

Secure configuration
Secure configuration is a technical security measure that must be performed by the IT department, but no interaction of an average employee is required. Updates and patches are mostly automatically pushed to the system and an employee do not notice this. Secure configuration will therefore also be out of the scope of this research.

Browsing security
Browsing security has two main implementation types: restrictions on which browser to use and restrictions on which websites to visit. As an employee you are confronted with these restrictions in case you download a browser which is not allowed or in case you visit a website from the blacklist of the company. The user will in these cases discover the drawbacks of the technical security measure. The fact that every employee uses the internet to require information, makes this technical security measure also suitable for the choice modelling survey.

Security monitoring
Monitoring is a measure that runs on the background of the computer. An IT department monitors specific traffic that flows over the network. As an employee you will not be able to judge the usability of this measure, because you are not confronted with it. What an employee can judge is the privacy aspect of monitoring. However, privacy is not in scope of this research, the focus is only on usability and security. Therefore, security monitoring will be out the scope of this research.

Data loss prevention
An employee could be confronted with data loss prevention when sending for example an e-mail. The DLP system could block specific e-mails that contain confidential company information. As an employee you are confronted with the fact that you are no longer allowed to send an e-mail and this have an influence on the usability level you experience. Although DLP is not implemented in every company, it will be possible to simply explain a specific instance of DLP to the respondents of the survey. Therefore, DLP will be in scope of this research.

Secure remote connection
When users work remotely, they have to establish a connection with the corporate network to get access to specific files and programs. Establishing such a connection has to be done with the help of the user. Mostly a key or password is required before such a connection can be made. Since working from home is supported by more and more companies (CBS, 2015), most employees will be familiar with this technical security measure. Secure remote working will therefore be in the scope of this research.

Conclusion
After selecting the technical security measure classes that are suitable for the purpose and the methods used in this study, a final list with five technical security measure classes remains. Table 5 provides an overview of these classes.

Table 5 - List of technical security measure classes in scope of this research

Technical security measure class	definition
Authentication	"The process of determining whether a user should be allowed access to a particular system or resource" (Wiedenbeck et al., 2005, p. 1).
Access control	"Set limits on who can (or cannot) see or use a shared resource" inside a company (Whalen et al., 2006, pp. 1517-1518).
Browsing security	Restrictions put in place on the browsing behaviour of the user.
Data loss prevention	"A strategy for making sure that end-users do not send sensitive or critical information outside the corporate network" (Rouse, 2014a, para. 1).
Secure remote working	"Provide remote workers with a secure access to the corporate network" (Richmond, 2012, para. 4).

4.6 Conceptual overview

The high-level story of what employees do at their work supports the technical security measures that are chosen. For everything an employee undertakes at work a technical security measure is in place to make sure the employee does this in a secure way. This shows that this research contains a broad scope of technical security measures and that for every important task an employee performs, at least one technical security measure is part of this research.

In their daily practice, employees have three main activities they undertake, in which they possibly encounter technical security measures. First they have to get onto their computers. They can do this by authenticating themselves on the computers. Authentication measures are in place to support this process. Secondly, they are going to collect information needed for the tasks they have to perform. Employees use the internet for collecting new information. Web-browser restrictions are in place to make sure that this activity is being done in a secure way. Sometimes, in addition to using the internet, employees collect information by looking at files other employees created. Access control mechanisms control to what information an employee has access. Thirdly employees share their new knowledge with others by e-mails or by file sharing applications. DLP tries to secure that no confidential data is leaked outside the company.

It is also possible that employees undertake these three activities remotely from home. A secure remote connection establishes a connection for those employees with the corporate network.

Figure 9 provides a visualisation of the relation between the selected technical security measure classes and the main activities of employees.

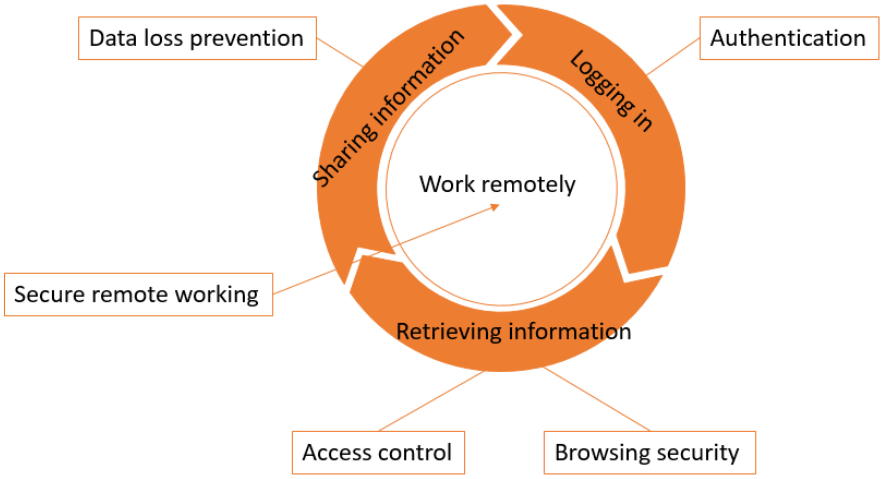


Figure 9 - Employees' main activities with related technical security measures

4.7 Specific technical security measures

The selected technical security measure classes that are used in this research (see table 5) cannot be implemented directly into the choice modelling survey. The selected technical security measures are still formulated as a general class and contain multiple possible practical implementations of these measures. Decided should be which practical implementations of these technical security measures in each selected class will be used for the choice modelling survey. In this study the most commonly used technical security measure implementations will be selected. This to guarantee that every type of employee will be able to make a well-founded trade-off between the importance of perceived usability and security of the technical security measures. This paragraph will discuss the possible implementations of each technical security measure class and select the ones that will be used in the survey.

Authentication

In the class authentication the most implemented method is authentication via a password. The strength of a password is dependent on two things: password length & password expiration frequency. A company can set requirements for the password length and the type of characters that a password must contain. A company mostly also sets requirements on how many times a year a password needs to be changed. This frequency of change is different per company. To give a broad scope of possibilities, it is decided to have options between changing your password once a year, once a quarter up to never. Other ways to authenticate yourself are by making use of biometrics or by the use of images. These are more advanced options and not very often implemented (yet) in companies. Most companies still rely on using passwords and therefore the scope of this research only contains passwords as an implementation of authentication.

Access control

The class access control contains two main resources to which one can have access to: software and files. This research will focus on access to files, because for software it is difficult to give a general access rule. Mostly it depends on the kind of software how the access to this software is organized. A more general implementation of access control is how the access to files is organized. Can everybody in the company see every file, is this department based or is by default every file private? These three options will be used in the choice modelling survey.

Browsing security

The technical security measure browsing security can be implemented in two ways. Restrictions can be put on the browser itself or on websites that are browsed to. The last one would probably consist of a blacklist of websites of which the company does not want their employees to visit them. Problem with this implementation is that this is heavily company dependent. Asking this in a survey would be not possible,

because it would require to specify which websites are on the blacklist. However, since this is company dependent this is not an option. The other implementation of browsing security is setting restrictions on which browser employees are allowed to use. Should employees work with one default browser of the company or are employees allowed to install every browser they prefer? This can be implemented in a choice modelling survey, because (almost) every employee is using a browser at their work to search for information on the web. The described options of having one default browser or allowing every browser will be both used in the choice modelling survey.

Data loss prevention

The class data loss prevention knows three possible ways of data sharing. Information sharing is mostly done via e-mail. A company could restrict information sharing via e-mail, when an e-mail is sent to a non-corporate e-mail address. This in order to prevent employees from sharing confidential information with people outside the company. This can be done by either warning an employee every time he/she sends an e-mail to somebody with a non-corporate e-mail address, or by warning when specific types of possible confidential words are used in the e-mail (e.g. confidential, private, sensitive). In most cases this last option is not only a warning, but also a pop-up in which the employee has to agree that he/she is sure that he/she wants to send this message, before it would be possible for him/her to send the mail. Sometimes files are of such a size that the mail system is not able to send the files. In that case other ways of sharing data are used. A company can restrict the sharing of big files by letting employees only use a shared drive (or a corporate SharePoint) for this purpose. This as an alternative for cloud based solutions such as Dropbox or Google Drive. Companies could also refrain from putting on the way information is shared. This means that employees are allowed to also make use of cloud applications. The third way of sharing data is by making use of removable media, such as usb-sticks. However, removable media are not that frequently used anymore. The two ways mentioned earlier, by e-mail and by a shared drive, are way more common. Therefore, only these two ways will be implemented in the choice modelling survey and removable media controls will not.

Secure remote working

In the class secure remote working the implementation that employees are mostly confronted with is establishing a connection with the corporate network in order to make use of specific types of applications. Such a connection is mostly established via a VPN connection. For such a VPN connection employees have to type in credentials in order to make it possible for the VPN to establish a connection. Different types of credentials can be used for establishing such a connection. This research will focus on establishing a connection via a token or a password. A token is a small device (e.g. a mobile phone). This token creates a digit number that the employees has to fill in on the computer. A third way to establish a connection is by using two-factor authentication; both a password and a token are required. All of these three options for establish a VPN connection (token, password, and two-factor authentication) will be used in the choice modelling survey.

4.8 Conclusion

This study focuses on technical security measures. A technical security measure is an electronic security method that protects information on a computer in a company. Following this definition, a selection of technical security measures was made that will be studied in this thesis. Table 6 shows an overview of technical security measure classes, technical security measures itself and their implementations. These will be used in the survey, described in the following chapter.

Table 6 - List of technical security measure with their implementations used in this research

Technical security measure class	Technical security measure	Option A	Option B	Option C
Authentication	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
Access control	Access to files	All files	Files of the department	Your own files
Browsing security	Browser 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 restrictions	Warning message with e-mail	Pop-up message with e-mail which contains confidential words
Secure remote working	Secure remote connection	Via password	Via token	Via password & token

5. Design of the experiment

5.1 Introduction

In this research project, data will be collected through a survey. This chapter will capture the design of this survey, including important survey design choices and a pilot study. The survey has two important functions: (1) measuring perceptions of employees and (2) measuring choices of employees. This chapter firstly describes the choice modelling part of the survey, since choice modelling surveys require a specific set-up. Subsequently discussed will be how perceptions will be measured and how this will be implemented inside the choice modelling survey. In addition to the functional requirements of a survey (fulfilling the goals of measuring perceptions and choices) it is also important to think about the design of the survey thoroughly, including the type of questions, terminology and length of the survey. Results and feedback from the pilot study are used to improve the efficiency and quality of the final survey design.

5.2 Design of the choice part of the survey

Number of alternatives in a choice set

To be able to estimate a choice model, choices of respondents on different alternatives are necessary. The number of alternatives shown for each choice question (also called the choice set), is dependent on the underlying assumptions of the choice model. Two different models are assumed in this research, as explained in section 3.4: the RUM model and the µRRM model. The RUM model requires at least two alternatives in a choice set (Molin, 2016). The µRRM model requires at least 3 alternatives in a choice set (Molin, 2016). In this survey each choice set will contain 3 alternatives, so that both models can be used.

Specifying attributes

Each alternative presented to the respondent consist of multiple attributes predefined by the researcher. Attributes are the elements for which trade-off in weighing is estimated by the choice model. This research is interested in the trade-off between the importance of perceived usability and security. So normally these two would be considered as the attributes of the design. Besides determining the trade-off between importance of perceived usability and security, another goal of this research is gaining knowledge on the perceived level of usability and security. This means that respondents should be able to specify the perceived usability and security levels, rather than have these levels predefined by the researcher. Therefore, security and usability should not be the attributes used in this choice modelling survey. Instead the attributes are the selected technical security measures described in chapter 4. Table 7 shows how the technical security measures are exactly used as attributes and as the corresponding attribute levels. In every alternative the same technical security measures are covered, but every alternative consist of different implementations of the technical security measures. 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.

Table 7 - Attributes & attribute levels

Attribute	Attribute level 1	Attribute level 2	Attribute 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
Access to files	All files	Files of the department	Your own files
Browser restrictions	Every browser is allowed	Obligatory browser	
File sharing within 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 words
Secure remote connection	Via password	Via token	Via password & token

Coding of the attributes

A choice model requires numerical input variables. The attributes from table 7 are however nominal variables. A nominal variable is a variable with multiple levels where no intrinsic ordering between these levels exist (de Vocht, 2009). Therefore, the nominal values should be coded by numbers. Effect coding is applied for this survey. In effect coding, each attribute is represented by a number of indicator variables. The number of indicator variables per attribute is the number of attribute levels minus one. In effect coding possible values of the indicator variables are -1, 0 or 1. For example, the attribute password expiry frequency is coded with two indicator variables PEFOY and PEFOQ in table 8. This is done in the same way for all the other attributes. In total 12 indicator variables are used to code 7 attributes. For a total overview of how all these attributes are effect coded appendix A can be consulted.

Table 8 - Effect coding of password expiry frequency

Attribute	Attribute level	PEFOQ	PEFOY
Password expiry frequency (PEF)	Once a Quarter (OQ)	1	0
	Once a Year (OY)	0	1
	Never	-1	-1

Design

The choice sets for this survey are created by specifying an efficient design, which seeks to minimise the standard errors (Rose & Bliemer, 2009). Other possible ways considered for this research were a full-factorial design and a fractional-factorial design. These two, however, resulted in too large a number of choice sets. A survey with too many choice questions is undesirable for respondents. Creating an efficient design can be done with a software called Ngene. In Ngene, the number of desired choice sets can be specified and Ngene will then generate a design for the number of choice sets. The rule for the minimum number of choice sets is that it should be possible, with the number of choice sets, to observe one choice probability more than the number of indicator variables. In each choice set two choice probabilities can be observed, since each choice set consist of three alternatives (for example when alternative A is chosen out of alternatives A, B, and C, the choice probability between A and B and between A and C can be observed). This causes that the minimum number of choice sets can be determined by the number of indicator variables plus one divided by two ((12+1)/2 = 6.5). This leads to a required number of choice sets of seven (rounded up). The desired number of choice sets used for this survey is instead set at eight, to make it possible for the attributes with two levels to appear across all alternatives an equal number of times. This is important for the reliability of these parameters (Rose & Bliemer, 2007). The design Ngene provided when making use of an efficient design can be found in Appendix B.

Result

The survey has 8 different questions for which the respondent has to choose between 3 alternatives which are containing different technical security implementations. The respondent is asked which alternative he/she would prefer at his/her work. Figure 10 shows an example of a choice question.

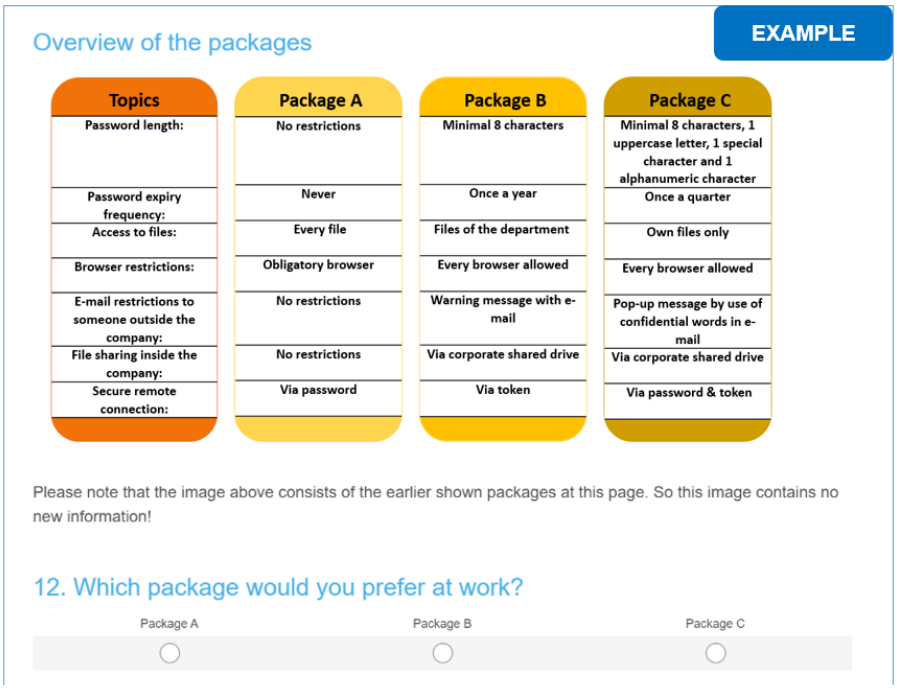


Figure 10 - Example of a choice question of the survey

5.3 Design of the perception part of the survey

Next, the perceptions of the respondents about usability and security should be implemented in the survey as well. The security and usability levels are reflected by the use of a 5-point scale. This means that the respondent can choose between the levels very user-unfriendly, user-unfriendly, neutral, user-friendly, very user-friendly for rating the usability level. For security the possible different levels are highly insecure, insecure, neutral, secure, and highly secure. In addition to making the perceived levels of security and usability explicit, this research also aims to gain insights to the trade-off in weighing between these two aspects. Therefore, the same alternatives for the choice part of the survey are used for asking about the perceived usability and security levels. This makes it possible to estimate a choice model based on the perceived levels of security and usability.

Figure 11 shows an example of how perceptions are captured in a choice question.

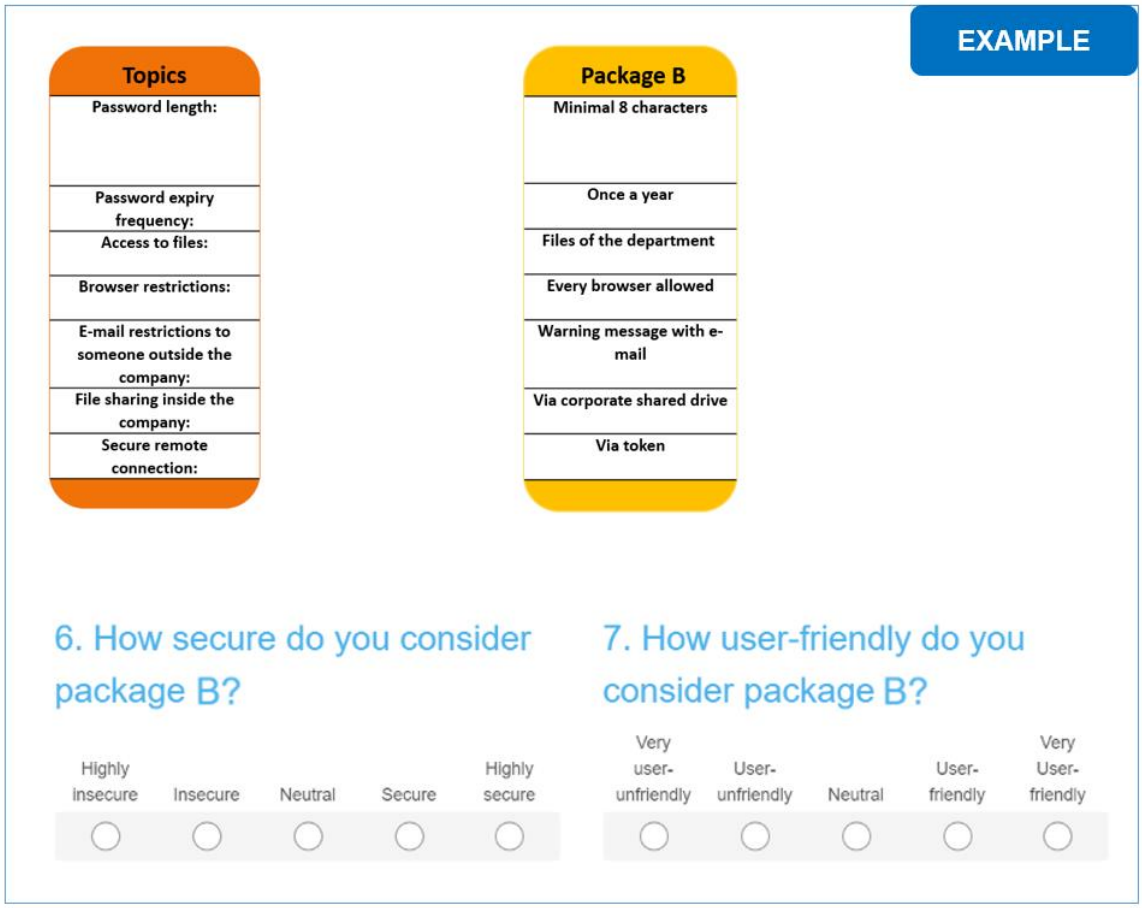


Figure 11 - Example of a perception related question in the survey

5.4 Other questions

5.4.1 Socio demographic questions

It is important to know some social demographic factors of the respondents. Firstly, this tells something about the type of people/the characteristics of people that participated in the survey. Secondly, it is also interesting to test if there exists any correlation between demographic variables and survey responses. Standard socio demographic variables as gender, age, education and nationality are asked in the survey. In addition, other variables related to information security are asked in the survey: self-declared level of computer knowledge, awareness of online risks, and personal experience with cybercrime. Firstly, when employees know more about the computer, they could find it easier to understand and use the different technical security measures. Secondly, people who are more aware of their online risks are expected to weight the importance of security higher in their overall choice. The last social factor that will be included in the survey is if the respondent was, or knew someone who was, a victim of cybercrime. People who

were, or knew someone who was, a victim of cybercrime are expected to find the security level of an alternative a more important aspect in their overall choice than people do not have the same experience.

In short, the following socio demographic factors will be included in the survey:

- Gender
- Age
- Highest level of completed education
- Nationality
- Self-declared level of computer knowledge
- Perceived awareness of online risks
- Personal experience with cybercrime

5.4.2 Work related questions

In addition to know the socio demographic factors of the respondent it is also useful to know something about the type of employees, because this could make it possible to give specific recommendations to companies based on the type of employees in their company. In chapter 2.2 a literature review in combination with a practical consideration is performed to identify these factors. The identified factors are:

- Size of a company
- Company sector
- Employee working in the information/cyber security domain or not
- Number of years working for the company
- Job type of the employee
- Percentage of computer use at work
- Perception of sensitivity level of information at work
- Followed security awareness training or not.

All these factors are collected by asking respondents about those. Figure 12 shows an example of such a question.

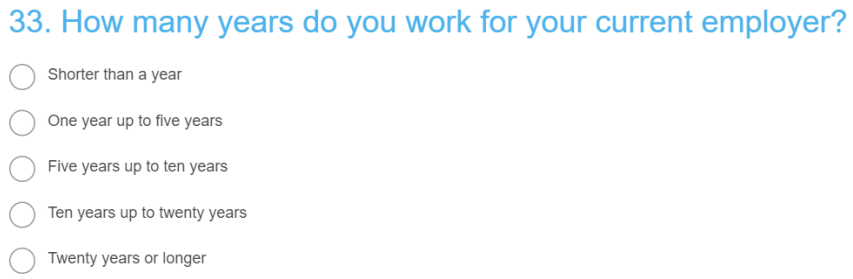


Figure 12 - Example of a work related question in the survey

5.4.3 Introductory questions

Since most of the concepts discussed in this survey are highly technical, extra information should be provided to the respondents in order for them to be able to understand the technical concepts. Especially the different technical security implementations require additional explanation. Explaining concepts can be done with the help of an introductory text. However, long texts could be seen as boring by participants and consequently they could skip reading this information. This could lead to the result that they did not capture all the explained information from the text. A better option is to implement introductory questions in the beginning of the survey in which the technical concepts are described. In this way respondents have to read the explanations, since they are expected to answer a question about this. This survey will contain 7 introductory questions each explaining one technical security measure with their belonging implementations. Each introductory question will ask the respondent how a specific technical security measure is implemented at their work. Although the main purpose of these introductory

questions is explaining the topic, this could also give insight in the current implemented technical security measures in multiple companies. However, since this is not the main focus of this research results of this are not extensively discussed here, but details can be found in appendix E.

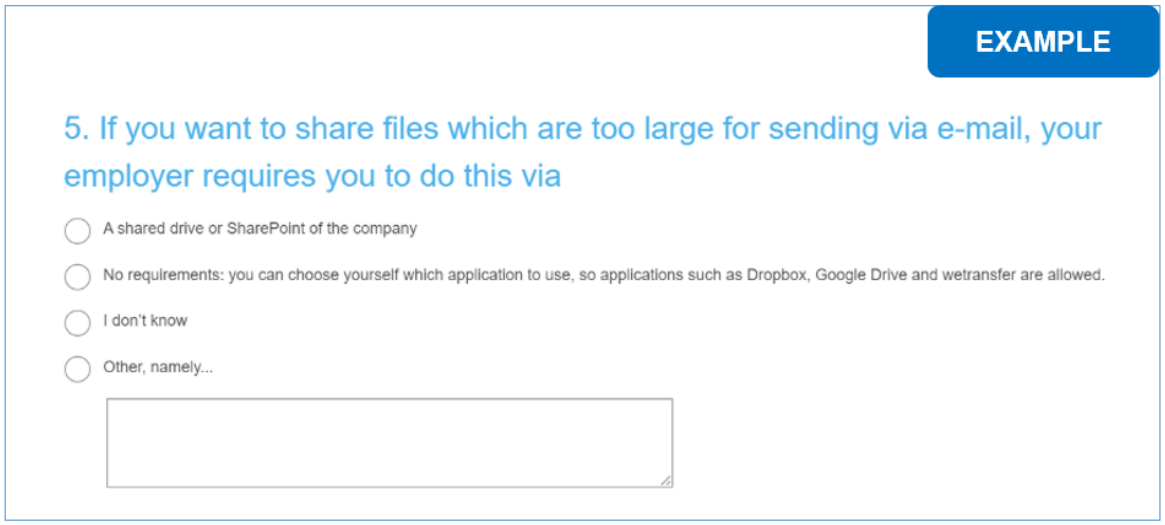


Figure 13 - An example of an introductory question

5.5 Survey Design Conclusion

The survey consists of three sections (see figure 14). First the respondent is asked about the current implementations of technical security measures at their work. This in order to be able to explain the technical concepts to the respondents. Secondly, the respondent is confronted with 8 questions containing each 3 different alternatives. For each of alternative respondents are asked to make their perception of the usability and security level of these alternatives explicit on a 5-point scale. Thereafter respondents are asked 8 times to choose between 3 alternatives the alternative that he/she would prefer the most at his/her work. In addition, the last part of the survey consists of socio-demographic and work related questions.

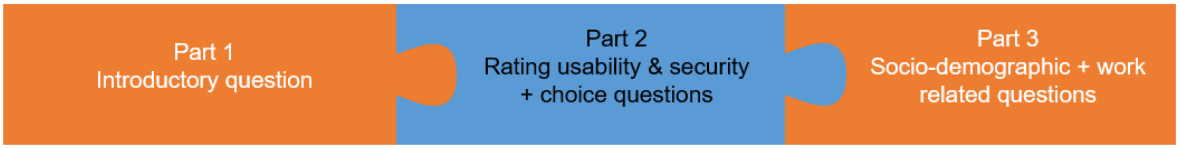


Figure 14 - Different parts of the survey

5.6 Pilot study

A pilot study is conducted to test and improve the final survey, such as making the design more efficient and the questions more easily understandable to the respondents. A more efficient design can be reached when making use of estimating priors. In addition to estimating priors the pilot study is also useful to get an idea from the respondents about if they think the survey is understandable and how it can be improved.

5.6.1 Pilot study respondents

For a pilot study only a small number of participants is required. A rule of thumb is to involve at least 30 persons. This pilot study was conducted among the author's network. In total, 34 employees were surveyed. From these 34 respondents, only 31 completed the whole survey. Only these 31 responses will be used for the result analysis of this pilot study.

5.6.2 Creating more user-friendly survey design

Length of the survey

Every respondent was asked at the end of the pilot study to give feedback about the pilot study. Besides small suggestions for improvements, the most frequent heard comments were that the survey was too long (77 questions in total) and that the packages with technical security measures were too complex. This could also be a reason why 3 out of the 34 respondents stopped halfway through the survey. This is undesirable for the final survey. In the pilot survey the author could rely on her network, however, the final study will be conducted within a larger population, who may be less willing to complete a long survey. Therefore, it is important to simplify or shorten the survey.

The part that most respondents found too long was the middle part of the survey, where respondent has to specify the security and usability of presented alternatives (48 questions) and thereafter choose between these alternatives (8 questions). Since, for this part already the minimum number of choice questions is used, this cannot be shortened. However, there are two options to make the survey simpler: reducing the number of attributes and making use of blocking.

The first option is to reduce the number of attributes. Some participants said that they found it difficult to understand the difference between sharing files and access to files. Access to files could indeed be confusing. For example, the implementation of access to files where an employee has access to files of his/her department. This access is probably created by putting this folder on a corporate shared drive which enables employees of the department to access all these documents. In file sharing one of the implementations is sharing via a corporate shared drive. So these two options are having overlap. It is decided to remove file access from the attribute list, since the different implementations are quite generalised. Take, for example, the option access to all the files of the company. Probably an employee does not have access to every file in a company, but to a lot of files. To which files the employee specifically has access depends on the company. Since the different options for the attribute file access could be confusing, this attribute will be out of scope of the final survey.

Another attribute level by which participants were confused was by using a token to create a secure remote connection. Some participants said a token is a difficult concept to understand for non-technical employees. Although one could argue that this can be solved by providing the respondents with a better explanation of a token, it is decided to remove the whole attribute 'secure remote connection' from the attribute list. Reason for this is that this attribute is mainly focused on authentication. Logging in by password and/or by a token is a way to authentication yourself as an employee. However, since already two of the attributes of the attribute list are focused on authentication ('password length' and 'password expiry frequency'), it is decided to remove 'secure remote connection' from the attribute list. Otherwise too much attention is put to authentication as technical security measure.

By reducing the number of attributes with two, the number of parameters to be estimated can be reduced with four (2 attributes effect coded by 2 indicator variables each). For the final survey this means a total number of 8 parameters will be estimated. Five choice sets are required to estimate all these parameters ((8+1)/2=4.5). This means that the survey is reduced with 3 choice questions: from 8 choice questions in the pilot survey to 5 choice questions in the final survey. This reduction in the number of choice questions leads to a large improvement in the number of perception related questions of the survey: from 48 in the pilot survey to 30 in the final survey.

The second option to reduce the length of the survey is by making use of blocking. This means that the choice sets are grouped in multiple blocks. Every respondent is only presented 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 will be used (since a number of 5/2=2.5 choice sets is not possible, the number is rounded up to 3 per block). This results in a survey where every respondent has to answer 3 choice questions and related to these 18 perception related questions.

Sequence of the questions

Another frequently raised comment was that respondents reveal that the more choice sets they had seen, the stricter they were when rating usability and security level of the alternatives. A useful technique would be to randomise the sequence of the choice questions to avoid skewed results where the last choice

question consistently considered more severely than earlier questions. However, the survey tool used for this research did not allow randomise sequence of questions. However, this is not a huge problem, since the number of choice questions is reduced to 3 per respondent in the final survey. The need for randomisation of the sequence of questions decreased compared to the pilot survey with 8 choice questions per respondent.

5.6.3 Efficient design

The utility contributions of the indicator variables from the pilot survey results are used to specify the choice sets of the final survey via best guesses on parameter values (priors). Since two attributes will be left out of the final survey they are also left out of calculations when estimating the utility contributions. Table 9 shows the utility contributions that are the result of the pilot survey. This table shows that the attribute level with the highest utility contribution (-0.78) is when there are no restrictions on password length. This has the most negative impact on the utility of the alternative. Smallest utility contributions are in the area of e-mail restrictions (0.08 and 0.09). Reasons and explanation about the size and direction of the utility contribution will be elaborated on in chapter 5 when the utility contributions for the final survey are estimated. Most important about these estimated utility contributions in the pilot is that they are used as priors to specify a more efficient final survey design. Appendix C provides the syntax of how the priors are used in Ngene to specify the design for the final survey.

Table 9 - Utility contributions of the attribute levels of the pilot study when assuming an RUM model

Attribute levels	Utility contribution
Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	0.54
Minimal 8 characters	0.24
Password length no restrictions	-0.78
Once a quarter	0.05
Once a year	0.25
Never	-0.30
Obligatory browser	0.23
Every browser is allowed	-0.23
Pop-up message with e-mail which contains confidential words	-0.17
Warning message with e-mail	0.09
No e-mail restrictions	0.08
Via corporate shared drive	-0.11
No restrictions	0.11

5.7 Conclusion

Table 10 shows the structure of the final survey. The final survey consists of 3 parts. The first part consists of 5 questions about the current situation of implemented technical security measures at work. These questions will explain the different technical security measures used further in the survey in a question based way. The second part consist of 18 rating questions about the perceived usability and security level and 3 choice questions. The pilot survey showed that confronting people with 48 rating and 8 choice questions was too much for the respondents, therefore the final survey is split in half (only part II is split) and is shortened by reducing the number of attributes (remaining attributes are password length, password expiry frequency, browsing restrictions, e-mail restrictions and file sharing). In the final survey each respondent is confronted with 9 questions about how they perceive the security level of the shown alternatives and 9 questions about how they perceive the usability level of these alternatives. After rating three alternatives, each time the respondent has to choose the alternative he/she would prefer at work. So in total the respondent will see 3 pages in this part of the survey with on each page 3 alternatives, 6 rating questions about their perceptions of these packages, 1 choice question between these packages. The third part of the survey will ask personal characteristics of the respondents. This in order identify if certain personal characteristics are of influence on how people perceive usability and security or how people make a trade-off.

Table 10 - Structure of the survey

Part	#Questions	Aim	Type
I: Questions about the current situation at work	5	Explaining technical security measures	Multiple choice questionnaire
II: Packages	21	- Measure perceptions of usability and security - Determine trade-off	Choice experiment Rating experiment
III: Personal characteristics	16	Influence personal characteristics on perceptions and trade-off	Questionnaire

Due to blocking, the survey has two versions: version A and version B. The difference between these versions are part II the packages the respondents are presented with. Respondents are randomly assigned to one of the versions of the survey. The survey is available in two languages: English and Dutch. The total final survey in English can be found in appendix D.

The final survey is designed in the survey tool Survey Monkey (SurveyMonkey, 2016). In order to randomly assign respondents to one of the survey versions a website domain was bought. This website randomly redirected the respondents to one of the versions of the survey. The survey was distributed in two large Dutch companies (say anything about the identity of these companies is not allowed). In addition, the survey is distributed across multiple social media channels. With these social media channels not only the network of the researcher herself is addressed, also others distributed the survey within their network. Snowball sampling is used to reach a larger number of people, whereby people were asked for three other people to fill in the survey as well.

6. Outcomes of the survey

6.1 Introduction

This chapter analyses the data retrieved from the survey. The aim of this chapter is to measure perceived usability and security of employees and to measure the trade-off between the importance of perceived usability and security by employees.

This chapter starts by describing the respondents to the survey. This can be found in section 6.2. Section 6.3 focuses on the levels of security and usability perceived by the respondents of the survey. The following section, section 6.4, is focused on how the respondents of the survey are making choices. Section 6.5 describes a model where a combination is made between perceptions and choice. Finally the chapter ends with a short conclusion section containing the key insights found in this chapter.

6.2 Respondents

In total 289 responses were gathered. However, 59 of the responses were incomplete, only part of the questions was answered. This number of not fully complete surveys is so high, due to a problem Survey Monkey had with their servers in the first couple of days when the survey was online. A couple of respondents reported to the researcher that they were confronted with a gateway error halfway through the survey. The researcher reported this problem to SurveyMonkey and after a couple of days SurveyMonkey accomplished to solve this problem. However, the big impact this gateway error had on the collection of respondents for this research was irreversible.

In total 230 employees completely filled in the survey. Table 11 shows that the number of surveys for version A & B are not equally divided. The reason for this is that the surveys are distributed randomly.

Table 11 - Number of completed surveys per version

	Version A		Version B	
	Complete	**Incomplete**	**Complete**	**Incomplete**
Dutch	99	32	98	15
English	12	7	21	5
Total	111	39	119	20

Representativeness

The target audience of the survey was 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 (for example no specific company branch was required). 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. Appendix F shows an overview of the different characteristics of employees that participated in the research. Important to mention is that it is difficult to reflect upon the representativeness of the sample group. Although there is information available about the characteristics of the active population in general, no information is available about which specific group of this entire active population makes use of a computer. What this research can do is test whether specific personal characteristics of respondents are of impact on the answers respondents gave. However, since the lack of information about the real population there cannot be reflected upon the outcomes of this research in a way that a specific effect is probably over or under-estimated due to the over or under representation of a specific group. For example, most of the respondents were men. What can be calculated is if men think differently about security and usability than women. There cannot be reflected upon if that means that the outcomes of this research are over- or underestimated, since perhaps in the population most of the employees who working with a computer are men as well.

6.3 Perceptions

In the survey rating question were asked to gather information about usability and security perceptions of employees. Possible rates for usability were (see section 5.3): very user-unfriendly (1), user-unfriendly (2), neutral (3), user-friendly (4), very user-friendly (5). Possible rates for security were (see section 5.3): highly insecure (1), insecure (2), neutral (3), secure (4), and highly secure (5). With these ratings the influence

of technical security measures on the perceived usability and security levels can be estimated. These calculations are done with linear regression. Since the independent variables in linear regression (the technical security measures in this case) are not of a continuous level (but of categorical scale), effect coding is applied. In section 5.2 is already discussed how effect coding is applied. The full coding scheme used for applying effect coding can be found in appendix A.

6.3.1 Linear regression usability

Table 12 shows the effect of the technical security measure implementations on the perceived usability. The regression constant is the average perceived level of usability. An average perceived usability of 3.49 is measured. This means that on average employees consider the packages with technical security measures between neutral user-friendly (3) and user-friendly (4). The effects of the technical security measures are representing the increase/decrease on the average usability when having this technical security measure implementation in place. For example, a package which include a password expiry of once a quarter is on average perceived with a usability level of 3.25 (3.49 -0.24). Table 12 reveals that the (most) negative signs of a technical security measure always belong to the strictest implementation. For example, a password expiry frequency of once a quarter has a negative sign. This is the strictest implementation possible compared to a password expiry frequency of once a year and never.

The t-values in table 12 are used to determine the significance of the found effect. The null-hypothesis tested is if in the population a technical security measure implementation has no effect on the perceived usability level. If an absolute value of the t-value of 1.96 or higher is calculated (Dougherty, 2001), the null-hypothesis can be rejected. That means that with a 5% (or lower) significance level it can be assumed that the technical security measure has an effect on the perceived usability in the population.

With the estimated effects of table 12 16% of the variance of perceived usability can be explained (this can be concluded from a calculated adjusted R-square of 0.16).

Table 12 - Effects of the technical security measure implementations on perceived usability

Technical security measure	Implementation	Effect	t-value
	Regression constant	3.49	185.52
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	-0.05	-1.75
	Minimal 8 characters	0.06	1.91
	Password length no restrictions	-0.01	*
Password expiry frequency	Once a quarter	-0.24	-8.89
	Once a year	0.12	4.43
	Never	0.12	*
Browsing restrictions	Obligatory browser	-0.27	-13.28
	Every browser is allowed	0.27	*
E-mail restrictions	Pop-up message with e-mail which contains confidential words	-0.14	-4.88
	Warning message with e-mail	-0.06	-2.39
	No e-mail restrictions	0.20	*
File sharing	Via corporate shared drive	-0.08	-3.76
	No restrictions	0.08	*

* 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.

To calculate the impact of a technical security measure on the perceived usability level, the effects of the different implementations per technical security measure should be compared. Table 13 lists the technical security measures sorted by impact on usability. The table shows that inside a package with technical security measures, the different types of browsing restrictions have the largest impact difference on the perceived usability level. This means that of all the technical security measures in table 13, the decision

for which implementation of browsing restrictions to use will result in the highest change in the perceived usability level. A package of technical security measures which contains an obligatory browser has a way lower perceived usability 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 a warning message and even less usable no e-mail restrictions. The different implementations of file sharing and password length only have a small difference in perceived usability. This means that for employees it does not really matter in terms of perceived usability whether a password length with no restrictions, 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.

Table 13 - Impact of technical security measures on perceived usability

	Technical security measure	Impact
1	Browsing restrictions	0.54
2	Password expiry frequency	0.36
3	E-mail restrictions	0.34
4	File sharing	0.16
5	Password length	0.11

Personal characteristics

To identify if different types of employees perceive a different level of usability the linear regression model is expanded by incorporating personal characteristics. The direct impact of the personal characteristic on the perceived usability is estimated as well as the interaction between the personal characteristic and the technical security measures. For example, there is estimated whether men and women perceive a different level of usability and there is estimated whether the impact of browsing restrictions on the perceived usability level differs between men and women. Formula 3 and 4 show the difference between both measurements. Formula 3 shows the direct effect and formula 4 shows the interaction effect.

$$Personalcharacteristic\ contribution\ to\ usability\ = Average\ perceived\ usability\ +\ Gendereffect\ *\ Gender \quad (3)$$

$$Personalcharacteristic\ contribution\ to\ usability = Average\ perceived\ usability + (B_{Browsingrestriction} + Interactioneffect * Gender) * Browsingrestiction \quad (4)$$

Where

$Gender = 1\ for\ female\ and\ -1\ for\ male$

$Browsing\ restriction = 1\ for\ an\ obligatory\ browser\ and\ -1\ for\ every\ browser\ is\ allowed$

Most of the personal characteristics were not found to be of significant influence (with a 95% confidence level), with the exception of a few. Table 14 shows these personal characteristics for which the influence on perceived usability was found to be significant. Important to mention is that some of the personal characteristics are effect coded and some are measured on an interval scale. For the effect coded characteristics table 14 only shows the effect of one specific category. To see the impact of the other categories for the same characteristics appendix G1 can be consulted. The personal characteristics that are not effect coded, but measured on an interval scale, are indicated with a *. This means that the size of the effect has to be multiplied with the specific level of the personal characteristic. For example, to see the impact of age on perceived usability the effect of age should be multiplied by the age of the employee.

Almost all of the significant effects of personal characteristics on the perceived usability level are very small effects. The personal characteristics which show to have a small effect are: (1) Employees who work 5 years or longer perceive a higher level of usability than employees who work shorter. (2) Employees

who work in the information/cyber security domain perceive a higher usability level than employees not working in this domain. (3) Employees who use 76-100% of their time at work a computer perceive a lower usability level of an obligatory browser than employees who use their computer less frequent or then when there are no browsing restrictions in place. (4) Employees who have ever been a cyber victim perceive a slightly lower usability level of an obligatory browser than people not being a cyber victim or when there are no browsing restrictions in place.

There are three personal characteristics that can have a larger effect on the perceived security, dependent on the level of that personal characteristic (since they are measured on an interval scale). For the perceived level of computer knowledge holds that the more knowledge about a computer an employee has, the less usable he/she perceived the technical security measures. An example is that an employee who perceive his/her level of computer knowledge as good, perceive a usability of -0.06*3 = -0.18 lower than average (3= the number used to specify a computer knowledge level of good). Second personal characteristic that is of larger influence is the age of an employee. The older an employee is, the more usable the employee perceive the technical security measures. An employee who is, for example 30 years old perceive a usability level of 0.01*30 = 0.30 higher than average. Last personal characteristic that can have a large influence is the interaction found between perceived sensitivity of work information with password expiry once a quarter. The more sensitive employees perceive the information they work with the more usable they found a password expiry frequency of once a quarter.

Besides reporting the influence of these characteristics on the perceived usability, it is difficult to give reasons why these characteristics specifically are of influence. Since this will be a subjective interpretation instead of a factual explanation, more research is recommended to research the reasons behind these relations between personal characteristics and perceived usability level.

Important to mention is that most of the found effects of the personal characteristics are relatively small. They only cause a small change in perceived usability. This is also reflected by the calculated R-square of 0.19. This means that incorporating these personal characteristics in the linear regression model would make an improvement of an extra 3% of the variance of usability that can be explained with both the technical security measures and the personal characteristics.

Table 14 - Influence of personal characteristics on perceived usability

Personal characteristic	Effect	t-value
Direct effect on perceived usability		
Years working for current employer: 5 years or longer	-0.10	-3.46
Perceived level of computer knowledge*	-0.06	-2.36
Working in information or cyber security: yes	-0.04	-1.98
Age*	0.01	2.06
Interaction effect		
Computer use at work:76-100% with obligatory browser	-0.11	-4.87
Perceived sensitivity of work information* with password expiry once a quarter	0.10	3.97
Cyber victim: yes with obligatory browser	0.05	2.69

* Personal characteristic measured on interval scale

6.3.2 Linear regression security

Table 15 shows the effect of the technical security measures on perceived security. The regression constant is the average perceived level of security. An average perceived security level of 2.90 is measured. This means that on average employees consider the packages with technical security measure as neutral secure (3). The effects of the technical security measures are representing the increase/decrease on the average security when having this technical security measure implementation in place. For example, a package which include a password expiry of once a quarter is on average perceived with a security level of 3.32 (2.90 + 0.42). An important aspect that table 15 reveals is that all the no restriction options are perceived as less secure than the technical security measures with restrictions. This can be seen by the negative sign of the effect of the no restrictions options.

With the estimated effects 41% of the variance of security can be explained by the technical security measures (concluded from a calculated R-square of 0.41).

Table 15 - Effects of the technical security measure implementations on perceived security

Technical security measure	Implementation	Effect	t-value
	Regression constant	2.90	156.51
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	0.58	20.06
	Minimal 8 characters	0.02	0.73
	Password length no restrictions	-0.60	*
Password expiry frequency	Once a quarter	0.42	15.92
	Once a year	0.02	0.83
	Never	-0.44	*
Browsing restrictions	Obligatory browser	0.04	1.83
	Every browser is allowed	-0.04	*
E-mail restrictions	Pop-up message with e-mail which contains confidential words	0.21	7.42
	Warning message with e-mail	0.14	5.15
	No e-mail restrictions	-0.35	*
File sharing	Via corporate shared drive	0.27	13.40
	No restrictions	-0.27	*

* 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.

To calculate the impact of a technical security measure on the perceived security level, the effects of the different implementations per technical security measure are compared. Table 16 lists the technical security measures sorted by impact on security. The table shows that of all the technical security measures in table 15, the decision for which implementation of password length to use will result in the highest change in the perceived security level. 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 of no restrictions. 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. A password expiry frequency of once a quarter is perceived as way more secure than an expiry frequency of never. 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.

Table 16 - Impact of technical security measures on perceived security

	Technical security measure	Impact
1	Password length	1.18
2	Password expiry frequency	0.86
3	E-mail restrictions	0.56
4	File sharing	0.54
5	Browsing restrictions	0.08

Personal characteristics

To identify if different types of employees perceive a different level of security, the linear regression model is expanded by incorporating personal characteristics. The direct impact of the personal characteristic on the perceived security is estimated, as well as the interaction between the personal characteristic and the technical security measures. Most of the personal characteristics were found to be of insignificant influence (with a 95% confidence level), with the exception of a few. Table 17 shows these personal characteristics for which the influence on security was found to be significant. Most of these personal characteristics have a very small effect on the perceived security level of the technical security measures. The small effects are: (1) Employees how have followed multiple security awareness trainings perceive a security level lower than employees who did not. (2) The more sensitive employees consider the information they work with the lower the perceived security level. (3) Employees who have been a cyber victim perceive a lower security level than employees who have not been a cyber victim (4) Employees who work in a company with 250 employees or more perceive a lower security level than employees in a smaller company. (5) Employees who work in a company with 250 employees or more perceive a higher security level for a password expiry of once a quarter.

The personal characteristic with the largest effect is perceived online risk awareness. For example, when employees consider themselves as very risk aware the perceived security level is decreased with 0.44 (-0.11*4 = -0.44).

Table 17 - Influence of personal characteristics on perceived security

Personal characteristic	Effect	t-value
Direct effect		
Perceived online risk awareness*	-0.11	-4.47
Followed security awareness training: multiple times	-0.10	-4.36
Perceived sensitivity of work information*	-0.01	-4.25
Cyber victim: yes	-0.04	-2.04
Company size: 250 employees or more	-0.05	-2.48
Interaction effect		
Company size: 250 employees or more *password expiry once a quarter	0.06	2.42

* Personal characteristics measured on an interval scale

Incorporating these personal characteristics in the linear regression model would make an improvement of an extra 4% of the variance of security that can be explained with both the technical security measures and the personal characteristics (concluded from a calculated R-square of 0.45). So an addition of personal characteristics to the technical security measures results in a better prediction of the perceived security level. For a total overview of the estimated regression model with incorporation of the significant personal characteristics appendix G2 can be consulted.

6.3.3 Correlation between usability and security

In table 18 the effects of the technical security measure implementations on perceived usability and security levels are shown next to each other. This makes it possible to compare the difference between the effects. What can be seen by this table is the difference in size of effect on either perceived usability or perceived security. For most of the technical security measures implementations the effect on the perceived level of security is larger (mostly twice as large or even larger) 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. The only technical security measure for which this effect does not hold is for browsing restrictions. For browsing restrictions holds that the difference between the two possible implementations: no restrictions or an obligatory browser, have a large difference in terms of perceived usability and a small difference in terms of perceived security.

What can also be observed is that for most of the technical security measures the signs for security and usability are opposing. When the perceived usability decreases for an alternative that consist of that

technical security measure implementation, the perceived security increases and the other way around. For example, an obligatory browser has a negative effect on perceived usability, while at the same time a positive effect on perceived security.

Table 18 - Effect of technical security measures on perceived usability and security

Technical security measure	Implementation	Effect on perceived usability	Effect on perceived security
	Regression constant	3.49	2.90
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	-0.05	0.58
	Minimal 8 characters	0.06	0.02
	Password length no restrictions	-0.01	-0.60
Password expiry frequency	Once a quarter	-0.24	0.42
	Once a year	0.12	0.02
	Never	0.12	-0.44
Browsing restrictions	Obligatory browser	-0.27	0.04
	Every browser is allowed	0.27	-0.04
E-mail restrictions	Pop-up message with e-mail which contains confidential words	-0.14	0.21
	Warning message with e-mail	-0.06	0.14
	No e-mail restrictions	0.20	-0.35
File sharing	Via corporate shared drive	-0.08	0.27
	No restrictions	0.08	-0.27

The estimated opposite signs of perceived security and perceived usability in table 18 are in line with what literature (see section 2.1) suggested: usability and security are negatively correlated. Calculating the correlation between the perceived security and usability in the sample data of this research, resulted in a negative correlation of -0.14. This negative correlation is a logical consequence of what most of the different technical measures in table 18 suggests: when the perceived usability level is higher compared to the average perceived usability, the perceived security level is lower than the average perceived security level 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).

6.4 Choice models

In the survey employees were asked, in addition to rate perceived level of security and usability, to choose between multiple packages of technical security measures. It is assumed that employees make choices based on the perceived security and usability levels. However, it also could be the case that employees choose based on the given technical security measures itself without considering security and usability. To see which assumption is true, both assumptions are tested. These two assumptions are tested within two different choice models: RUM and µRRM.

6.4.1 Choice model based on usability and security

The model fits of the first option of choosing a specific alternative with multiple technical security measures (based on the perceived usability and security level of this alternative) can be found in table 19. 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 large (5 or larger). The estimated µ of 323 is indeed very large. This means that employees, who are taking perceived security and usability into account when choosing an alternative, do this based on the principle of utility maximisation. The alternative with the highest utility has the highest chance to get chosen by the employees.

Table 19 - Model fit of usability and security choice model

	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

Since table 19 reveals that the choice behaviour of employees is based on utility maximisation, the betas of the usability and security perceptions in the RUM model are estimated. Table 20 show these betas. What can be seen in table 20 is that both security and usability perceptions have a positive beta. This means the higher the perceived security and usability, the higher the utility of the alternative. Surprisingly, the beta of perceived security is higher than the beta of perceived usability. This means that the perceived security is considered as a more important component than perceived usability for employees when they are making a choice for a package with multiple technical security measures. To test if the difference between both betas can be seen as statistically significant difference a t-test can be applied. A t-ratio of 3.69 is computed where a |t-ratio| of minimal 1.96 is needed for a 5% significance level. This means that difference between the betas of perceived usability and security is statistically different from 0 at a 5% level of significance.

Table 20 - Betas of security and usability in the RUM model

Perceptions	Beta	Std. error	t-value
Security	1.33	0.08	14.74
Usability	1.06	0.09	11.58

Quadratic component

It could be that the surprising betas of table 20 (perceived security is considered more important than perceived usability) is caused by the fact that the assumed linear relation between perceived security/usability and utility (see the RUM formula in section 3.4) is not the perfectly correct relation. Perhaps the utility is also dependent on a quadratic security/usability component. This means that the importance of perceived security/usability would be dependent on the perceived level of usability and security, instead of assuming the same importance of security/usability for each perceived level of usability and security. To see if this claim holds, a new model is estimated with the addition of two quadratic components in the RUM model. Table 21 shows the betas of the components in the new model. The table shows that the betas of both quadratic components are statistically significant (|t-value|>1.96). Both quadratic components have a negative beta, 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. With the addition of these quadratic components the utility contribution of the linear components of perceived security and usability have changed compared to table 20. The influence of the linear components per unit increase became higher.

The betas of the linear security and usability components show a slightly difference (2.51 compared to 2.68), however the 95% confidence intervals almost fully overlap each other. This is in line with the calculated t-ratio of 0.27 for the difference between the betas of linear perceived security and usability, where a |t-ratio| of minimal 1.96 is needed for a 5% significance level. This means that the difference between the betas of perceived usability and security cannot be seen as different from zero and therefore the contribution of perceived security and usability to utility can be considered as equal. The same holds for the 95% confidence intervals of the quadratic components of perceived usability and security (belonging t-ratio of 0.55 for the difference). Figure 15 is a visual representation of table 21. The error bars show that the difference in contribution of perceived security and usability to utility overlap with each other, which means that the contribution perceived usability and security give to utility is equal. In

conclusion, perceived security and usability are equally important, although the impact of one unit increase in perceived security/usability on the utility becomes less when the perceived usability/security level increases.

Table 21 - Quadratic components in 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

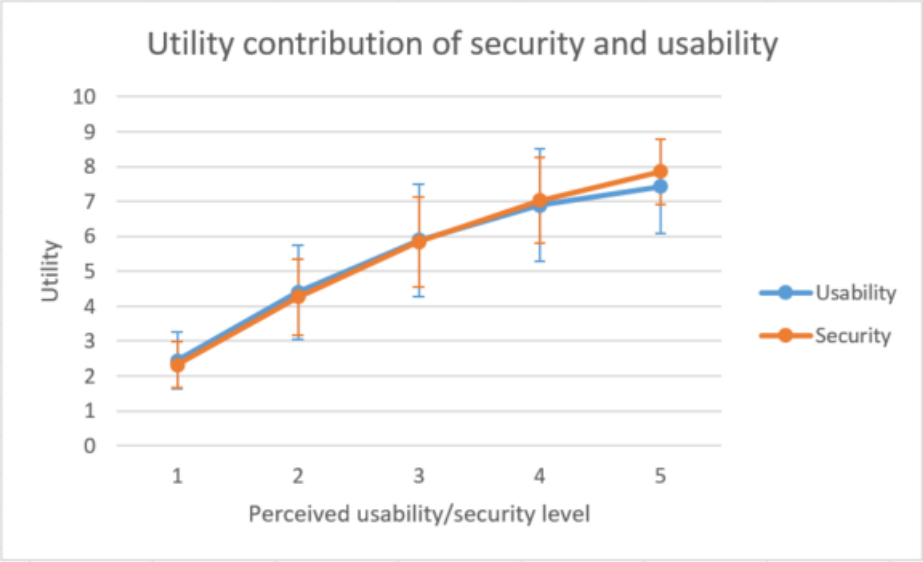


Figure 15 - Visualization of the security and usability components in the utility function

The implementation of the quadratic components in the RUM model shows to have a better model fit than a RUM model with only the linear components. Table 22 shows for a linear RUM a final log likelihood of -472.82, whereas a RUM model with the addition of quadratic components have a final log likelihood of -460.77. To identify whether this difference in model fit is statistically significant and not a matter of coincidence, a Likelihood ratio test is performed. The result of this test is a likelihood ratio statistic (LRS) of 24.10, where a LRS value of minimal 5.99 is required for a 5% significance level (PennState Science, n.d.). This means that the RUM model with incorporation of quadratic components for usability and security is a better model than the linear RUM model.

Table 22 - Model fit of linear RUM compared with linear & quadratic RUM

	Linear RUM	Linear + quadratic RUM
0 log likelihood	-758.04	-758.04
Final log likelihood	-472.82	-460.77
Rho square	0.38	0.39
Number of cases	690	690

6.4.2 Choice model based on technical security measures

The second option of choosing a specific alternative with multiple technical security measures is that employees do this based on the technical security measures inside the alternatives directly instead of on the perceived usability and security of these alternatives. Table 23 shows the different model fits when the two earlier discussed models (RUM and µRRM) would be applied on this assumption. The table shows that there is no difference in model fit. The RUM model (-565.66) has the same model fit as the µRRM

model (-565.66). Again here the µRRM behaved as a RUM model due to the large estimated µ of 172. This means that the package with technical security measures that give employees the highest utility has the highest chance to be chosen.

Table 23 - Model fit of system attributes choice model

	RUM	µRRM
0 log likelihood	-758.04	-758.04
Final log likelihood	-565.66	-565.66
Rho square	0.25	0.25
Number of observations	690	690
µ		172

To investigate the utility contribution of different technical security measures, the estimated RUM model can be found in table 24. A utility contribution of a technical security measure implementation can only be interpreted when this implementation is compared with another implementation of the same technical security measure. The utility contributions should be subtracted from each other. For example, a password expiry frequency of once a quarter contribute 0.73(0.31- -0.42) points more to utility than a password expiry frequency of never.

Table 24 - Utility contribution of the technical security measures when assuming an RUM model

Technical security measure	Implementation	Utility contribution	t-value
Password Length	No restrictions	-0.87	*
	Minimal 8 characters	-0.02	-0.23
	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	0.89	11.28
Password expiry frequency	Never	-0.42	*
	Once a year	0.11	1.46
	Once a quarter	0.31	4.78
Browser restrictions	Every browser is allowed	0.35	*
	Obligatory browser	-0.35	-7.23
E-mail restrictions	No restrictions	-0.11	*
	Warning message with e-mail	0.09	1.35
	Pop-up message with e-mail which contains confidential words	0.02	0.21
File sharing	No restrictions	-0.19	*
	Via corporate shared drive	0.19	3.86

* For the utility contributions which match with the estimated parameter value of the indicator variable, the t-value is given. The utility contributions 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.

Since table 24 can only be interpreted when the utility contribution of a technical security measure implementation is compared with another implementation of the same technical security measure, table 25 gives an example of such a comparison. Table 25 gives an overview of the difference in utility contribution per technical security measure implementation compared to the no restrictions alternative for the same technical security measure. The larger the utility contribution, the more important employees consider the implementation of this technical security measure. The table reveals that is the biggest contribution to utility is gained when from no password length restrictions shifted is to a password with minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character is implemented. The biggest decrease in utility contribution will be reached when an obligatory browser will be implemented instead of allowing the use of every browser. The smallest effect on the utility contribution is the implementation of e-mail restrictions. Both a warning message and a pop-up message shows a very small increase in utility contribution compared to no e-mail restrictions.

Table 25 - Utility contribution of technical security measure implementations vs. no restrictions

Technical security measure	Implementation	Utility contribution
Password Length	Minimal 8 characters	0.85
	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	1.76
Password expiry frequency	Once a year	0.53
	Once a quarter	0.73
Browser restrictions	Obligatory browser	-0.70
E-mail restrictions	Warning message with e-mail	0.20
	Pop-up message with e-mail which contains confidential words	0.13
File sharing	Via corporate shared drive	0.38

6.4.3 Compare choice models

To see which of the two assumptions (Section 6.4.1 or 6.4.2) makes a better prediction for employees choosing a package with technical security measures, the model fits of both assumptions are compared in table 26. A choice model based on perceived security and usability has a much higher final log likelihood (-460.77) than the choice model based on technical security measures (-565.66). With a calculated likelihood ratio statistic of 209.78, the chance that a better fit for the choice model based on security and usability is due to coincidence is smaller than 1%.

Table 26 - Model fits of two choice models

Choice model based on...	Final log likelihood
Perceived security and usability	-460.77
Technical security measures	-565.66

6.4.4 Personal characteristics

Since table 26 revealed that a choice model based on perceived security and usability has a better model fit than a choice model based on technical security measures, the security and usability choice model will be elaborated on in the following section. The estimated betas for security and usability in table 21 are generalized utility contributions. They are generalized in such a way that for each type of employee the utility contribution is the same. However, the contributions could differ between different kinds of employees, since one employee could make his/her choices based on different importance for perceived security and usability than others. To investigate the potential differences, the interaction effects of the importance of the usability/security perceptions with personal characteristics are estimated. This interaction shows the increase or decrease in the importance of the usability/security perceptions to be incorporated when an employee with a specific characteristic makes a choice. Formula 5 shows an example of the contribution of a personal characteristic on the (linear) usability level.

$$Personalcharacteristic\ contribution = (Attributeweight + Interactioneffect * Personalcharacteristic) * Usabilitylevel \quad (5)$$

For every characteristic of an employee described in section 5.4.1 & 5.4.2 it is tested whether these characteristics have a significant influence on the importance of perceptions. Most of the characteristics are proven to be of insignificant influence. For example, whether employees have followed some sort of security awareness training or not does not play a role in the trade-off between the importance of perceived security and usability. Of all the characteristics, only one was found to be of significant influence: current employment in the information and/or cyber security domain. With the incorporation of this characteristic a new choice model is estimated. Table 27 shows the outcomes of this model. The characteristic 'current employment in the information and cyber security domain' is found to have a large effect on the contribution of perceived usability to the utility. The interaction found is positive, which means that for employees who are currently working in the information/cyber security domain, the importance of perceived usability in their preference towards technical security measures increases. For employees not working in the information/cyber security domain, the utility contribution of perceived

usability will decrease. Current employment in information/cyber security domain does not have an impact on the utility contribution of perceived security. This stays the same for every type of employee. To give a clearer insight in the found relation between the importance of perceived usability and employment in the information/cyber security domain figures 16 and 17 are created. These figures show that for employees employed in the information/cyber security domain perceived usability contribute more to the utility of an alternative than perceived security. For employees not working in the information/cyber security domain the effect is the other way around: there perceived security contribute more to the utility of an alternative than perceived usability. The figures 16 and 17 reveal also the effect of the found interaction with the quadratic components of perceived usability. For employees not working in the information/cyber security domain the difference between utility contributions by perceived security and usability increases the higher the perceived security and usability level of the alternative became (see figure 17). For employees working in the information/cyber security domain, this situation is different. For a perceived security and usability level up to 3 (=neutral), the difference between utility contributions by perceived usability and security increases, but from level 3 upwards this difference decreases (see figure 16).

Table 27 - Choice model with personal characteristics

Variables	Beta	t-value
Perceptions		
Security (linear)	2.46	5.77
Usability (linear)	3.32	5.70
Security (quadratic)	-0.18	-2.70
Usability (quadratic)	-0.35	-4.14
Interactions		
Usability (linear) with employed in security	1.13	2.01
Usability (quadratic) with employed in security	-0.19	-2.33

The results found are counter intuitive, one would expect that for employees working in the information/cyber security domain, security is a more important component than usability, but this research showed that it is the other way around. A possible explanation for this effect could be that employees working in information/cyber security domain are confident of their own security behaviour. They could think that they do not need technical security measures with a high security level, since they would behave already in a secure way despite the technical security measure that would be implemented. In that case usability of the implemented technical security measures is more important for them. This could be one of the possible arguments for explaining the betas found in table 27. However, hypothesizing of what causes this effect is more guessing than knowing. More research is needed to be able to give a well-founded answer to the cause of the found effect. In addition, the significance of the effect found only reveals that there is indeed an effect of current employment in the information/cyber security domain on the utility contribution of perceived usability. It does not reveal if the strength of this effect within the population is as strong as it was found to be for this sample. More research is needed to give more insight into the strength of the effect as well.

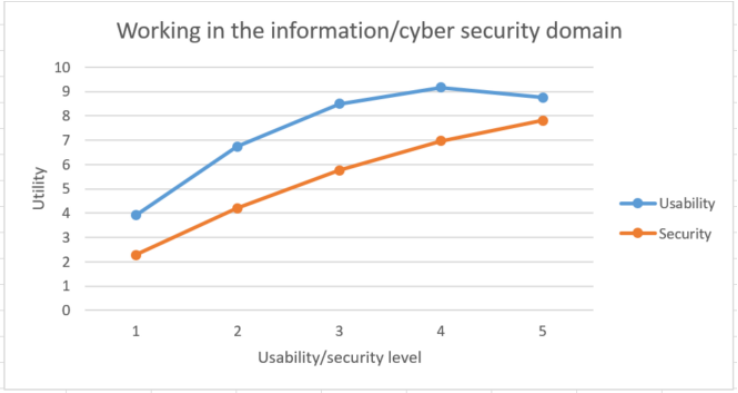


Figure 16 - Visualization of the effect of working in the information/cyber security domain

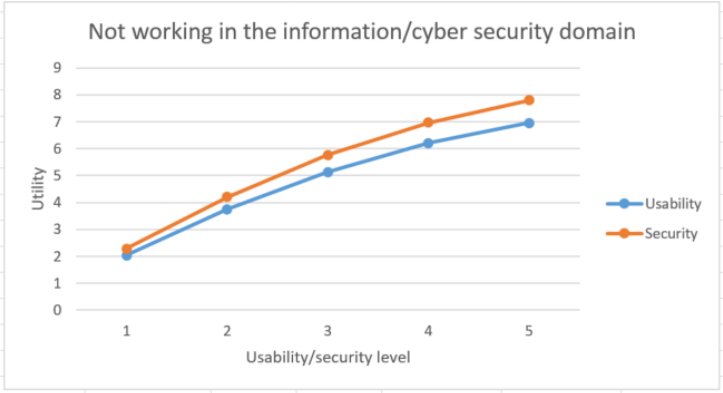


Figure 17 - Visualization of the effect of not working in the information/cyber security domain

6.4.5 Combined choice model

Besides comparing the two choice models (section 6.4.3), combining them is also a possibility. This combined model can be found in table 28. The final log likelihood of this model, -425.37, reveals that this combined model has a better model fit than the separate choice models (table 26). To be sure if this better model fit is not due to coincidence a likelihood ratio test is performed. With a calculated likelihood ratio statistic of 70.80, the chance that a better fit for the combined choice model compared to a choice model based on only usability and security is due to coincidence, is less than 1%. With a calculated likelihood ratio statistic of 280.58, the chance that a better fit for the combined choice model compared to a choice model based on only usability and security is due to coincidence, is also less than 1%.

This model reveals two important insights. Firstly, table 28 shows that the parameters of the perceptions about usability and security are much larger than the parameters of the technical security measures. This implies that usability and security perceptions are a better predictor of choices than the technical security measures in themselves. This in in line with what is already discussed in section 6.4.3, that the choice model with perceptions on usability and security has a much better model fit than the choice model with the technical security measures. More research is needed to research how this is possible, since the usability and security perceptions are based on these technical security measures.
Secondly, this research reveals that this combined choice model fits better than the separated choice models, which means that this combined model has extra prediction power. So the addition of perceptions about usability and security much add something new. A possibility could be that for specific combinations of technical security measures other usability/security level are perceived. This kind of interaction could be revealed by the extra prediction power of this model. However, more research is needed to investigate what actually the aspects are that cannot be measured by either only the technical security measures or only usability/security weights, but that can be measured with the combined model.

Table 28 - Utility contribution of the variables in a combined choice model

		Parameter	t-value
Attributes	**Indicator variables**		
Password Length	Minimal 8 characters	-0.11	-1.14
	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	0.57	5.89
Password expiry frequency	Once a year	-0.03	-0.30
	Once a quarter	0.28	3.46
Browser restrictions	Obligatory browser	-0.22	-3.98
E-mail restrictions	Warning message with e-mail	0.03	0.43
	Pop-up message with e-mail which contains confidential words	-0.07	-0.73
File sharing	Via corporate shared drive	0.05	0.78
Perceptions	**Linear or quadratic**		
Security	Linear	2.51	5.74
Usability	Linear	2.33	4.37
Security	Quadratic	-0.24	-3.62
Usability	Quadratic	-0.19	-2.57

6.5 Combination of regression and choice model

The estimated combined choice model can be of practical use by estimating the choice probabilities of different alternatives with technical security measures. This gives a company insight in which package with technical security measure will probably be preferred by her employees. A required input of the choice model is the perceived usability and security levels. These perceived levels can be estimated with the help of the linear regression model of section 6.3. To see how this combination of the regression model with the choice model can be used, two examples are given below.

The choice probabilities in figure 18 and 19 are calculated as follows. First the perceived usability and security level of each technical security measure within each packages is estimated. This is done with the estimated linear regression model of section 6.3. Thereafter these perceived levels are used as input in the combined choice model of section 6.4.5. This result in an estimated utility per alternative. With the estimated utility the choice probability can be estimated.

The first example shows two extreme scenarios of what a CISO in a company can decide. The first alternative (package A) is that no technical security measures are implemented at all. The second alternative is that all the strictest versions of the technical security measures are implemented. Figure 18 shows that package B has 98% of being chosen by the employees. This means that employees in general would prefer the stricter scenario over the no restrictions scenario. This is due to the difference in impact on perceived usability and perceived security of the technical security measures in the regression model. The technical security measures in package A score very low on the perceived security level, compared to package B. Although package B is perceived as less usable, as described before the impact difference in security is larger than the impact difference of usability.

	Package A	**Package B**
Password length:	No restrictions	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Never	Once a quarter
Browser restrictions:	Every browser is allowed	Obligatory browser
E-mail to someone outside the company:	No restrictions	Pop-up message with e-mail which contains confidential words
File sharing within company:	No restrictions	Via corporate shared drive
Choice probability	2%	98%

Figure 18 - A first example of using the model to estimate choice probabilities

The second example shows the extreme scenario again with all the strictest restrictions (package B) compared to a medium strict scenario (package A). Figure 19 shows that package A has a chance of 47% to be chosen by the employees and package B a 53% to be chosen. Now the difference in choice probability is relatively small. This is due to the fact that the difference in security and usability for both packages is smaller than the differences in figure 18. Since the choice model reveals that security and usability are (almost) equally important the choice probabilities of both packages are relatively close to each other.

	Package A	**Package B**
Password length:	Minimal 8 characters	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Once a year	Once a quarter
Browser restrictions:	Every browser is allowed	Obligatory browser
E-mail to someone outside the company:	Warning message with e-mail	Pop-up message with e-mail which contains confidential words
File sharing within company:	No restrictions	Via corporate shared drive
Choice probability	47%	53%

Figure 19 - A second example of using the model to estimate choice probabilities

Both examples reveal the practical advantage the estimated model of this research can have. When companies have multiple options of combinations of technical security measures they could estimate per option the chance that their employees would choose the package when they would have been possible to make the choice. This can be a powerful tool for companies to get insight into the preferences of their employees with regard to technical security measures.

6.6 Conclusion

This chapter discussed the results retrieved from the data of the conducted survey. The key insights from this chapter are:

- From all the technical security measures in an alternative, the implementation of which browsing restrictions to use has the highest impact on the perceived usability level. Followed by the different implementations of password expiry frequency and e-mail restrictions. Only a very small difference in perceived usability is observed in the different implementations of file sharing restrictions and in the different implementations of password length
- From all the technical security measures in an alternative, the decision which implementation of password to use has the highest impact on the perceived security level. Also the different types of password expiry frequency have a large impact on the perceived security level of the alternative. Followed by e-mail restrictions and file sharing implementations. The different options of browsing restrictions show to have almost no difference in terms of perceived level of security.
- For most of the technical security measures, it holds that there is a large difference between the possible implementations of a technical security measure in terms of perceived security. The difference between the implementations on perceived usability is smaller. This means that there is a larger difference (mostly twice as large or even larger) of perceived level of security of the different implementations of a technical security measure than on the perceived level of usability.
- Perceived usability and security are found to be slightly negatively correlated.
- Employees actually make a trade-off between perceived usability and security when choosing between packages with multiple technical security measures.
- Perceived usability and security are equally important to an employee when choosing between packages with multiple technical security measures.
- Per unit increase in perceived usability or security the increase in utility will be smaller. This means that if 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. However, 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.
- Most of the personal characteristics of an employee do not play an important role in perceived usability and security and in the trade-off between security and usability.
- The personal characteristic that has a large impact on the perceived security level is perceived online risk awareness. The more online risk aware employees consider themselves, the lower the perceived security level by these employees.
- The personal characteristics 'current employment in the information/cyber security domain' has a large impact on the importance of perceived usability in the trade-off between perceived security and usability. Employees who are working in the information/cyber security domain consider perceived usability as more important than perceived usability. 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.
- A combined choice model where the trade-off between perceived usability and security is combined with the effect of technical security measures allows for better estimation than both models separately do.

7. Conclusion and recommendations

7.1 Introduction

Companies implement technical security measures to protect themselves from hacks and data losses. However, employees can circumvent these measures, making them less effective and making it easier for hackers to attack the company. To prevent this circumventing behaviour, companies should design the measures in line with the employees' desires. Companies should acknowledge their employees' preferences, because when the technical security measures implemented correspond with the preferred technical security measures of the employees, a lower circumvention rate is expected. It is assumed that employees' preferences towards technical security measures are based on the degree of usability and security of these measures. The way in which employees perceive the usability and security of these technical security measures is important when making a choice between different technical security measures, as well as finding the trade-off between the importance of perceived security and usability. Since there is no knowledge yet about what employees think of usability and security of technical security measures, this thesis is the first to investigate this. Research was conducted to gain insight into (1) the way employees perceive usability and security and (2) what trade-off between the importance of perceived usability and security employees make.

The following sections outline the main outcomes of this research. In section 7.2 the answers to the sub-questions of this thesis are given and in section 7.3 the main question of this research is answered. In section 7.4 recommendations are provided for further research as well as recommendations for companies how they can incorporate these insights in their daily practices. In section 7.5 the relative position within scientific literature will be discussed. This chapter ends with reflecting upon the limitations of this research.

7.2 Answers to the sub-questions

1. *"What technical security measures exist and which of these are suitable for researching the trade-off between usability and security?"*

This research focused on technical security measures that fit the definition of a technical security measure used for this research: A technical security measure is an electronic security method that protects information on a computer. Using this definition, the following technical security measures were found: authentication, encryption, network security, secure device pairing, access control, endpoint protection, redundancy of critical systems, secure configuration, browsing security, security monitoring, data loss prevention and secure remote working. Out of these measures a selection of the most appropriate measures was made. This selection was done based on a couple of selection criteria and on insights from a pilot study. The left column of table 29 shows the chosen measures. However, since these technical security measures are quite broad, they can better be seen as technical security measures classes. Specific technical security measures for each class were selected to be used in this thesis (see the right column of table 29).

Table 29 - Selected technical security measures and their overarching classes

Technical security measure class	Technical security measure
Authentication	Password length
	Password expiry frequency
Browsing security	Browser restrictions
Data loss prevention	File sharing inside company
	E-mail to someone outside the company

2. *"How do employees perceive the usability and security level of the selected technical security measures?"*

For all the technical security measures mentioned above the impact that these measures have on perceived usability and security is estimated.

For perceived usability the biggest impact is caused by browsing restrictions. Having an obligatory browser in place results in a lower perceived usability than when employees have the possibility to use the browser they want. Password expiry frequency and e-mail restrictions are of less strong effect, but still the impact should not be ignored. For password expiry frequency holds that employees perceive an expiry frequency of never or once a year as more usable than an expiry frequency of once a quarter. For e-mail restrictions, employees perceive no e-mail restrictions as more usable than a warning message and even more usable than a pop-up message with e-mails which contain confidential words. File sharing and password length have a very small effect on the perceived usability level. For employees it does not really matter in terms of perceived usability whether a password length with no minimum length of complexity, 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 biggest impact is caused by the different implementations of password length. 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 higher perceived security level than a password length with minimal 8 characters and even a substantially higher perceived security level than a password length with no minimum length of complexity. Also the password expiry frequency has a large effect on the perceived security. Employees perceive an expiry frequency of once a quarter as more secure than an expiry frequency once a year and even as way more secure than a password expiry frequency of never. E-mail restrictions and file sharing are medium important for the perceived level of security. For e-mail restrictions holds that 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 holds that employees consider file sharing via a corporate shared drive as more secure than when it is allowed to use every type of application. Browsing restrictions is the technical security measure that has the least impact on perceived security level. Employees perceive an obligatory browser as almost same secure as when there are no browsing restrictions in place.

Important to note is that for the discussed effects on perceived usability and security, for most of the technical security measures holds that the effects on perceived security have a larger spread than the effects on perceived usability. The effect on perceived security is twice as large (or even larger) as the effect on perceived usability. An exception is browsing restrictions, there the difference between the possible implementations: no browser restrictions or an obligatory browser, have a larger difference in terms of perceived usability than the difference in terms of perceived security.

What is revealed as well by the analysis on perceived usability and security is that for most of the technical security measures the sign for perceived security and usability is opposite. For example, an obligatory browser has a negative effect on perceived usability, while at the same time has a positive effect on perceived security. Calculating this relation between perceived usability and security in general result in a slightly negatively correlation (-0.14) between perceived usability and security.

Tested is whether personal characteristics of employees influence the perceived usability and security level. Most of the personal characteristics of an employee did not play an important role in perceived usability and security. The personal characteristic that had the largest impact on the perceived security level is perceived online risk awareness. The more online risk aware employees consider themselves, the lower the perceived security level by these employees.

3. *"What is for employees the trade-off in weighing perceived usability and security when choosing between different combinations of technical security measures?"*

This research showed that employees choose between packages with technical security measures based on utility maximisation behaviour. This means that the package which gives employees the highest utility has the highest chance to be chosen. The utility of each package is dependent on the trade-off between the importance of perceived usability and security. In general employees consider perceived security and

usability as equally important. This means that the perceived level of security of technical security measures contribute with the same size to utility than the perceive level of usability of technical security measures does. What the analysis also reveals is that the influence of an increase in either perceived security or usability decreases when the perceived security or usability level increases. So when the usability and security level of a technical security measure is perceived as low, one level increase in perceived 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 perceived usability or security will have a less strong effect on the gained utility.

Tested is whether personal characteristics of employees influence the trade-off between the importance of perceived usability and security. Although most of the characteristics are not of influence, one characteristic has a big influence: current employment of employees 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.

7.3 Answer to the main question

"How do employees perceive security & usability of technical security measures at their work and what is the trade-off they make between these aspects in their choices for technical security measures?"

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. For perceived usability the largest effect is caused by browsing restrictions. While browsing restrictions show to have almost no effect on the perceived security. The biggest effect on perceived security is caused by password length restrictions. While password length restrictions show to have 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 level of usability and security is determined by the trade-off. Employees consider perceived usability and security to be equally important in their choice for technical security measures. The influence of an increase in either perceived security or usability decreases when the perceived security or usability level increases.

7.4 Recommendations

7.4.1 Recommendations for practice

In order to advice companies on how they can align the preferences and perceptions of their employees with their implemented technical security measures, the outcomes of this research can be used for practical recommendations.

An important outcome of this study is that employees' preferences for technical security measures are based on utility maximisation. This implies that when employees can choose between multiple packages with different implementations of technical security measures, the package that brings employees the highest utility has the highest chance to be chosen. For practice this means that companies should emphasize the utility that can be gained by technical security measures, because employees prefer technical security measure that brings them high utility. They should show the positive side of technical security measures to their employees. A common practice nowadays is showing employees the dangerous things that can happen when no technical security measures are implemented (Boerman, 2016). This however, is focused on the possible regret that one could experience not using technical security measures. However, what this research shows it that a company should talk to its employees about the opportunities that can be realized by implementing technical security measures, since this triggers employees in their preferences for technical security measures.

An important message that this research tries to convey is that the viewpoint of employees is important to take into account when making decisions about which technical security measures to implement in a

company. Companies could do this by using the model used in section 6.5 to estimate the choice probability of different technical security measure alternatives. However, if a company has different technical security measures that are not in scope of this research (which in practice often will be the case) this model cannot be used. Another possibility would then be to design a new survey with the technical security measures inside that specific company. This research shows that using a survey about technical security measures can give useful insights. One of the most important outcomes that this research generates is that perceived usability is considered equally important as perceived security for employees. This gives an opportunity for companies to incorporate the perceptions and preferences of employees into the security designing process of a company. Mostly the decision process for technical security measures is a top-down approach where employees are not involved in this decision process. However, since this research reveals that employees do care about security, companies could think about a more cooperative security decision process.

Most of the personal characteristics did not have and influence (or only a relative small influence) on either employees' perception of usability and security or the trade-off between the two. One of these characteristics was security awareness training, meaning that there is (almost) no difference in the perceptions and the trade-offs of employees who did or did not follow a security awareness training. This outcome is quite surprising, since security awareness training is mostly seen as the Holy Grail to educate employees about security (Bracht, 2016; Ferrillo, 2015). Nevertheless, it is not recommended to stop with giving security awareness trainings, but companies should critically evaluate the content of their trainings. Perhaps the way in which the security awareness trainings are organised and the topics that are covered in these trainings are not effective enough. The earlier-made recommendations about how to approach employees could be useful in improving these trainings.

If companies want to consider quick wins in implementing technical security measures that are in line with their employees' preferences they should consider a password requiring a minimum of 8 characters, 1 uppercase letter, 1 special character and 1 numeric character. A password with these restrictions gives a high increase in perceived security, while at the same time the perceived usability will not decrease. Apparently employees are not annoyed by these password restrictions and see the added value it has to security. Another quick win can be realised by not installing an obligatory browser. An obligatory browser decreases the perceived usability and employees do not see the added value of this technical security measure when it comes to security. Important to mention here is that these technical security measures are quick wins through the eyes of employees. What the real impact is for the security level of the company is something which was not incorporated in this research.

7.4.2 Recommendations for science

Since this research is a thesis research, the time to perform this research was limited. Due to these time constraints, narrow scoping and simplified assumptions were inevitable. The result is that some interesting aspects were left out of the scope of this study. This section will reflect on these aspects by elaborating on the aspects that could be explored further in future studies.

It would be interesting to see if the technical security measures that employees think are secure are indeed the ones that have the have a high security level. This research focused on perceived security rather than on factual security. Further research could measure the factual security level of the technical security measures as well. Measuring the factual security level could be done by measuring the strength of each technical security measure against certain attacks or through interviews with security experts. Then a comparison can be made between the factual security level and the perceived security level. This could reveal the security knowledge of employees. Insights generated by that research can reveal if employees should be educated more about the real security level of technical security measures or not.

A consequence of the narrow scope of this research is that only a few of the many existing technical security measures were incorporated in this research. This means that the usability and security measurements made in this research are only applicable to these measures. It would be interesting to see if the same conclusions can be drawn for other technical security measures. Recommended for further research is to conduct a new survey where other technical security measures are shown to the respondents

than the ones used in this study. The questions in this survey would remain the same. With the data of the new survey new estimations can be made about the perceptions and the trade-off between usability and security. These estimations can be compared with the calculations of this research to see whether a generalization of the usability and security conclusions of this research is possible or not.

A surprising outcome of this study is that employees who currently are employed in the information/cyber security domain consider perceived usability as more important than perceived security, whereas for employees not working in the information/cyber security domain, perceived security is more important than perceived usability in their overall preferences towards technical security measures. Intuitively, once would expect that this effect would be the other way around. People working in the information/cyber security domain consider security as more important and people not working in this field consider usability as more important. Since the found effect in this research is counterintuitive, it is difficult to give a reason for this effect. Therefore, detailed research is needed to discover what causes this effect. In addition, more research is needed to measure the strength of this effect. Repeating this research among different respondents can reveal if this effect also holds when another sample group is used. This research showed that 'current employment in information/cyber security domain' has a big impact on the weights of security and usability, but perhaps in another sample group this effect is much smaller. Additional research on this effect could also give more insights on the strength of this effect.

This research tested whether some personal characteristics of employees could be of influence on the perceptions and trade-off in weighing security and usability. Although most of the tested personal characteristics were found to have no significant influence, a couple of characteristics did have a significant influence (see section 6). Besides that it is good to know that these characteristics are of influence, further studies could investigate why these personal characteristics are of influence, to better understand people's circumventing behaviour. For example, what is the reason behind the fact that the more knowledge about a computer an employee has, the less usable he/she perceived the technical security measures in general? This would be good to know, since this implies that in some companies with specific types of employees different type of technical security measures may be more effective. Future research, with more emphasize on the influence of personal characteristics, is desired to gain more knowledge on this topic.

Another possible direction for future research is a study that employs a hybrid choice model. In this thesis a model is estimated with a linear regression model used as the input for a choice model. This is a sequential model, where first the regression model is estimated and subsequently the choice model. However, a possibility would be to make use of a simultaneous model, where everything is estimated at once. This is called a hybrid choice model. It would be interesting to see if the hybrid choice model has a better predication power than the model used in this research.

7.5 Discussion

It is important to see the relative position of this study with regards to already existing scientific literature. Therefore, this section discusses new insights this research gives to scientific literature, but is also provides a critical reflection about the validity of these results in a broader scope than used in this research.

Perceptions

Existing literature reveals that usability and security are negatively correlated: improving one will negatively affect the other (Andersson, 2013; Kainda et al., 2010; Nurse et al., 2011). However, this claim was barely supported with empirical results. This research fills this gap by providing empirical evidence for the afore mentioned claim. This research reveals that security and usability are indeed negatively correlated. The advantage of having empirical results is that this makes it possible to measure the strength of the correlation between security and usability. Literature never made explicit how strong the negative correlation is. Measurements in this research reveal that the perceived security and usability level of technical security measures are only slightly negatively correlated: a correlation of -0.14 is measured. Although it is useful to have this correlation measured, these empirical results should be interpreted with restraint. Firstly, the measured correlation between security and usability only holds within the specific scope of this research. This means that this measured correlation only reflects the relation perceived by the group of respondents used in this research and only upon the 5 technical security measures in scope

of this research. More research is needed to see whether this measured correlation also holds for other technical security measures and other respondent groups. Secondly, a point of discussion is whether it was appropriate at all 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 6.3.3 could be not fully correct.

Choice modelling

Besides giving empirical insights, this research was also useful to see whether it is possible to apply choice modelling within the field of information security. This research shows that choice modelling is indeed a useful method to measure security related choices of employees. However, since this is the first information security study that used this method (as far as the author knows), a critical reflection of this study is required. Since it is the first study, the aim of this research was to sketch a broad perspective upon employees' trade-off between security and usability rather than giving very specific recommendations. The outcomes of this research should not be considered as the only truth on how employees think about information security, since a couple of assumptions and simplifications were made (see the section discussion below). Despite the fact that these simplifications have an impact on the outcomes and the validity of the research, this research reveals some first insights on the trade-off made by employees. However, these insights can be expanded by for example, focus on other security measures or on another group of people instead of employees in general. It is therefore recommended to consider this research not as final stage, but as a launching pad for more research within this research area.

Viewpoint of employees

Another important contribution of this research to science is that this is research focuses on security and usability from the viewpoint of employees. In the majority of the studies usability and security are measured by experts or scientific researchers rather than asking employees about their perceptions. Since employees are the end-users of technical security measures, their perceptions and preferences towards usability and security of technical security measures are important aspects when designing these security measures. End-users are the ones that can let a security measure fail or succeed. This research provides some first insights into the view of employees on security and usability. However, more user-centric research is needed to give a more well-founded insight in the perceptions and preferences of employees. One of the possible directions for this research can be for example performing interviews rather than a survey, to explore the perceptions and preferences of employees. Hopefully the importance of this study will create urgency among other researchers to expand this research area with more empirical user-studies.

7.6 Limitations

Performing research required the researcher to make decisions. Despite the fact that these decisions are made with cognition, every decision has its consequences. This section will reflect upon the negative consequences of these decisions by exploring the drawbacks and limitations of this research.

Respondents

Important point of discussion is the randomness of the sample group. Is the group of respondents indeed a random group taken out of the population or is the sample not as random as it ideally should be? To distribute the survey snowball sampling is used, whereby respondents were asked to send the survey to three other persons. Since the starting point of this snowball effect was the network of the researcher herself, it could be questioned if the sample can be considered as random. An argument against considering the sample random is for example the high percentage of highly educated employees in the sample. This is a sign that the sample taken out of the population was only a sample of a specific type of employees.

Hypothetical situation

A big disadvantage of this research is that the survey regarded a hypothetical setting in which employees were giving 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 (Loomis, 2011). Employees could pretend to be the perfect employee by choosing the alternative with an equal level of security and usability, whereas they would actually prefer the other alternative with a higher 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 of them by the company.

Choice model

A limitation of this research is that the priors used for specifying the design of the final survey are based on RUM. Ngene, the software used to design the final survey, can only specify a design based on RUM. It would therefore be strange to insert priors based on a RRM model into an RUM model. Van Cranenburgh, Rose, and Chorus (2016) are now conducting research about the potential influence this has on the model fits of RUM and RRM of the final study. This research reveals that it indeed has an effect on the model fits of the final study. In this thesis, a better model fit of RUM was estimated. However, this is quite logical since the survey was also designed based on a RUM model. Van Cranenburgh et al. (2016) stated that the performance of the RRM model is always underestimated when the study in designed based on RUM.

A design decision which impacts the outcomes of the study is to explicitly ask people about usability and security before asking them to choose an alternative. Forcing people to think about usability and security makes them conscious about these aspects. This could be a reason why the choice model based on security and usability has a better model fit than the choice model based on the technical security measures. Looking back, a control group where respondents were first asked to make a choice and thereafter specify their perceived levels of usability and security of the alternatives, would have been a good addition. This would have made it possible to see if the order of choice and perception questions is of influence.

Impact on circumvention

A last important limitation that needs to be mentioned is the assumed effect of 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 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, reality should show if adapting to these preferences will indeed lead to a high decrease in circumvention.

References

Andersson, D. (2013). Authentication with Passwords & Passphrases: Implication on Usability and Security. *RLV Blog.* Retrieved April 18, 2016, from http://www.rlvision.com/blog/authentication-with-passwords-passphrases-implications-on-usability-and-security/

Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. *Security & Privacy, IEEE, 5*(1), 36-44.

Bejtlich, R. (2004). What is Network Security Monitoring. Retrieved June 23, 2016, from http://www.informit.com/articles/article.aspx?p=350391

Belden, M. M., & Hirschmann, J. M. (2011). Network rudandancy reduces risk, downtime. Retrieved May 12, 2016, from http://www.controleng.com/single-article/network-redundancy-reduces-risk-downtime/fbb380911a5b1769eb01347fdc8c30c7.html

Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997). *A concrete security treatment of symmetric encryption.* Paper presented at the Foundations of Computer Science, 1997. Proceedings., 38th Annual Symposium.

Boerman, P. (2016). Cybercrimespecialist Deloitte: 'Managers creëren zelf hun cyberrisico's'. Retrieved August 17, 2016, from http://www.mt.nl/90/89447/management/cybercrimespecialist-deloitte-managers-creeren-zelf-hun-cyberrisico-s.html

Bracht, D. (2016). The importance of security awareness training for enterprise IT governance. Retrieved August 27, 2016, from http://www.appstechnews.com/news/2016/jan/22/importance-security-awareness-training-enterprise-it-governance/

Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a trade-off between usability and security: a metrics based-model *Human-Computer Interaction–INTERACT 2007* (pp. 114-126): Springer.

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation *People and Computers XIV—Usability or Else!* (pp. 405-424): Springer.

Brostoff, S., Sasse, M. A., Chadwick, D., Cunningham, J., Mbanaso, U., & Otenko, S. (2005). 'R-What?'Development of a role-based access control policy-writing tool for e-Scientists. *Software: Practice and Experience, 35*(9), 835-856.

Cao, X., & Iverson, L. (2006). *Intentional access management: Making access control usable for end-users.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.

Carifio, J. (1976). Assigning Students to Career Exploration Programs by Preference. *Career Education Quarterly.*

Carifio, J. (1978). Measuring Vocational Preferences: Ranking versus Categorical Rating Procedures. *Career Education Quarterly, 3*(2), 17-28.

CBS. (2015). Telewerken weer in de lift. Retrieved May 25, 2016, from https://www.cbs.nl/nl-nl/nieuws/2015/51/telewerken-weer-in-de-lift

Chorus, C. G., Arentze, T. A., & Timmermans, H. J. (2008). A random regret-minimization model of travel choice. *Transportation Research Part B: Methodological, 42*(1), 1-18.

Communications-Electronics Security Group, Department for Business Innovation & Skills, Centre for Protection of National Infrastructure, & Cabinet Office. (2012). Reducing the Cyber Risk in 10 Critical Areas. Retrieved May 25, 2016, from https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Cranor, L. F., & Garfinkel, S. (2004). Guest Editors' Introduction: Secure or Usable? *Security & Privacy, IEEE, 2*(5), 16-18.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

de Vocht, A. (2009). *Basishandboek SPSS 17 SPSS Statistics.* Utrecht: Bijleveld Press.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2006). *User behavior toward preventive technologies-cultural differences between the United States and South Korea.* Paper presented at the ECIS.

Dougherty, C. (2001). t Distribution: Critical Values of t. In S. Tables (Ed.): Oxford University Press.

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Ferrillo, P. A. (2015). Is employee awareness and training the holy grail of cybersecurity? Retrieved August 17, 2016, from http://www.advisenltd.com/2015/03/11/is-employee-awareness-and-training-the-holy-grail-of-cybersecurity/
Festinger, L. (1962). *A Theory of Cognitive Dissonance*: Stanford University Press.
Festinger, L., & Carlsmith, J. M. (1959). Cognitive consequences of forced compliance. *The Journal of Abnormal and Social Psychology, 58*(2), 203.
Fidas, C. A., Voyiatzis, A. G., & Avouris, N. M. (2010). *When security meets usability: A user-centric approach on a crossroads priority problem.* Paper presented at the Informatics (PCI), 2010 14th Panhellenic Conference on.
Garfinkel, S. L., & Miller, R. C. (2005). *Johnny 2: a user test of key continuity management with S/MIME and Outlook Express.* Paper presented at the Proceedings of the 2005 symposium on Usable privacy and security.
Herley, C. (2009). *So long, and no thanks for the externalities: the rational rejection of security advice by users.* Paper presented at the Proceedings of the 2009 workshop on New security paradigms workshop.
Identity Theft Resource Centre. (2016). Identity Theft Resource Center Breach Report hits Near Record High in 2015.Retrieved Juli 20, 2016, from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html
Kainda, R., Flechais, I., & Roscoe, A. (2010). *Security and usability: Analysis and evaluation.* Paper presented at the Availability, Reliability, and Security, 2010. ARES'10 International Conference.
Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International journal of information management, 23*(2), 139-154.
Kassner, M. (2011). Endpoint security: What makes it different from anitvirus solution. Retrieved May 26, 2016, from http://www.techrepublic.com/blog/it-security/endpoint-security-what-makes-it-different-from-antivirus-solutions/
Khosrow-Pour, M. (2006). *Dictionary of Information Science and Technology*: Idea Group Reference.
Kobsa, A., Sonawalla, R., Tsudik, G., Uzun, E., & Wang, Y. (2009). *Serial hook-ups: a comparative usability study of secure device pairing methods.* Paper presented at the Proceedings of the 5th Symposium on Usable Privacy and Security.
Kuo, C., Romanosky, S., & Cranor, L. F. (2006). *Human selection of mnemonic phrase-based passwords.* Paper presented at the Proceedings of the second symposium on Usable privacy and security.
Laerd Statistics. (2013). Background & Requirements. *Simple Linear Regression.* Retrieved 11 August, 2016, from https://statistics.laerd.com/premium/spss/lr/linear-regression-in-spss-3.php
Loomis, J. (2011). What's to know about hypothetical bias in stated preference valuation studies? *Journal of Economic Surveys, 25*(2), 363-370.
Manski, C. F. (1977). The structure of random utility models. *Theory and decision, 8*(3), 229-254.
McFadden, D. (1974). Conditional Logit Analysis of Qualitative Choice Behavior. In P. Zarembka (Ed.), *FRONTIERS IN ECONOMETRICS* (pp. 105-142). New York: Academic Press.
Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information management & computer security, 16*(4), 377-397.
Molin, E. (2016). SPM4612: Lecture 4 Efficient designs. Delft: TU Delft.
Molin, E., & Marchau, V. (2004). User perceptions and preferences of advanced driver assistance systems. *Transportation Research Record: Journal of the Transportation Research Board*(1886), 119-125.
Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). *Guidelines for usable cybersecurity: Past and present.* Paper presented at the Cyberspace Safety and Security (CSS), 2011 Third International Workshop.
Parekh, S., Madan, B., & Tugnayat, R. (2012). Approach For Intrusion Detection System Using Data Mining. *Journal of Data Mining and Knowledge Discovery, 3*(2), 83 - 87.
PennState Science. (n.d.). Chi-Square Distribution table.
Piper, S. (2013). *Security Configuration Management for Dummies*. Hoboken: John Wiley & Sons, Inc.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237.
Raja, F., Hawkey, K., Jaferian, P., Beznosov, K., & Booth, K. S. (2010). *It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls.* Paper presented at the Proceedings of the 3rd ACM workshop on Assurable and usable security configuration.
Richmond, R. (2012). How to maintain security when employees work remotely. Retrieved May 26, 2016, from https://www.entrepreneur.com/article/224241
Rose, J., & Bliemer, M. (2007). Designing Stated Choice Experiments: State-of-the-Art: The University of Sydney.
Rose, J., & Bliemer, M. (2009). Constructing efficient stated choice experimental designs. *Transport Reviews, 29*(5), 587-617.
Rouse, M. (2014a). Data loss prevention. Retrieved May 25, 2016, from http://whatis.techtarget.com/definition/data-loss-prevention-DLP
Rouse, M. (2014b). Encryption. Retrieved May 12, 2016, from http://searchsecurity.techtarget.com/definition/encryption
Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425-426.
Schultz, E. (2007). Research on usability in information security. *Computer Fraud & Security, 2007*(6), 8-10. doi:http://dx.doi.org/10.1016/S1361-3723(07)70075-1
Sharpened Productions. (2010). Antivirus Definition. Retrieved May 12, 2016, from http://techterms.com/definition/antivirus
Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.
Statista. (2016). Annual number of data breaches and exposed records in the United States from 2005 to 2015 (in millions). Retrieved July 20, 2016, from http://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
SurveyMonkey. (2016). SurveyMonkey. Retrieved May 16, 2016, from https://nl.surveymonkey.com/
Symantec. (2010). What's malware and how can we prevent it? Retrieved May 29, 2016, from http://www.pctools.com/security-news/what-is-malware/
Symantec. (2016). Internet Security Threat Report.Retrieved June 20, 2016, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16287835&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2
Timmermans, H. (1982). Consumer choice of shopping centre: an information integration approach. *Regional Studies, 16*(3), 171-182.
Uzun, E., Karvonen, K., & Asokan, N. (2007). Usability analysis of secure pairing methods *Financial Cryptography and Data Security* (pp. 307-324): Springer.
van Cranenburgh, S. (2015). The µRRM model. *Advanced Random Regret Minimization Models.* Retrieved August 8, 2016, from http://www.advancedrrmmodels.com/#!mu-rrm/cjq5
van Cranenburgh, S., Guevara, C. A., & Chorus, C. G. (2015). New insights on random regret minimization models. *Transportation Research Part A: Policy and Practice, 74*, 91-109. doi:http://dx.doi.org/10.1016/j.tra.2015.01.008
Van Cranenburgh, S., Rose, J. M., & Chorus, C. G. (2016). *On the robustnes of efficient experimental designs towards the underlying decision rule*. Working Paper. Retrieved September 14, 2016, from http://media.wix.com/ugd/4e8049_9a15f92aa2e6414fbd609df6266559ff.pdf
Wei, W. (2016). Top 4 Data Breaches reported in the last 24 Hours: The Hacker News.
Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers, 22*(3), 153-164.
Whalen, T., Smetters, D., & Churchill, E. F. (2006). *User experiences with sharing and access control.* Paper presented at the CHI'06 extended abstracts on Human factors in computing systems.
Whitten, A., & Tygar, J. D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.* Paper presented at the Usenix Security.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). *Authentication using graphical passwords: effects of tolerance and image choice.* Paper presented at the Proceedings of the 2005 symposium on Usable privacy and security.

Zeelenberg, M., & Pieters, R. (2007). A theory of regret regulation 1.0. *Journal of Consumer psychology, 17*(1), 3-18.

Appendix A: Coding scheme

Technical security measure	Implementation		Indicator variables	
Password length (PL)		**Labels**	**PLMM**	**PLM**
	No restrictions	0	-1	-1
	Minimal 8 characters (PLM)	1	0	1
	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character (PLMM)	2	1	0
Password expiry frequency (PEF)			**PEFOQ**	**PEFOY**
	Never	0	-1	-1
	Once a year (PEFOY)	1	0	1
	Once a quarter (PEFOQ)	2	1	0
Browser restrictions (BR)			**BR**	
	Every browser is allowed	0	-1	
	Obligatory browser (BR)	1	1	
E-mail restrictions (ER)			**ERPM**	**ERWM**
	No restrictions	0	-1	-1
	Warning message with e-mail (ERWM)	1	0	1
	Pop-up message with e-mail which contains confidential words (ERPM)	2	1	0
File sharing (FS)			**FS**	
	No restrictions	0	-1	
	Via corporate shared drive (FS)	1	1	

Appendix B: Pilot survey design

Ngene syntax

```
Design
;alts = alt1, alt2, alt3
;rows = 8
;eff = (mnl,d)
;model:
U(alt1) = pl.effects[0|0]*PL[0,1,2] + pef.effects[0|0]*PEF[0,1,2] +
fa.effects[0|0]*FA[0,1,2] +br.effects[0]*BR[0,1] + er.effects[0|0]*ER[0,1,2]
+ fs.effects[0]*FS[0,1] + svc.effects[0|0]*SVC[0,1,2] /
U(alt2) = pl*PL + pef*PEF + fa*FA + br*BR + er+ER + fs*FS + svc*SVC /
U(alt3) = pl*PL + pef*PEF + fa*FA + br*BR + er+ER + fs*FS + svc*SVC
$
```

Normally an efficient design is only used for the final study since actually priors are required to make use of an efficient design. However, since full-factorial design and a fractional factorial design both resulted in a too large number of choice sets, efficient design is already used for the pilot. Since no priors are available about the weights of the attributes, all the priors are set to zero.

Design of the pilot study

Design																					
Choice situation	alt1.pl	alt1.pef	alt1.fa	alt1.br	alt1.er	alt1.fs	alt1.svc	alt2.pl	alt2.pef	alt2.fa	alt2.br	alt2.er	alt2.fs	alt2.svc	alt3.pl	alt3.pef	alt3.fa	alt3.br	alt3.er	alt3.fs	alt3.svc
1	1	2	1	0	0	1	0	2	0	0	0	1	1	1	0	1	0	1	0	0	2
2	2	1	1	1	1	1	0	0	2	1	0	2	0	1	1	0	2	0	0	0	0
3	0	0	2	0	1	0	0	2	1	1	1	0	0	1	1	0	0	0	2	1	2
4	1	1	2	1	2	0	1	1	0	1	0	0	1	2	0	2	0	1	1	1	0
5	1	0	0	1	0	0	1	0	1	2	1	2	1	0	0	1	1	0	1	0	1
6	0	1	0	0	0	1	1	1	2	2	1	1	0	2	2	0	1	1	2	0	0
7	2	2	0	0	2	0	2	0	0	0	1	0	1	0	1	1	1	1	1	1	1
8	0	0	1	1	1	1	2	1	1	0	0	1	0	0	2	2	2	0	0	1	1

Appendix C: Final survey design

Ngene syntax

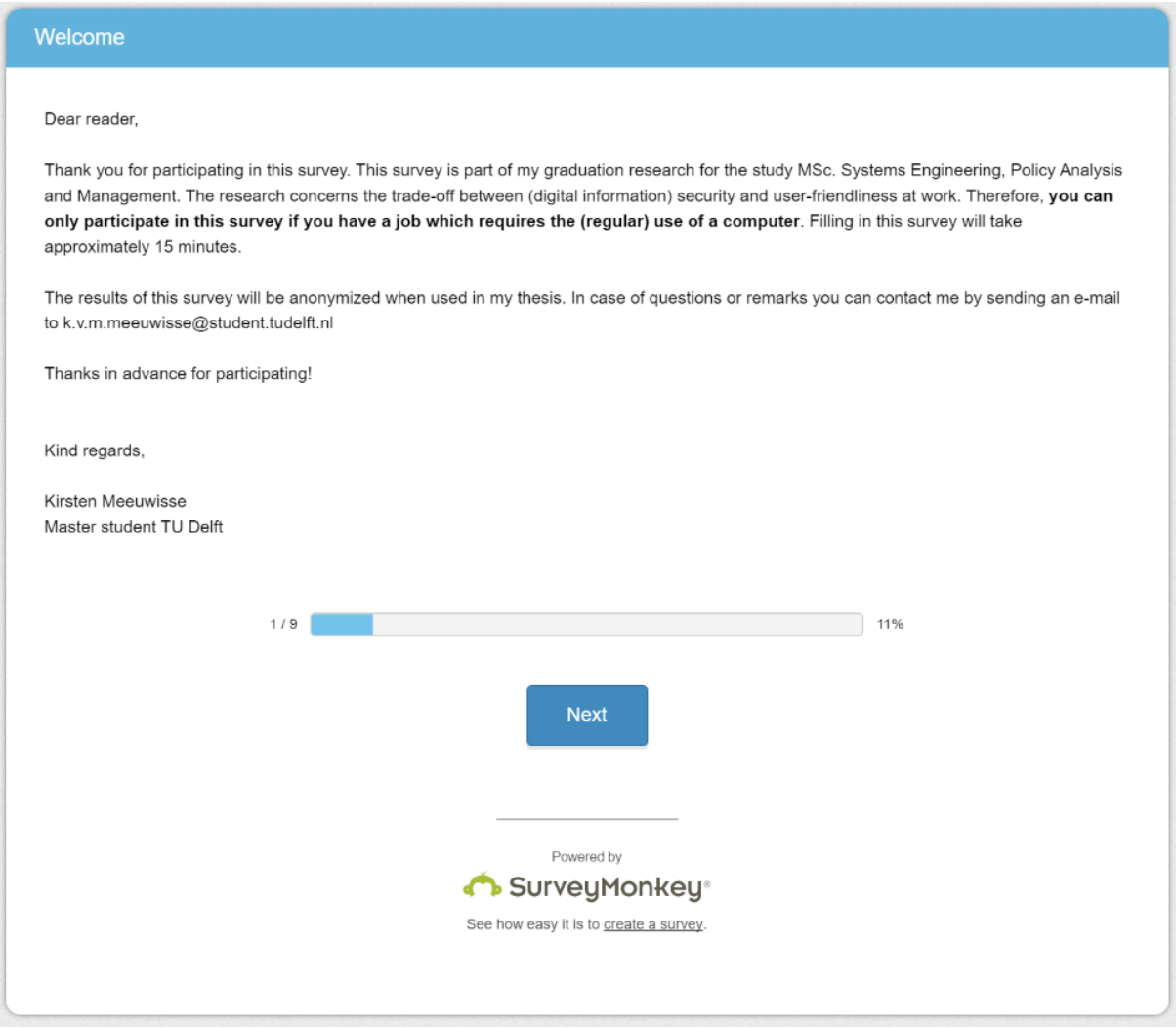
```
Design
;alts = alt1, alt2, alt3
;rows = 6
;eff = (mnl,d)
;block = 2
;model:
U(alt1) = pl.effects[-0.78|0.24]*PL[0,1,2] + pef.effects[-
0.30|0.26]*PEF[0,1,2] +br.effects[-0.23]*BR[0,1] +
er.effects[0.08|0.09]*ER[0,1,2] + fs.effects[0.11]*FS[0,1] /
U(alt2) = pl*PL + pef*PEF + br*BR + er+ER + fs*FS /
U(alt3) = pl*PL + pef*PEF + br*BR + er+ER + fs*FS
$
```

For specifying an efficient design with Ngene the estimated utility contributions of table 9 in section 5 are used. Since effect coding is used for every attribute levels two utility contributions are used. These are the parameters of the indicator variables. These are the numbers between [ ] separated by | in the utility function of the Ngene design syntax. For example, for the technical security measure password expiry frequency the weights of password expiry never (-0.30) and once a year (0.26) are used: pef.effects[-0.30|0.26]*PEF[0,1,2]

Design of the final study

Design																
Choice sit	alt1.pl	alt1.pef	alt1.br	alt1.er	alt1.fs	alt2.pl	alt2.pef	alt2.br	alt2.er	alt2.fs	alt3.pl	alt3.pef	alt3.br	alt3.er	alt3.fs	Block
1	2	2	0	1	1	1	1	1	2	1	2	0	1	0	0	1
2	0	1	1	0	1	2	0	0	2	0	1	2	1	1	1	1
3	1	1	0	0	0	2	0	1	1	1	0	2	0	2	0	2
4	0	0	1	2	1	1	2	0	0	1	0	1	1	1	0	2
5	2	2	1	2	0	0	1	0	1	0	1	0	0	0	1	2
6	1	0	0	1	0	0	2	1	0	0	2	1	0	2	1	1

Appendix D: Final survey English



Welcome

Dear reader,

Thank you for participating in this survey. This survey is part of my graduation research for the study MSc. Systems Engineering, Policy Analysis and Management. The research concerns the trade-off between (digital information) security and user-friendliness at work. Therefore, **you can only participate in this survey if you have a job which requires the (regular) use of a computer**. Filling in this survey will take approximately 15 minutes.

The results of this survey will be anonymized when used in my thesis. In case of questions or remarks you can contact me by sending an e-mail to k.v.m.meeuwisse@student.tudelft.nl

Thanks in advance for participating!

Kind regards,

Kirsten Meeuwisse
Master student TU Delft

1 / 9 11%

Next

Powered by SurveyMonkey

See how easy it is to create a survey.

Questions about the current security measures at your work

1. What requirement is there for the length of your log-in password for your work computer?

It is possible to choose multiple answers

- [ ] No requirements, so every password is allowed
- [ ] Password must contain minimal 8 characters e.g. "hiwelcome"
- [ ] Password must contain an uppercase letter e.g. "hiWelcome"
- [ ] Password must contain a numeric character e.g. "hiwelcome1"
- [ ] Password must contain a special character e.g. "hi*welcome"
- [ ] I don't know
- [ ] Other, namely...

2. How often do you have to change your password to log in on your work computer?

- ( ) Never
- ( ) Once a year
- ( ) Once every six months
- ( ) Once a quarter
- ( ) Once a month
- ( ) I don't know
- ( ) Other, namely...

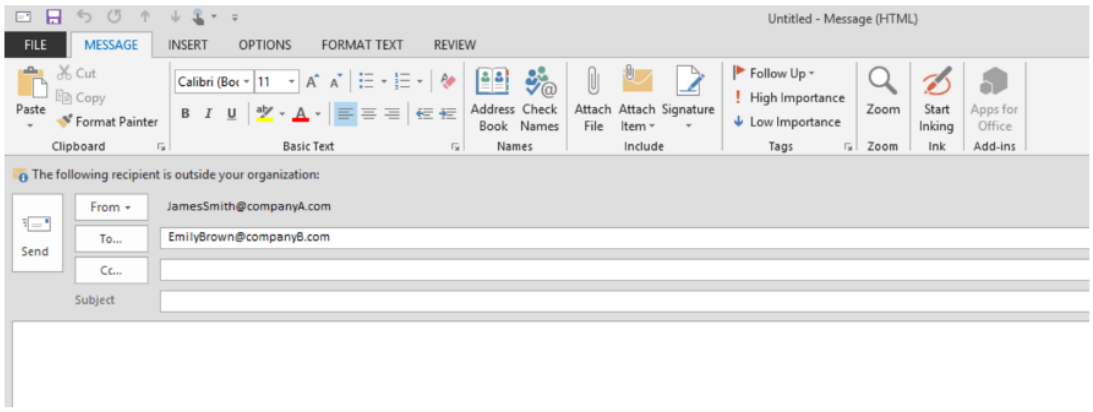
3. Are there restrictions about which browser (e.g. Internet Explorer, Google Chrome, Firefox, Safari) you should use when surfing the internet at your work?

- ◯ No restrictions: every browser allowed
- ◯ Yes, 1 obligatory browser: My employer obligates me to use 1 specific browser
- ◯ I don't know
- ◯ Other, namely...

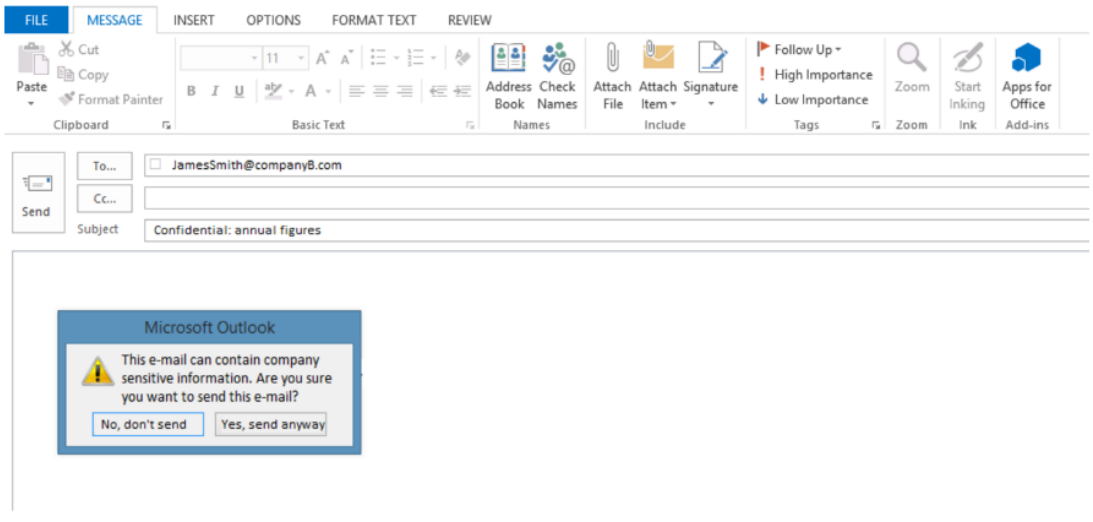
4. Are there restrictions at your work when sending an e-mail to someone outside the company?

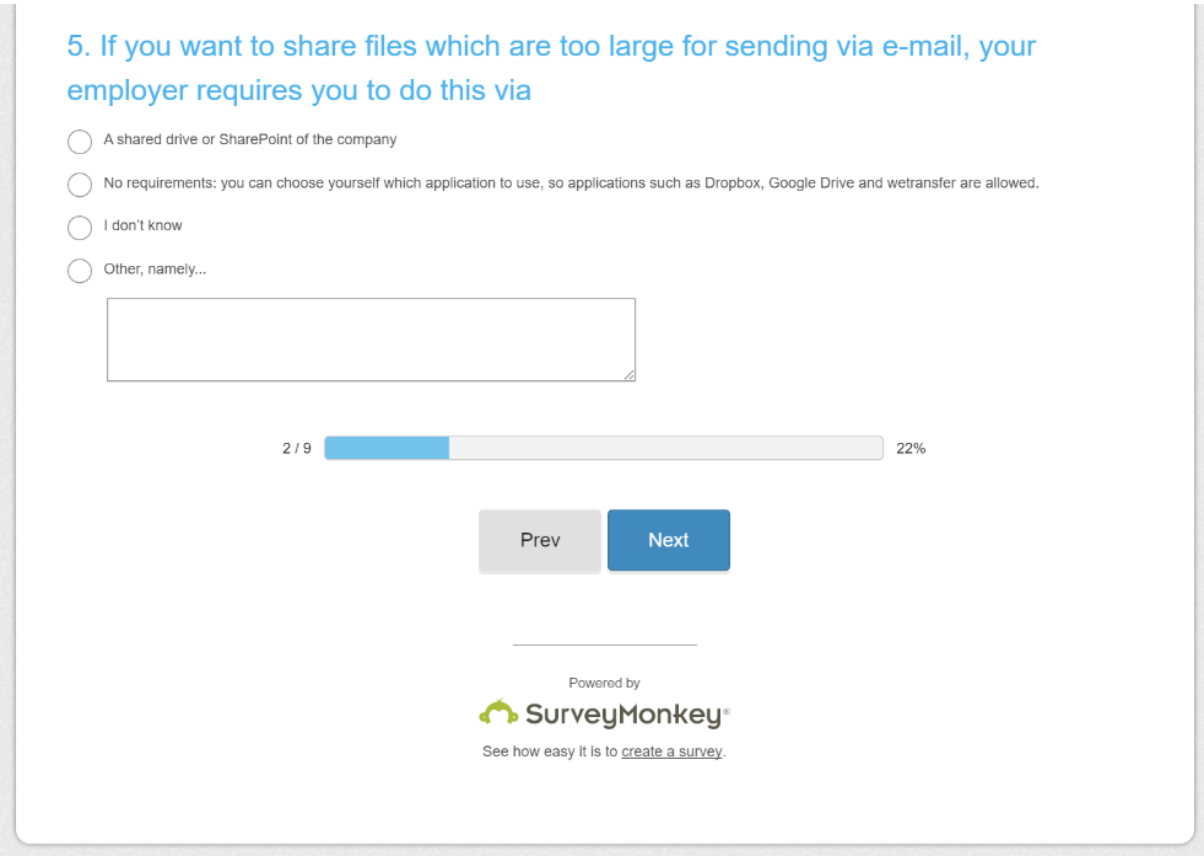
- ◯ No restrictions: I can send an e-mail to everyone
- ◯ I receive a warning message with the e-mail (see image 4B below)
- ◯ I receive a pop-up message when I use certain company sensitive words in my e-mail, such as "confidential", "secret" and "private" (see image 4C below)
- ◯ I don't know
- ◯ Other, namely...

4B: Warning message



4C: Pop-up message




5. If you want to share files which are too large for sending via e-mail, your employer requires you to do this via
A shared drive or SharePoint of the company
No requirements: you can choose yourself which application to use, so applications such as Dropbox, Google Drive and wetransfer are allowed.
I don't know
Other, namely...
2 / 9
22%
Prev
Next
Powered by
SurveyMonkey
See how easy it is to create a survey.

Explanation about the survey

This part of the survey consists of 3 pages which show three alternatives on each page. Each alternative consists of a combination of multiple security measures. See the image below for an example. On each row in the left table a topic is mentioned, for example: password length. In the other three tables ('Package A', 'Package B', 'Package C') the specific information security measure for this topic is mentioned.

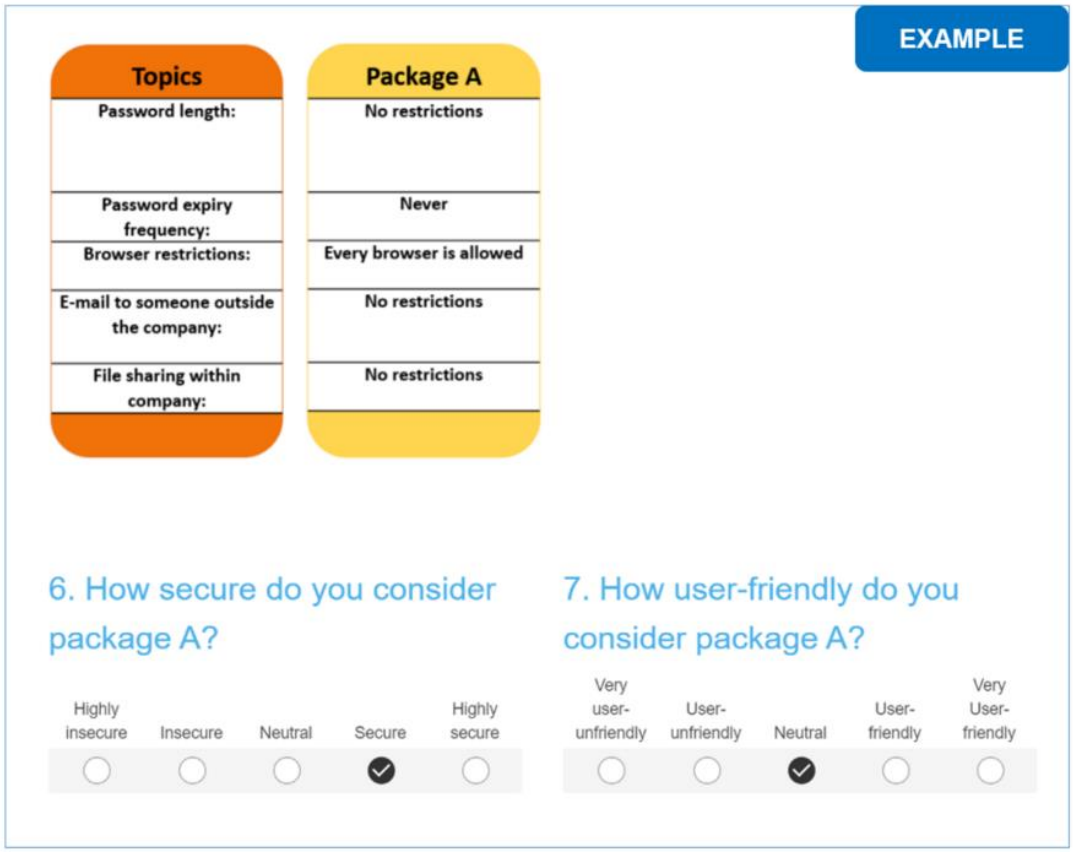
EXAMPLE

Topics	Package A	Package B	Package C
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	Every browser is allowed
E-mail to someone outside the company:	No restrictions	Warning message with e-mail	Pop-up message with e-mail which contains confidential words
File sharing within company:	No restrictions	Via corporate shared drive	No restrictions

Example question part 1

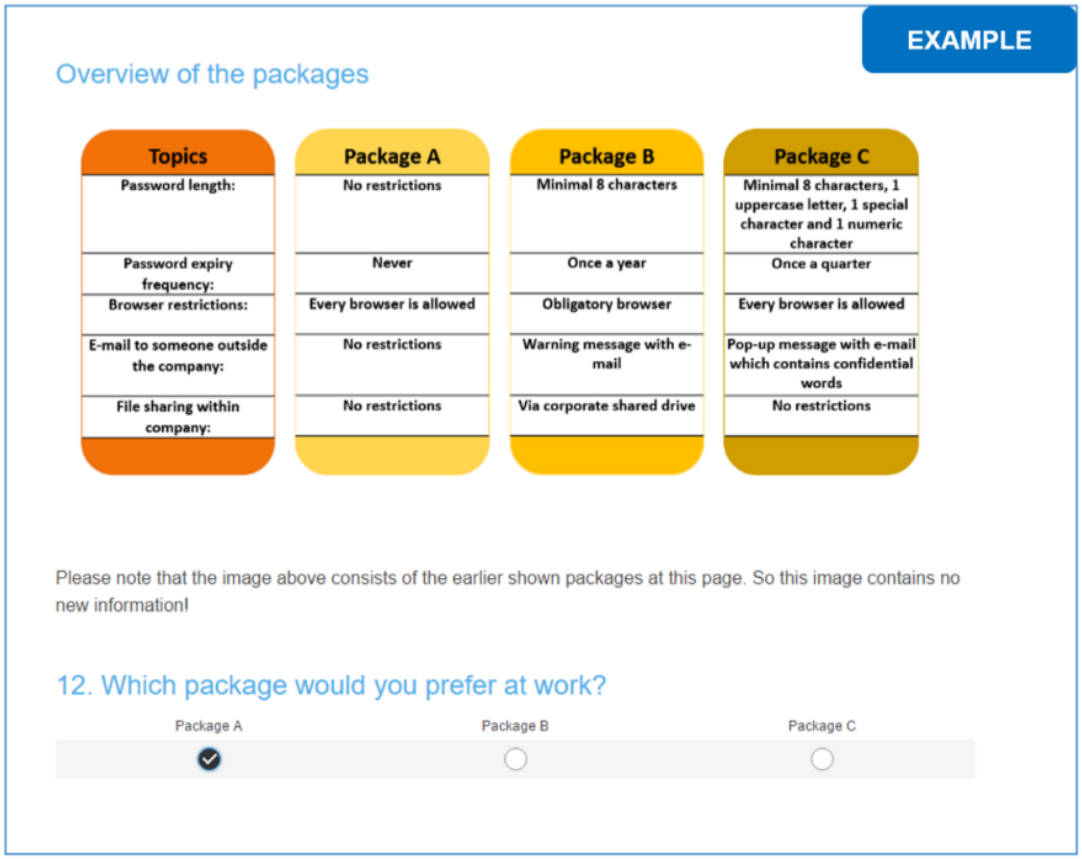
Firstly, two questions will be asked about each package:

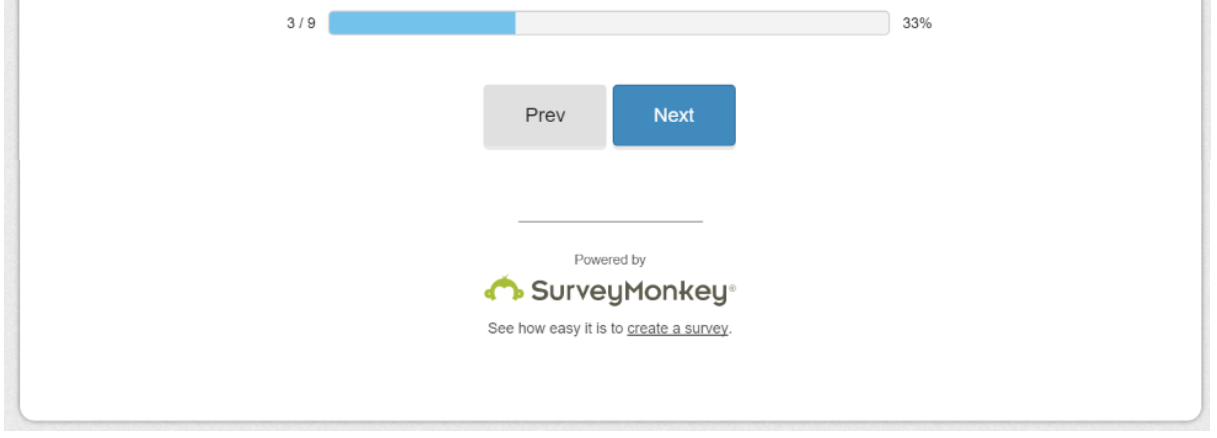
1. How secure do you consider this package? You can choose between the following 5 answers: highly insecure, insecure, neutral, secure, highly secure. The example below shows that someone considers package A as secure.
2. How user-friendly do you consider this package? You can choose between the following 5 answers: very user-unfriendly, user-unfriendly, neutral, user-friendly, very user-friendly. The example below shows that someone considers package A as neutral.



Example question part 2

At the bottom of each page you will be asked which of the three shown packages you would prefer at work: package A, package B, or package C. Note that this covers the same packages that you have valued on security and user-friendliness in the questions before. The image with the overview of the three packages is just a summary of what you have seen before and does not contain any new information. The example below shows that someone prefers package A.





Package page 1 out of 3

Topics	Package A
Password length:	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Once a quarter
Browser restrictions:	Every browser is allowed
E-mail to someone outside the company:	Warning message with e-mail
File sharing within company:	Via corporate shared drive

6. How secure do you consider package A?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

7. How user-friendly do you consider package A?

Very user-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics	Package B
Password length:	Minimal 8 characters
Password expiry frequency:	Once a year
Browser restrictions:	Obligatory browser
E-mail to someone outside the company:	Pop-up message with e-mail which contains confidential words
File sharing within company:	Via corporate shared drive

8. How secure do you consider package B?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

9. How user-friendly do you consider package B?

Very User-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics
Password length:
Password expiry frequency:
Browser restrictions:
E-mail to someone outside the company:
File sharing within company:

Package C
Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Never
Obligatory browser
No restrictions
No restrictions

10. How secure do you consider package C?

Highly insecure | Insecure | Neutral | Secure | Highly secure

11. How user-friendly do you consider package C?

Very user-unfriendly | User-unfriendly | Neutral | User-friendly | Very User-friendly

Overview of the packages

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

Please note that the image above consists of the earlier shown packages at this page. So this image contains no new information!

12. Which package would you prefer at work?

Package A | Package B | Package C

Package page 2 out of 3

Topics	Package D
Password length:	No restrictions
Password expiry frequency:	Once a year
Browser restrictions:	Obligatory browser
E-mail to someone outside the company:	No restrictions
File sharing within company:	Via corporate shared drive

13. How secure do you consider package D?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

14. How user-friendly do you consider package D?

Very user-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics	Package E
Password length:	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Never
Browser restrictions:	Every browser is allowed
E-mail to someone outside the company:	Pop-up message with e-mail which contains confidential words
File sharing within company:	No restrictions

15. How secure do you consider package E?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

16. How user-friendly do you consider package E?

Very user-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics
Password length:
Password expiry frequency:
Browser restrictions:
E-mail to someone outside the company:
File sharing within company:

Package F
Minimal 8 characters
Once a quarter
Obligatory browser
Warning message with e-mail
Via corporate shared drive

17. How secure do you consider package F?

Highly insecure | Insecure | Neutral | Secure | Highly secure

18. How user-friendly do you consider package F?

Very user-unfriendly | User-unfriendly | Neutral | User-friendly | Very User-friendly

Overview of the packages

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

Please note that the image above consists of the earlier shown packages at this page. So this image contains no new information!

19. Which package would you prefer at work?

Package D | Package E | Package F

Package page 3 out of 3

Topics	Package G
Password length:	Minimal 8 characters
Password expiry frequency:	Never
Browser restrictions:	Every browser is allowed
E-mail to someone outside the company:	Warning message with e-mail
File sharing within company:	No restrictions

20. How secure do you consider package G?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

21. How user-friendly do you consider package G?

Very user-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics	Package H
Password length:	No restrictions
Password expiry frequency:	Once a quarter
Browser restrictions:	Obligatory browser
E-mail to someone outside the company:	No restrictions
File sharing within company:	No restrictions

22. How secure do you consider package H?

Highly insecure	Insecure	Neutral	Secure	Highly secure
○	○	○	○	○

23. How user-friendly do you consider package H?

Very user-unfriendly	User-unfriendly	Neutral	User-friendly	Very User-friendly
○	○	○	○	○

Topics	Package I
Password length:	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character
Password expiry frequency:	Once a year
Browser restrictions:	Every browser is allowed
E-mail to someone outside the company:	Pop-up message with e-mail which contains confidential words
File sharing within company:	Via corporate shared drive

24. How secure do you consider package I?

Highly insecure | Insecure | Neutral | Secure | Highly secure

25. How user-friendly do you consider package I?

Very user-unfriendly | User-unfriendly | Neutral | User-friendly | Very User-friendly

Overview of the packages

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

Please note that the image above consists of the earlier shown packages at this page. So this image contains no new information!

26. Which package would you prefer at work?

Package G | Package H | Package I

Personal characteristics

27. What is your gender?

- ◯ Male
- ◯ Female

28. What is your nationality?

- ◯ Dutch
- ◯ Other, namely...

29. What is your birth year?

30. What is the highest degree or level of education you have completed?

- ◯ No education completed
- ◯ Primary school
- ◯ Secondary school
- ◯ Post-secondary college
- ◯ Bachelor's degree
- ◯ Master's degree
- ◯ PhD
- ◯ Other, namely...

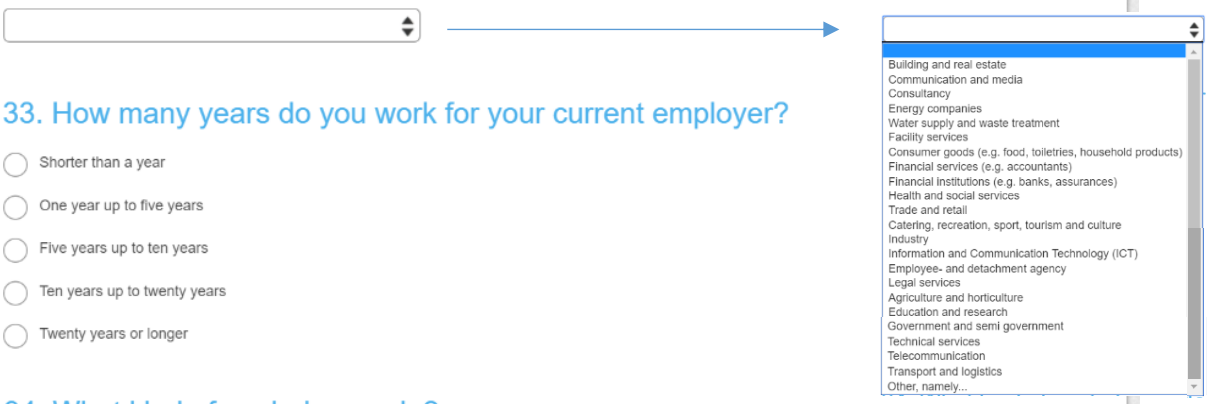
31. How many employees does your company/organisation have?

If the company/organisation has internationally based sites, select the global total number of employees.

- ◯ Less than 10
- ◯ 10 - 49
- ◯ 50 - 249
- ◯ 250 - 499
- ◯ 500 - 999
- ◯ 1000 - 9999
- ◯ 10000 or more

32. In which sector does your company/organisation mostly operate?

If multiple answers are possible, choose the most appropriate one



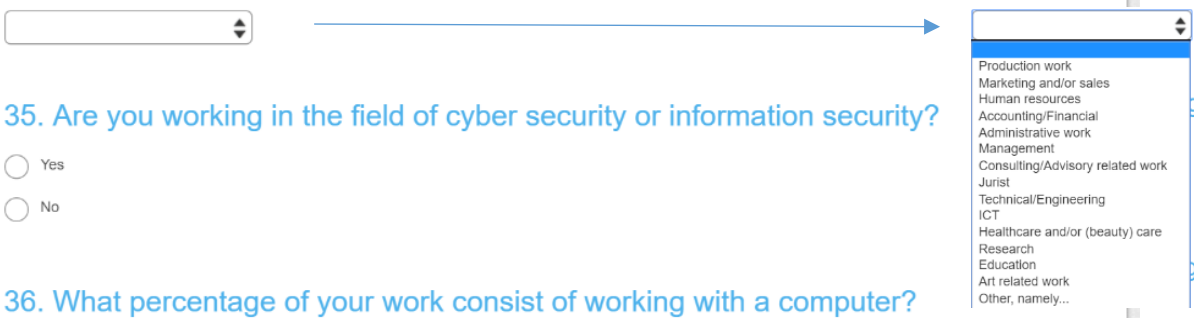
33. How many years do you work for your current employer?

- ◯ Shorter than a year
- ◯ One year up to five years
- ◯ Five years up to ten years
- ◯ Ten years up to twenty years
- ◯ Twenty years or longer

34. What kind of work do you do?

If multiple answers are possible, choose the most appropriate one.

Difference with question 32 is that that question focuses on the general company/organisation and this question focuses on your own tasks inside this company/organisation.



35. Are you working in the field of cyber security or information security?

- ◯ Yes
- ◯ No

36. What percentage of your work consist of working with a computer?

- ◯ 0-25%
- ◯ 26-50%
- ◯ 51-75%
- ◯ 76-100%

37. How do you consider your computer knowledge?

Very limited	Limited	Medium	Good	Very good
◯	◯	◯	◯	◯

38. Which digital security measure hinders you most at work?

39. How sensitive do you think the information you work with is for outsiders?

Not sensitive	A little sensitive	Sensitive	Very sensitive
○	○	○	○

40. How aware are you of online risks?

Totally unaware	Unaware	Neutral	Aware	Very aware
○	○	○	○	○

41. Are you or do you know someone who has been victim of cybercrime (e.g. hacking, digital bank fraud, phishing)?

- ☐ Yes, myself
- ☐ Yes, someone else
- ☐ No

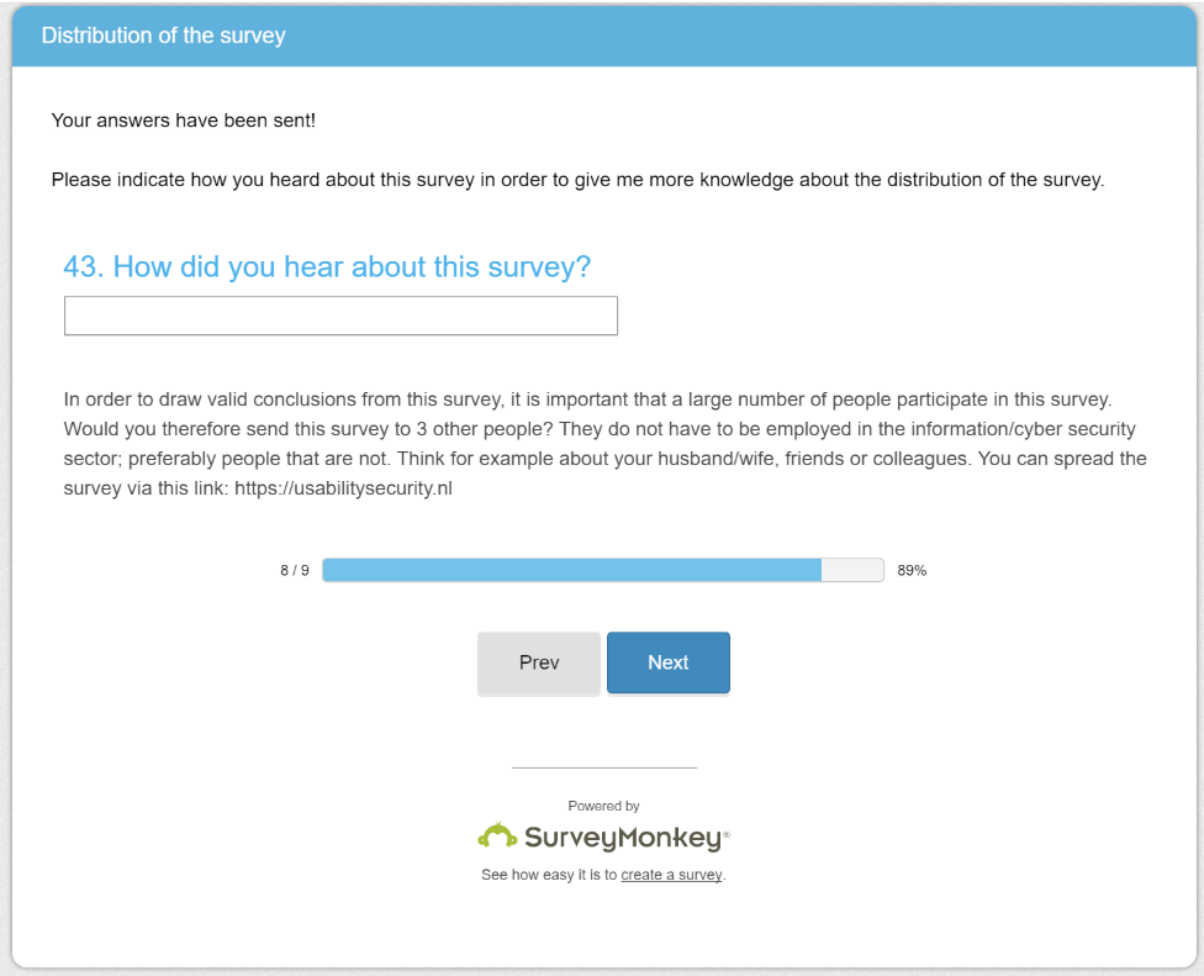
42. Did you ever have security awareness training*?

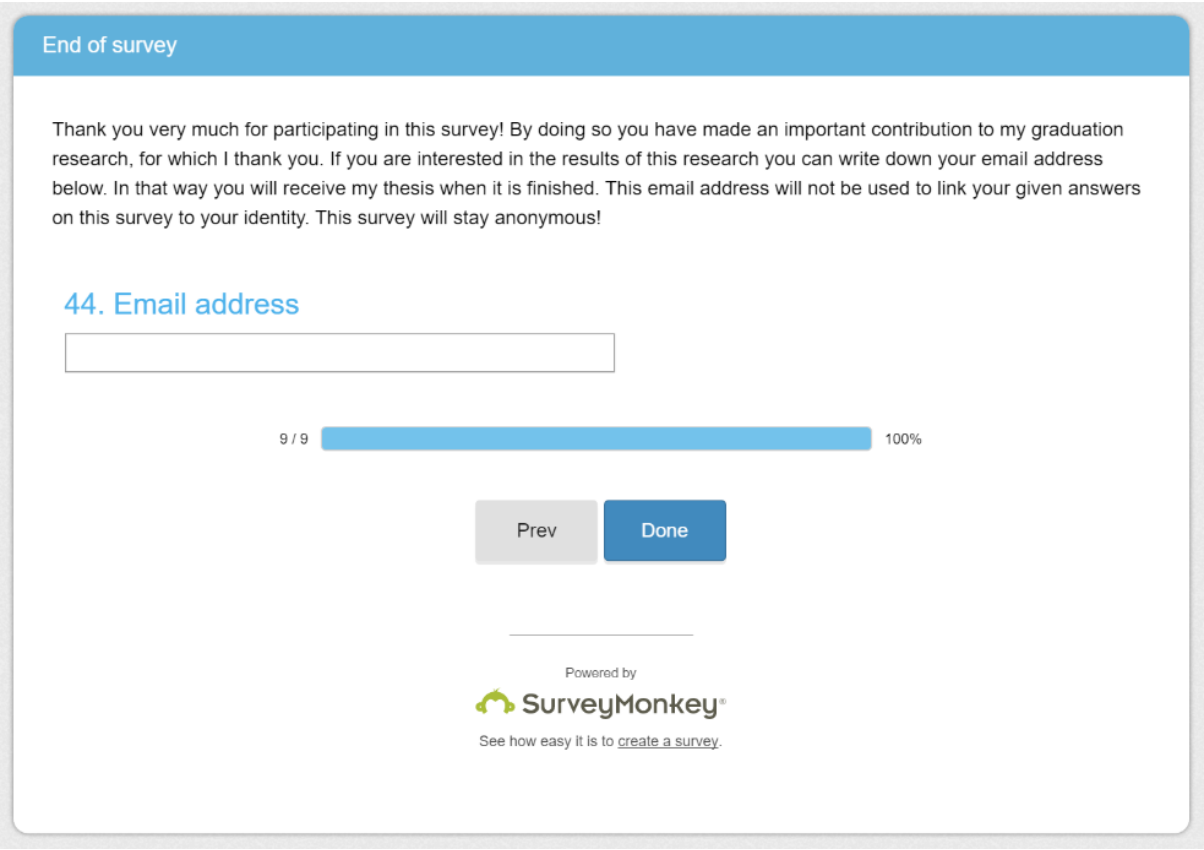
*In a security awareness training you will be taught about the dangers of cyberattacks and you will receive tips about how you can secure data/information the best against such attacks

- ○ Yes, once
- ○ Yes, multiple times
- ○ No

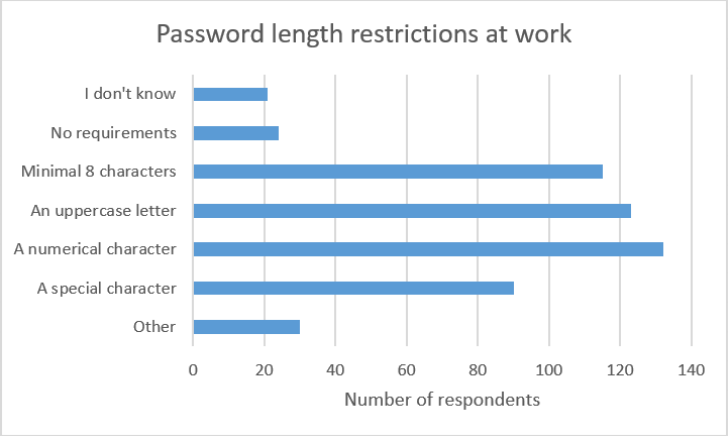
7 / 9 78%

Prev Next

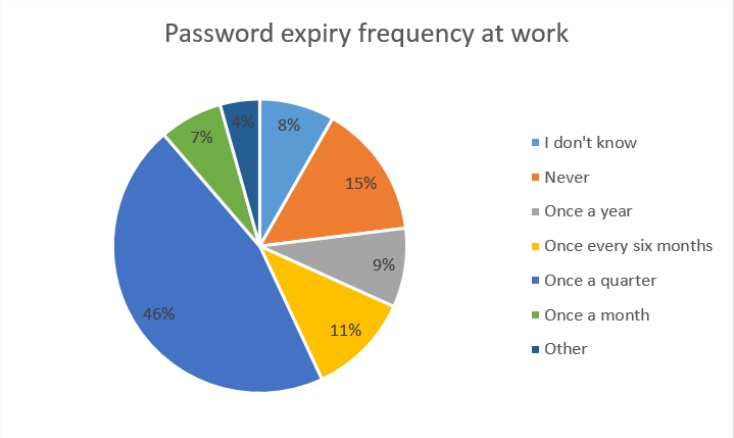

Distribution of the survey
Your answers have been sent!
Please indicate how you heard about this survey in order to give me more knowledge about the distribution of the survey.
43. How did you hear about this survey?
In order to draw valid conclusions from this survey, it is important that a large number of people participate in this survey. Would you therefore send this survey to 3 other people? They do not have to be employed in the information/cyber security sector; preferably people that are not. Think for example about your husband/wife, friends or colleagues. You can spread the survey via this link: https://usabilitysecurity.nl
8 / 9
89%
Prev
Next
Powered by
SurveyMonkey
See how easy it is to create a survey.

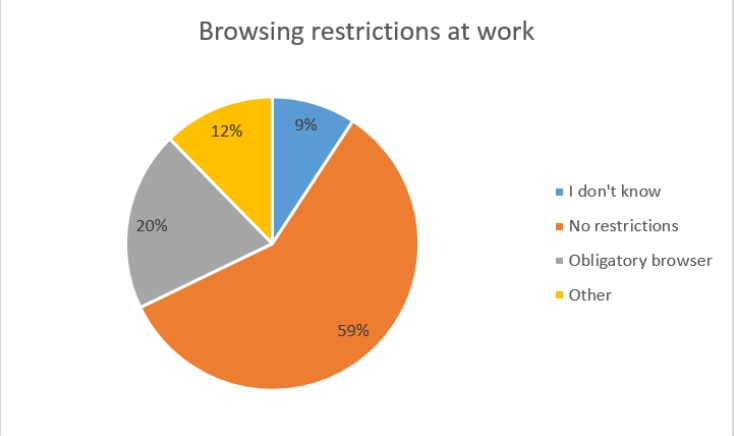

End of survey
Thank you very much for participating in this survey! By doing so you have made an important contribution to my graduation research, for which I thank you. If you are interested in the results of this research you can write down your email address below. In that way you will receive my thesis when it is finished. This email address will not be used to link your given answers on this survey to your identity. This survey will stay anonymous!
44. Email address
9 / 9
100%
Prev
Done
Powered by
SurveyMonkey
See how easy it is to create a survey.

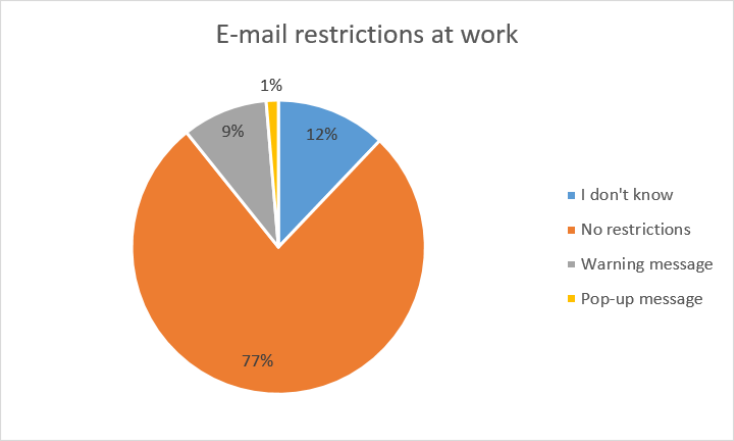
Appendix E: Current security measures at work

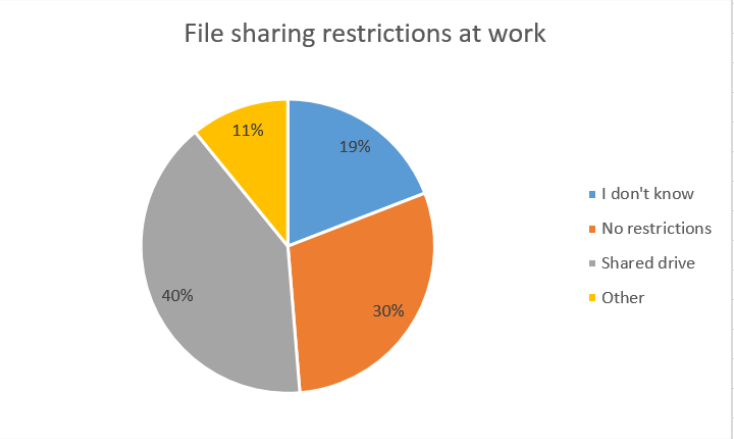


The distribution in current password length restrictions at work are not visualised by percentages, but by the number of respondents. Since for this technical security measure multiple restrictions can be implemented at the same time.

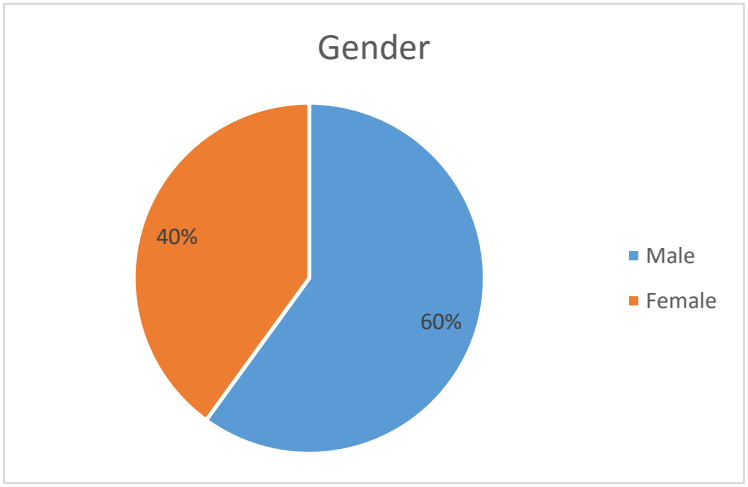


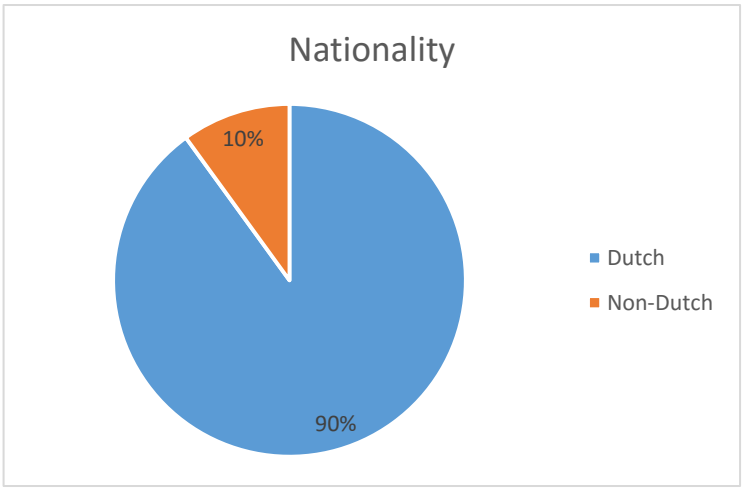


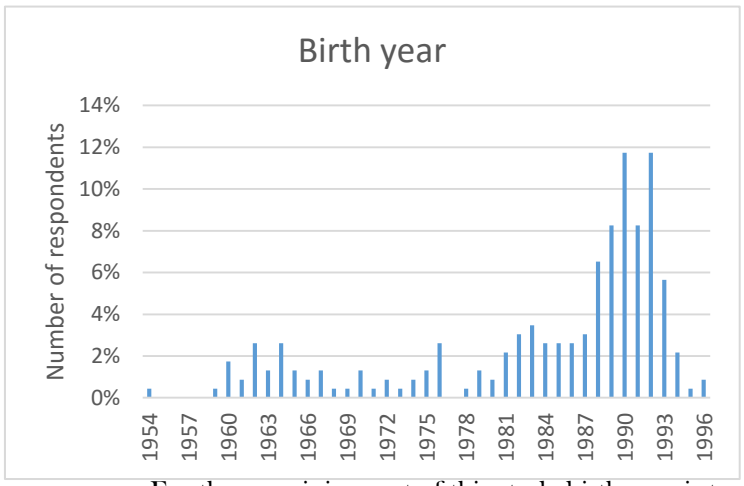


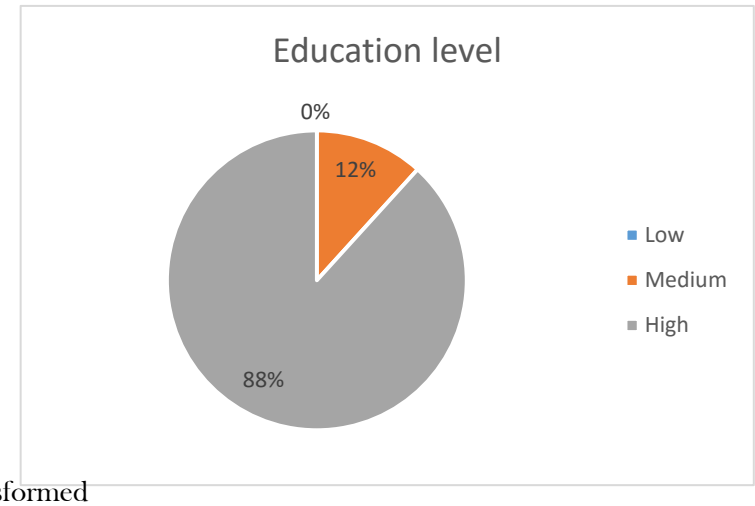


Appendix F: Personal characteristics of respondents

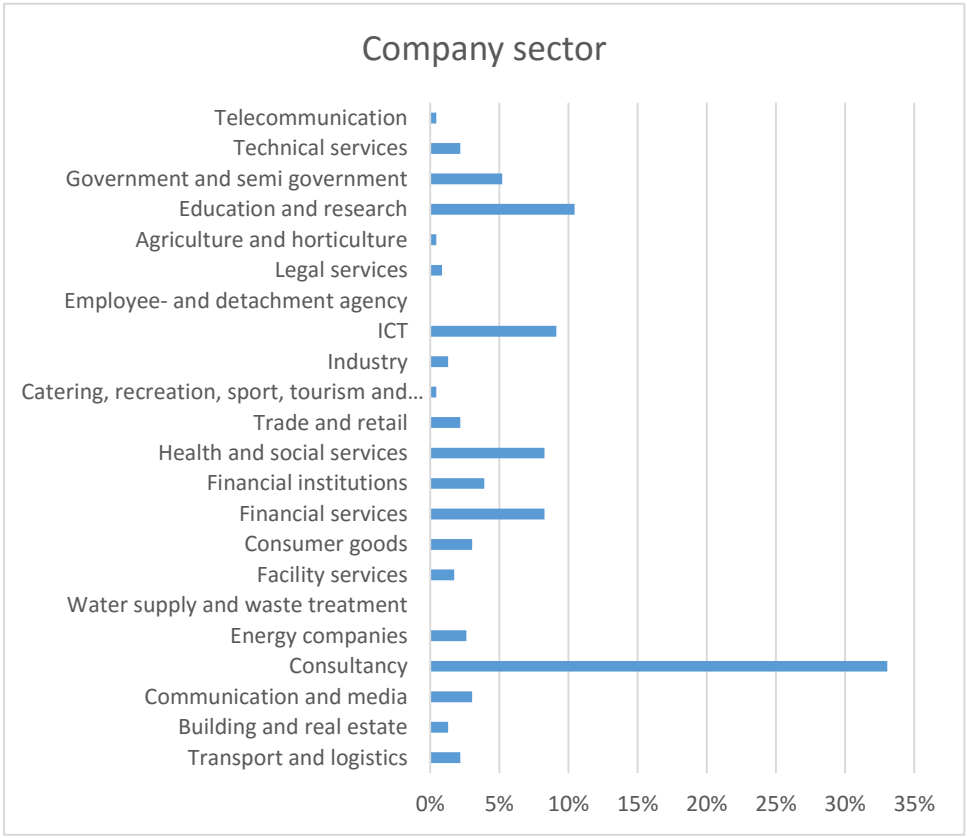


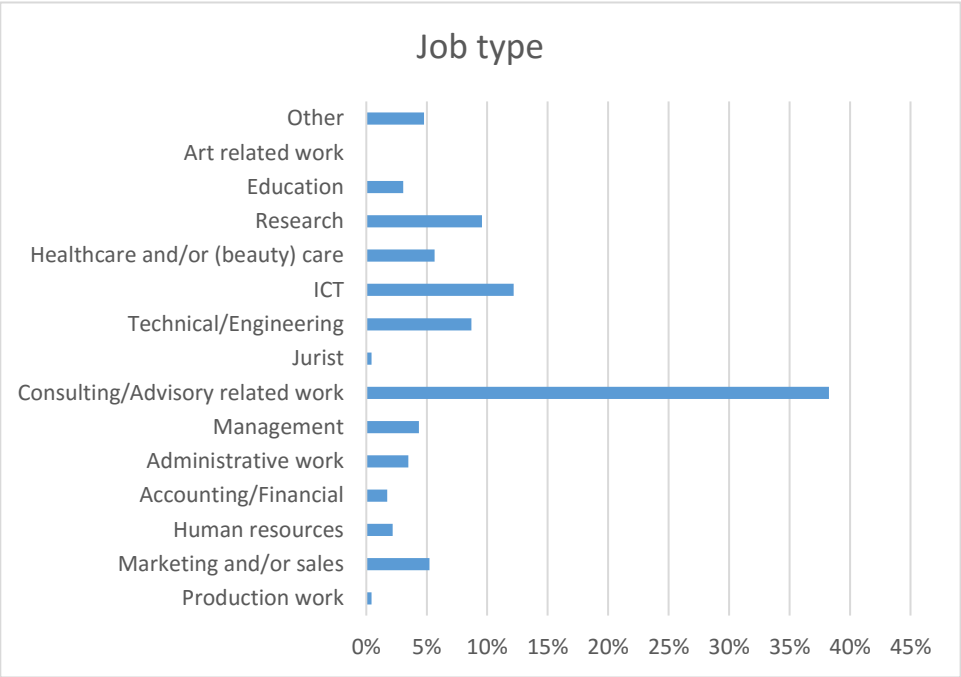


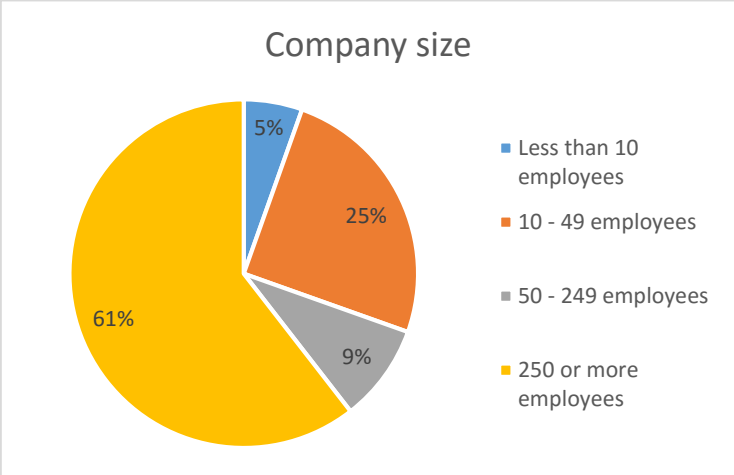


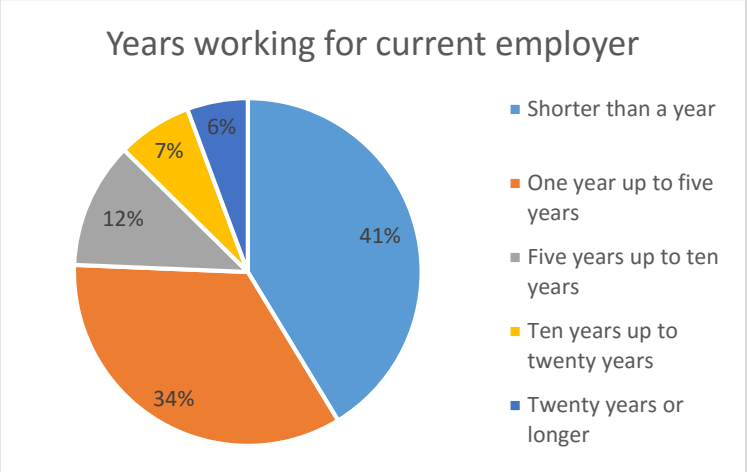


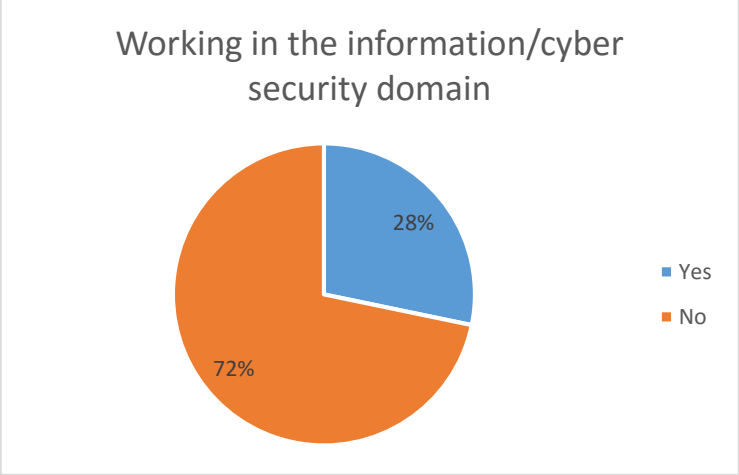
For the remaining part of this study birth year is transformed into age. Assumed is that people already had their birthday in 2016.

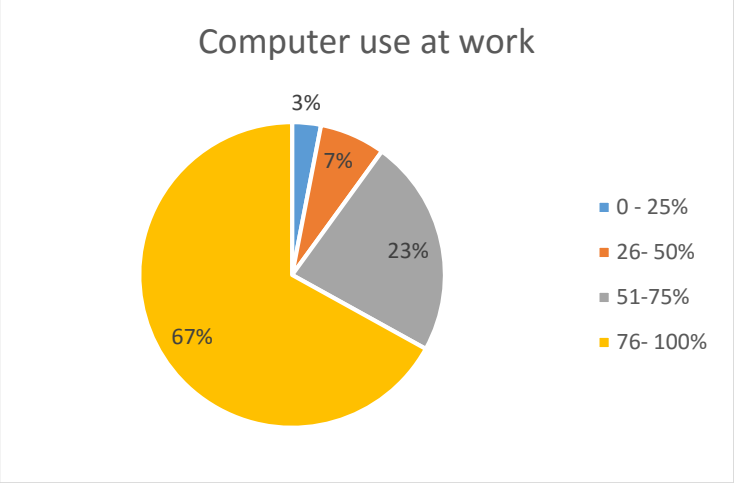


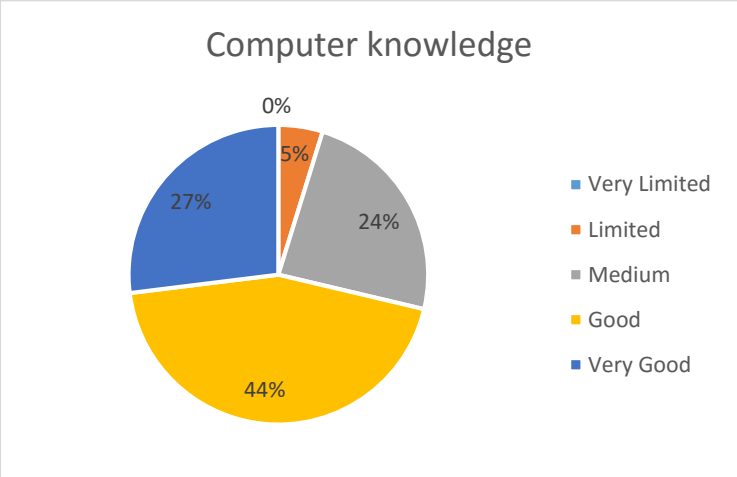

Job type
Other
Art related work
Education
Research
Healthcare and/or (beauty) care
ICT
Technical/Engineering
Jurist
Consulting/Advisory related work
Management
Administrative work
Accounting/Financial
Human resources
Marketing and/or sales
Production work
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%

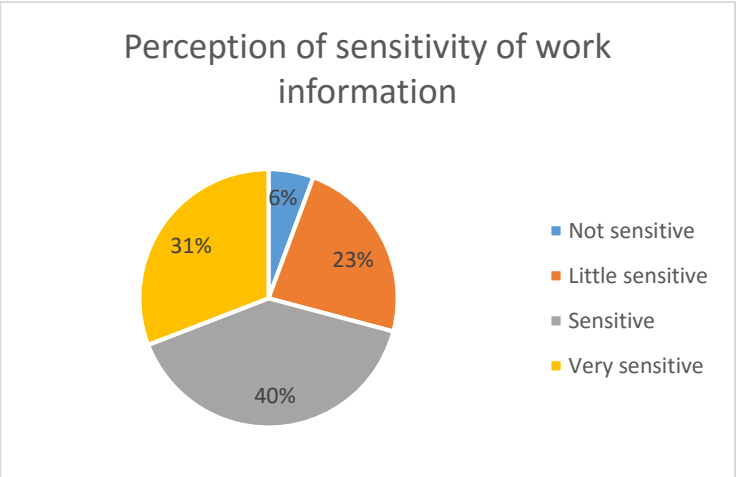

Company size
5%
25%
9%
61%
Less than 10 employees
10 - 49 employees
50 - 249 employees
250 or more employees

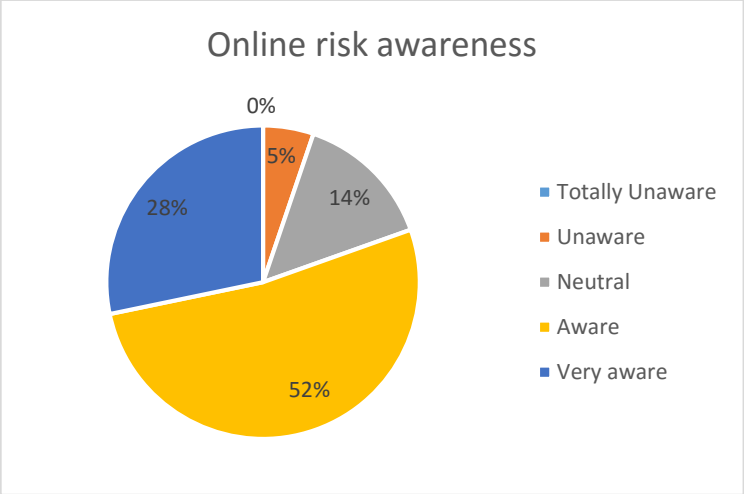

Years working for current employer
6%
7%
12%
41%
34%
Shorter than a year
One year up to five years
Five years up to ten years
Ten years up to twenty years
Twenty years or longer

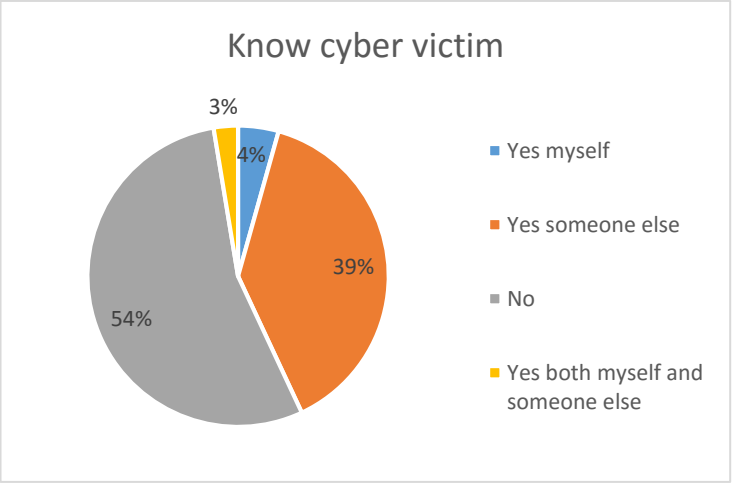

Working in the information/cyber security domain
28%
72%
Yes
No

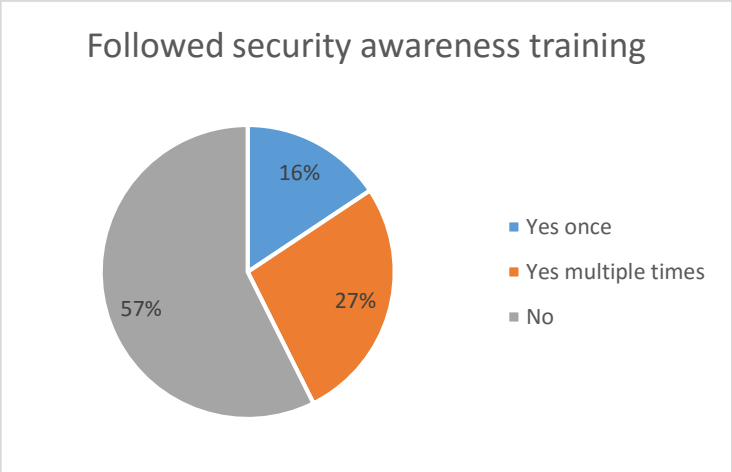

Computer use at work
3%
7%
23%
67%
0 - 25%
26- 50%
51-75%
76- 100%











For the personal characteristics nationally and education level it was not possible to estimate the impact these characteristic have on the perceptions and the trade-off between the importance of perceived usability and security, since the distribution between the categories was scares. For example, almost all the respondents in this survey belong to the category high education level. The number of respondents belonging to the other categories was too small (smaller than 30).

Appendix G: Influence of personal characteristics on perceptions

G.1 Influence of personal characteristics on the perceived level of usability

Attribute	Attribute level	Effect	T-value
	Constant	3.47	31.14
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	-0.06	-1.96
	Minimal 8 characters	0.06	2.07
	Password length no restrictions	0.00	*
Password expiry frequency	Once a quarter	-0.44	-7.63
	Once a year	0.12	4.53
	Never	0.32	*
Browsing restrictions	Obligatory browser	-0.06	0.84
	Every browser is allowed	0.06	*
E-mail restrictions	Pop-up message with e-mail which contains confidential words	-0.14	-5.01
	Warning message with e-mail	-0.07	-2.60
	No e-mail restrictions	0.21	*
File sharing	Via corporate shared drive	-0.08	-3.88
	No restrictions	0.08	*
Age		0.01	2.06
Working Years	Shorter than a year	0.10	*
	One year up to five years	0.00	*
	5 years or longer	-0.10	-3.46
Working in information/cyber security domain	Yes	-0.04	-1.98
	No	0.04	
Computer knowledge**		-0.06	-2.36
	Interaction		
	Perceived computer knowledge** with browser restrictions	-0.11	-4.86
	Perceived sensitivity of work information*** with password expiry of once a quarter	0.10	3.97
	Cyber victim: yes with browser restrictions	0.05	2.69
	Cyber victim: no with browser restrictions	-0.05	

* 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.

** 0=very limited, 1= limited, 2=medium, 3=good, 4=very good

*** 0=not sensitive, 1=little sensitive, 2=sensitive, 3=very sensitive

G.2 Influence of personal characteristics on the perceived level of security

Variable	Level	Effect	T-value
	Constant	3.43	41.91
Password length	Minimal 8 characters, 1 uppercase letter, 1 special character and 1 numeric character	0.58	20.76
	Minimal 8 characters	0.02	0.74
	Password length no restrictions	-0.60	*
Password expiry frequency	Once a quarter	0.39	14.18
	Once a year	0.02	0.84
	Never	-0.41	*
Browsing restrictions	Obligatory browser	0.04	1.88
	Every browser is allowed	-0.04	*
E-mail restrictions	Pop-up message with e-mail which contains confidential words	0.20	7.69
	Warning message with e-mail	0.14	5.39
	No e-mail restrictions	-0.34	*
File sharing	Via corporate shared drive	0.27	13.98
	No restrictions	-0.27	*
Company size	Less than 250 employees	0.05	*
	250 or more employees	-0.05	-2.48
Perceived sensitivity of work information**		-0.10	-4.25
Risk Awareness***		-0.11	-4.47
Cyber Victim	Yes	-0.04	-2.04
	No	0.04	*
Followed security awareness training	No	0.10	*
	Yes, once	0.00	*
	Yes, multiple times	-0.10	-4.36
	Interaction		
	Company size: 250 employees or more with password expiry once a quarter	0.06	2.42
	Company size: less than 250 employees with password expiry once a quarter	-0.06	2.42

* 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.

** 0=not sensitive, 1=little sensitive, 2=sensitive, 3=very sensitive

*** 0=totally unaware, 1=unaware, 2=neutral, 3=aware, 4=very aware

Appendix H: RUM and µRRM choice models

H.1 Choice model based on perceived security and usability

	RUM		µRRM	
Variables	**Beta**	**t-value**	**Beta**	**t-value**
Security	1.33	14.74	0.79	14.72
Usability	1.06	11.58	0.68	11.58
mu			323	0.59

H.2 Choice model based on technical security measures

	RUM		µRRM	
Indicator variables	**Beta**	**t-value**	**Beta**	**t-value**
PLMM	0.89	11.28	0.59	11.28
PLM	-0.02	-0.23	-0.01	-0.23
PEFOQ	0.31	4.78	0.21	4.78
PEFOY	0.11	1.46	0.07	1.46
BR	-0.35	-7.23	-0.23	-7.23
ERPM	0.02	0.21	0.01	0.21
ERWM	0.09	1.35	0.06	1.35
FS	0.19	3.86	0.13	3.86
mu			172	1.03