People ignore design that ignores people

Understanding the impact of security training on the security behaviour of employees within an organisational context

Master Thesis CoSEM

B.A.P van den Kieboom

Delft University of Technology

TU Delft

People ignore design that ignores people

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements of the degree of

MASTER OF SCIENCE

in **Complex System Engineering and Management**

at the Faculty of Technology, Policy and Management

by

B.A.P van den Kieboom

4451937

To be defended online on the 16th of August 2021

Graduation Committee

Chair:	Prof. dr. M.J.G. van Eeten, Section Governance of Cybersecurity
First supervisor:	S. Parkin, Section Governance of Cybersecurity
Second Supervisor:	Dr. F.W. Guldenmund, Section Safety Science & Security
External Supervisor:	Ir. R.D. Boomsma, Cybersecurity Consultant

TU Delft

Preface

In front of you lies the Master Thesis report on 'Understanding the impact of security training on the security behaviour of employees within an organisational context'. The foundation of this research is a combination of semi-structured interviews and a survey that was distributed amongst employees of several departments of a global Financial Services Organisation. The report has been written as part of the completion of the Master Complex System Engineering and Management at the Technical University of Delft. I have been engaged in researching this topic from mid March until end July 2021.

Personally, I have always been interested in technology and the aspects surrounding it. My family would always make fun of my lack of general knowledge regarding history or geography, but the moment I would start about the Internet and cyberspace they would lose me in seconds. When I started at the Technical University of Delft, this interest only grew. For the completion of my bachelor, I wrote my thesis on open IoT systems of Dutch hospitals and the implications to quality of care together with the privacy of personal medical data. This opened my eyes to the lack of security in organisations that fulfill an important role in society. More importantly the risks that came to light when handling sensitive data and the of impact of these risks on society.

After completing my Bachelor System Engineering Policy Analysis and Management, I decided to start the Master Complex System Engineering and Management. The choice for this particular Master was mainly based on the Master having a focus on both technical as social aspects of infrastructures. Subsequently, this study allows students to solve problems within complex socio-technical systems. Within this study, I was provided with the opportunity to follow the track Information and Communication, which stimulated my interests regarding ICT even more. The last course I took gave me a quick insight into cybersecurity risk management and a guest lecture of EY got me curious. The view I have created on cybersecurity in the past several years is: if this security is not in place, we cannot make use of all the amazing possibilities that the Internet and connected devices have to offer. Someone has to protect everything that is happening in a world that is changing faster than we can keep up with. Helping companies protect their informational assets is something I would love to keep doing in the future and that's why writing my thesis within the cybersecurity team of a global operating company is a perfect begin to my future.

I would like to thank Simon Parkin, who was involved in my regular meetings and helped me with designing and structuring my thesis research. Your enthusiasm for my thesis research has motivated me throughout this process. Next to that, I would like to thank my supervisors Michel van Eeten and Frank Guldenmund, for guiding me and asking me critical questions to improve my thesis project. Also, a big appreciation to my supervisor of the company, who has helped me in getting to know the company and the activities the team is engaged in on a daily basis. Together with supervising me, reviewing my work and helping me wherever I needed.

B.A.P van den Kieboom
Delft, July 2021

Executive Summary

Research shows that most of the security issues arise through human shortcomings, instead of technical issues (Abawajy, 2014). Therefore, users of information systems have to become more security aware. The reasonable solution to these human shortcomings was to provide users with policies that tell them what to do and have the technical systems behind them for support. However, within an organisational environment, information technology is increasingly needed for the completion of work activities. This creates problems for users to follow policies that require an excessive amount of effort and introduces human errors. Mainly caused by employees feeling like the amount of effort is unreasonable and not fitting into their daily work activities (Kirlappos, Parkin, & Sasse, 2014). Subsequently, cyber attacks are mostly caused by liabilities created due to the human error and social engineering (Schneier, 2015). Therefore, it is of importance for organisations to find a way to manage security in an effective manner, by taking into account the interactions between the social and physical environment. Accordingly, there is a possibility that employees find complying to security rules and procedures to have higher costs than benefits to their company. Finally, it is fundamental to find aspects where the business and security processes clash, in order to improve the security and productivity of the organisation (Beautement, Becker, Parkin, Krol, & Sasse, 2016).

To address this issue, this research focuses on the security training provided to employees within an organisational context and the impact of this training on their security behaviour. To get a view of employee's their perceptions regarding the security training, their perceived effectiveness, impact on their productivity, their perceived security knowledge and their security behaviour, a survey has been distributed amongst different departments of the organisation. Two interviews were conducted, with the information security awareness team and the learning team of the company. This not only provided the possibility to see how the security training is perceived from different perspectives, but the interview results also provided a basis for the quantitative part of the research. Combining qualitative and quantitative research methods, will allow for the researcher to provide a broader and deeper understanding of the phenomenon and result in more confidence in the results drawn from the research.

Further, the analysis consists of two types of factor analysis to validate the constructs and test reliability of the variables. Next to that, a structural equation model including the reliable and validated constructs was used to analyse dependencies and test the hypotheses stated in the literature review. The reliability tests excluded some variables and the structural equation model would not allow for questions to be included that were not measured on a Likert scale. Therefore, these items have been analysed separately, by performing a regression analysis. The constructs included in the survey are demographics, perceived security training, perceived effectiveness, perceived security knowledge, perceived impact on productivity and self-stated employee security behaviour. The results to these statements have been analysed, in order to get an understanding of the vision of employees on the current security training of their company and how this interacts with their security behaviour.

This resulted in the conclusion that, the strongest two interactions between constructs are, first the interaction between perceived security training and the security knowledge of employees. Second, the interaction between the perceptions on security training and the perceived effectiveness of employees. Where a positive perception of security training entails, being easy to put into practice, acting as a reminder, being useful and not burdensome to complete. This positively effects (as expected) the feeling that an employee can work securely and can manage unexpected situations. Also, these perceptions on security training positively effect the knowledge of employees regarding security and mainly the policy knowledge. The policies are translated into the security training modules. This interaction indicates that employees who perceive security training positively are more likely to take in the information provided and therefore have more policy knowledge. Another strong positive relationship resulted between security knowledge and the security behaviour of employees. Where more knowledge of threats, risks and policies, emerged into better self-stated security behaviour.

Also, all employees generally view the security training either in a positive way or in a negative way. This was measured by the question on security training characteristics, where respondents could select the top three that applied to their security training. The only combination between a positive and a negative characteristic, that was chosen often by respondents, is hard to find time for and informative. Tailoring back to the results of the interview, that indicates that the company structure won't allow for security training to be completed within working hours without this having an impact on the productivity of employees. This is in line with employees finding it hard to find time to complete the training. However, the interviews also explain security training to be perceived as informative and easy to understand. The information security awareness team that creates the security training, spends a lot of time and effort in developing this security training and creates training for all employees of the organisation. Therefore, the information in the training is likely to be informative, but also easy to comprehend since the content is created for all employees. On the other hand, employees perceive security training often to be boring, repetitive and general. Training gets repeated every year and is created for the entire company, which can be an explanation for these characteristics.

The excluded variables from the structural equation model and rejected items have been analysed separately. Perceived impact on productivity is measured in terms of an employee feeling like the amount of time spend on training and on behaving securely is appropriate and if security training does not impact the efficiency of completing their work. This efficiency is mostly impacted by security training to be perceived as time consuming and text-heavy. Where the repetitive and irrelevant nature of the security training is not seen as appropriate. However, when employees feel like their productivity is positively impacted by security training, their security behaviour will also increase slightly. This is mostly the case, when employees do not feel like the security training reduces their work efficiency. Also, the text-heavy and time consuming nature of training have an impact on employee security behaviour. These characteristics relate negatively to the perceived security knowledge and also the security behaviour of employees. However, respondents mostly agree that the security training can be put into practice within their abilities. This also has a small positive effect on their security behaviour.

In correspondence with other research, this study reveals a small favour to females on behaving securely and on their perceptions regarding security training. Moreover, employees between 25 and 35 years old, rely more on security structures provided by the company and will therefore also state their behaviour to be more secure and perceive the security training to be better. A significant interaction occurred between employees who are involved in security related projects and their security behaviour. This is probably created by their background knowledge on the security risks and on aspired security behaviour, which they also translate to their clients.

All together, this results in the recommendation, that overall an organisation should look into the perceptions of employees regarding security training. Subsequently, the feeling of security training to be general, boring and irrelevant could be reduced by providing training per target group and free employees of training that is not applicable to them. In terms of creating more specific training, the constructs within this research can be used specifically to improve training in order to enhance secure behaviour. For instance, redesigning training to fit into busy work environments and being easy to put into practice. In order to make the cost of compliance for employees not higher than the security benefit, it is recommended to honour the commitment of employees to security training. This entails helping the employee complete the training by not only redesigning training but also providing it through an user-friendly application. In order to help employees, a feedback loop between user and creator of the training should be in place. This will result in employees feeling heard, connected and actually contributing to the security posture of the organisation.

Next to that, the perceptions of security training to be hard to find time for and time consuming, together with their the impact on the productivity of employees is very important. When employees have the feeling that the costs of compliance is higher than the benefits gained, they will not be as engaged in the security training and find ways to work around this. The organisation should look into providing employees with security training hours, that do not influence the pressure on employee's primary tasks and try to make security processes fit into the business processes. Being transparent and structured when providing security training and elaborating what the specific goal of security training is, can enhance the feeling of employees that their security behaviour is effective and that they can contribute to the security goals of their organisation. A possibility also could be, to look into reward structures for security training. This will provide employees with motivation to complete the training and enhance their security training performance. So, to make sure people do not ignore security training, we should design training that does not ignore them.

Contents

Nomenclature

Abbreviations

Abbreviation	Definition
CoSEM	Complex System Engineering and Management
WEF	World Economic Forum
ICT	Information, Communication and Technology
IT	Information Technology
CIA	Confidentiality, Integrity and Availability
SETA	Security Education, Training and Awareness
NIST	National Institute of Standards and Technology
ISO	International Organisation for Standardisation
DDoS	Distributed Denial of Service
WBL	Web-Based Learning
PKI	Public Key Infrastructure
HREC	Human Research Ethics Committee

List of Figures

List of Tables

1 Introduction

1.1. Background

Cybersecurity continues to be of high interest and a serious challenge to various organisations, business areas, enterprises and governments. Primarily, due to the cybersecurity landscape currently consisting for a large part of cyber attacks and breaches, that endure losses and create a significant amount of risk (Peković, Zdravković, & Pavlović, 2019; Ponnusamy, Selvam, & Rafique, 2020). Organisations depend on information systems to perform daily work activities and to achieve their goals. Information systems reinforces an organisation's performance and productivity. However, users of information systems are likely to serve as a leading factor in the existence of cybersecurity risks (Abawajy, 2014). Establishing a robust cybersecurity protection system remains complex, given the dynamic, the frequency and the composure of cyber attacks, especially the attacks that make use of social engineering (Conteh & Schmick, 2016). Social engineering is a method that causes users to endanger their information systems. Oppositely to technical attacks, social attacks use manipulation, influence and even persuasion to target humans with access to information systems. Protection against this type of attacks is usually ineffective and humans are likely to perform poorly on detecting deception and lies (Marett, Biros, & Knode, 2004; Qin & Burgoon, 2007).

The main security priority of organisations is to protect their network against intruders or attackers. The weakest link identified by researchers and experts, are the employees in the organisations, whom are both a threat and the first line of defence to the security of the organisation (Aldawood & Skinner, 2018). For this reason, organisations should provide employees with adequate security resources and training, but above all create a security aware environment (Norris, Mateczun, Joshi, & Finin, 2019). To prepare employees for possible attacks and reduce the risks of cybersecurity threats, awareness training in an interactive and innovative way is introduced. Along with providing employees with cybersecurity awareness campaigns (Sallai, 2016). A definition of cybersecurity awareness is stated as, the level of understanding that users have of the information security best practices and the importance of cybersecurity. Overall, in every organisation the levels of security awareness vary among employees. Whom are progressively involved in all sorts of online activities, like messaging and social networking, with a significant number of employees unaware of the security risks they are exposed to when they do so (Shaw, Chen, Harris, & Huang, 2009).

Providing employees with security training is needed to change employees their security attitude and security behaviour. Also, the security training is aimed at generating an organisational-wide security minded culture, where employees protect the information assets and perform their day to day activities in a more secure manner (Albrechtsen & Hovden, 2010). This evolves around creating, promoting and maintaining sufficient security habits, as the most important factor of effective security management. The goal of cybersecurity awareness training is to change this overall security culture and increase the understanding of employees on how to behave securely and the rationale behind this. All together, this will decrease the likelihood of possible attacks and threats and increase the early detection of suspicious activities and prevent possible losses (Abawajy, 2014).

Organisations recognise that employees can be of significant value to reduce cybersecurity risks. In order to reduce the human error, organisations focus on the compliance of employees in terms of adhering to security regulations and completing security training. Comprehension of compliant behaviour seems to be crucial and the solution to enhancing information security (Bulgurcu, Cavusoglu, & Benbasat, 2010). However, cybersecurity training providers and professionals solely concentrate on measuring effectiveness of cybersecurity awareness practices by measuring compliance (Korpela,

2015) and do not try to understand why employees wouldn't comply and how they perceive the security training provided.

1.2. Research Problem

In this section, the research problem will be explored. By considering a series of previous studies and the knowledge gaps that appear when analysing previous work that show relevance for further research. Together, this will result in the final problem statement and a description of the scope of the project.

1.2.1. Prior Research

A series of previous studies work with interviews and/or surveys to investigate the relationship between the behaviour of employees and the organisations their security training. These studies are mostly directed at exploring the impact of attitude and perceptions on employee security behaviour and take into account the intrinsic and extrinsic factors influencing this behaviour.

First of all, in the research of Pahnila, Siponen, and Mahmood (2007) it appeared that careless employees are a mayor threat to the security of a company. This study states that employees are not only asked to be aware of the cyber risks, but also need to comply with the security procedures and policies. The intention to comply is significantly impacted by the attitude, norms and habits of employees. This research also suggests that the propensity of an employee to comply is affected by the social environment around them.

Expanding on intrinsic factors influencing employee behaviour, Rheea, Kimb, and Ryuc (2009) model the impact of security experience on the self-efficacy by using the social cognitive theory. They also analyse the role of self-determination on the impact of security related scenarios. This resulted in the conclusion that high self-efficacy shapes individuals whom are more security aware and use cybersecurity tools to a greater extent.

Secondly, several models are being used to study the human factors influencing cybersecurity. Like, models based on the theory of planned behaviour and the protection motivation theory (Ajzen, 2002; Rogers, 1975). However, these models provide an inadequate or mediate fit to actual human behaviour. Where the theory of planned behaviour is ignorant of more broad contextual factors and is likely to assume that compliance to security training procedures is a positive outcome. Although, the right cybersecurity behaviour of employees can be predicted by social norms, attitudes and perceived behavioural control. Most of this effort is positioned to the compliance to security policies and security training procedures (Bada, Sasse, & Nurse, 2019).

Previous research measures the level of security in terms of compliance to security policies and procedures and perceive compliance as the most effective way to reduce cybersecurity attacks in organisations. The employee security behaviour has to be improved, in line with security policies and regulations, to generate a secure environment (Woon & Kankanhalli, 2007). Ifinedo (2014) used the social bond theory perspective to investigate information security compliance behaviour. This involved employee attachment, commitment, involvement in particular activities and the belief that behaving secure is important to guard the information assets of their organisation. In another study, Cheng, Li, Li, Holm, and Zhai (2013) revealed that the bond of an employee to their organisation is likely to result in better security compliant behaviour.

In addition to this, there has been a shift from perceiving employees as the biggest issue regarding security and trying to fix them, to understanding why they do not comply or do not want to comply to security policies and procedures. For instance, usability of security has been researched by Ben-Asher and Gonzalez (2015), to understand how users cope with security tasks and if organisations provide security that is realistic to complete within human capacities. In addition, a paper on 'shadow security' Kirlappos et al. (2014) focuses on understanding the non-compliance to organisational security policies, in order to offer security policies that fit within the organisation. The failure to comply to policies has also been researched by Beautement, Sasse, and Wonham (2008) in terms of managing security behaviour of employees based on the perceptions of individuals regarding the costs and benefits to behaving

securely. Finally, Beautement et al. (2016) add to this, with managing security by looking for aspects where business processes and security processes clash, in order to be a more secure and productive organisation at the same time. Still, there is room to explore this shift further and the knowledge gaps that were found are discussed next.

1.2.2. Knowledge Gaps

Researchers of security behaviour have shifted from considering humans as the weakest link (Pahnila et al., 2007) and solely focusing on their compliance to security rules and procedures (Ifinedo, 2014; Woon & Kankanhalli, 2007) to understanding the usability of security (Ben-Asher & Gonzalez, 2015) and the perceptions of individuals regarding security training (Beautement et al., 2008) as well as comprehending non-compliant behaviour (Kirlappos et al., 2014). This is a fundamental shift, where the perceptions of employees on the top-down provision of rules, procedures and training are more central. That can create insights from a user point of view, in order to provide effective security. This specific research will add to this, since it does not only capture the employee perspective on the costs and benefits to behaving securely and being compliant, but also has the opportunity to capture the perspective of the team that creates the training and the team that checks employee compliance. This will then in return provide the possibility to see how the security training is provided and if expectations towards employees actually match up with the employee perspective. The opportunity to align different views on security training, by using qualitative and quantitative research opportunities, is a knowledge gap that hasn't been researched before.

Second, exploring security behaviour and how this phenomenon is experienced by employees within a company, could add to improving the actual effectiveness of security training. Behaviour has been proven to be hard to change and measure, but very important in analysing the effectiveness of organisational structures (Beautement et al., 2008). That's why it is even more important to try to define this behaviour. Defining employee security behaviour is a challenging task and a very important one, to understand the security culture and improve this culture within organisations. This research will contribute in measuring behaviour for this particular organisational context and how this inter-relates to the different constructs. It adds to previous research, by creating a new employee security behaviour scale that has not been used before.

Overall, adding to research regarding effective security from a user point of view. This research will contribute by not only capturing different perspectives to security training and how these perspectives align, but will also provide another security behaviour scale than used before. Also, performing the research within this specific organisational context, will provide conclusions and recommendations with respect to this security culture and organisational setting.

1.2.3. Problem Statement

Several researchers and organisations belief that employees are the weakest link to securing a system, but also recognise them to be the primary defence. Security awareness is therefore acknowledged to be of high importance for organisations and in order to raise awareness security training is provided to employees. In line with security training, security policies are in place to enforce the security behaviour of employees. These policies are translated in the form of security training modules to employees. However, organisational security is solely focused on compliance, in terms of employees completing the security training and adhering to security rules. The problem here is situated around the lack of interest on how perceptions on security training influence effectiveness and if employees feel like the training can be included into their daily activities. Most importantly, this research is aimed to explore how security training can be designed in order to be effective and not create a conflict between the productivity of employees and secure behaviour. Subsequently, this research will be based on the security trainings in place within the organisation and possible improvements for their organisational culture will be examined.

1.2.4. Scope

Security training occurs in educational and organisational contexts. This research will address security training within the context of an organisation. All the employees in any organisation are prone to various cyber threats. The goal is to reduce the risks of these events happening. This is done by reducing the likelihood that one of the employees is prone to threats. To reduce this likelihood, employees need to be made more aware of the existence of threats and know how to react if they occur. Therefore security training is in place. In every company, employees have different knowledge levels regarding cybersecurity, which will vary among each department. In this research, different departments of a global Professional Services Firm, that is used as the case for this study, will be included. Assuming that employees with a technical background, will have more security knowledge than employees in non-technical departments. Also, all the security training modules will be included in this research and will be referred to as security training. Next to that, the employees included in the research are located in the Netherlands. So, only the Netherlands is in scope of this research.

1.2.5. Research Questions, Method and Flow

The research question to be answered in this thesis project is:

How do employees perceive the security training of their organisation and what is the impact of that perception on their security behaviour?

After constructing this question, several sub-questions were formulated. Together these questions are used to solve the fundamental research problem.

- SQ1: What are the organisations security policies and security training modules and how do they relate to each other?
- SQ2: How is compliance to the security training measured and what happens when employees don't comply to learning policy?
- SQ3: How do employees perceive this way of receiving security training?
- SQ4: What is the impact of security training on the employee self-stated security behaviour?
- SQ5: In light of the answers to the previous sub-questions, what aspects of security training can be improved within an organisational context?

In order to get a profound understanding of security training and the compliance expectations related to this training, the information security awareness team and learning team of the organisation will be interviewed. The information gathered from these interviews will be used to inform the survey statements. This survey will be developed and distributed to several departments within the organisation. So, a combination of qualitative and quantitative research methods will be used to answer the research question and sub-questions.

All together, the research flow diagram (shown in figure 1.1) provides an overview of the suggested research phases. Connected to the phases on the left of the diagram is the build up of the chapters of the report and on the right of the figure are the research methods and phase deliveries. With subsequently, each sub-question connected to the phase. All together, this will result in a research discussion and conclusion and all come together in the final report.

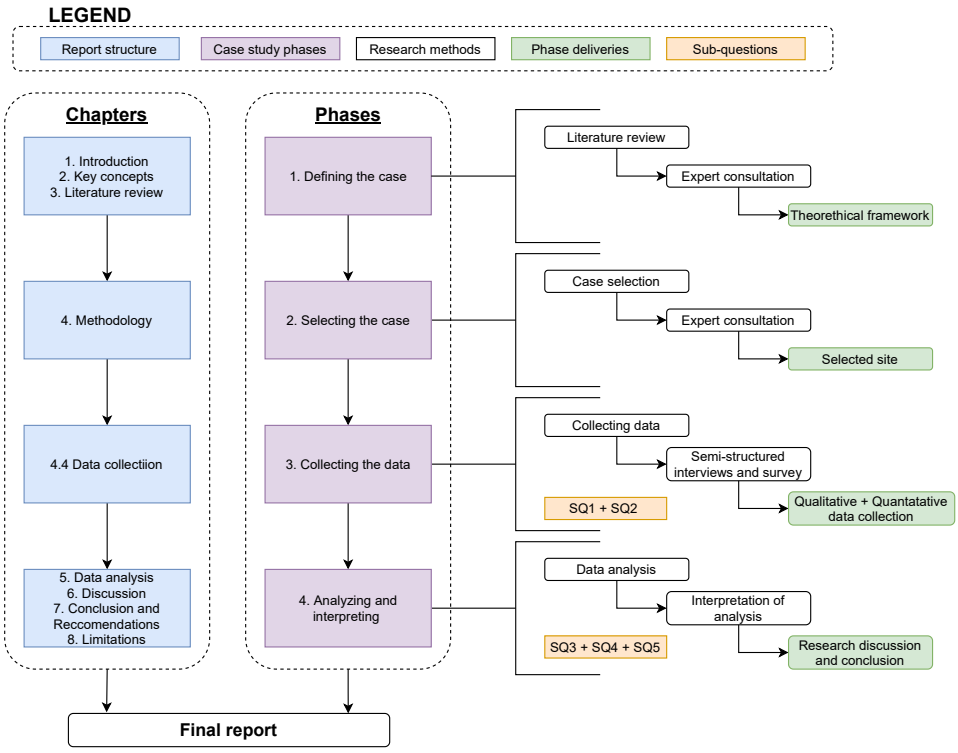

Figure 1.1: Research Flow Diagram

1.3. Relevance

In this section, the academic and societal relevance of the research are discussed. In addition, the final subsection will explain the fit of this research project to the CoSEM Master and to the track Information and Communication.

1.3.1. Academic Relevance

The protection of organisational information assets and cybersecurity have been the subject of many previous studies. Still, cyber threats and attacks keep increasing and the cyberspace consists for a major part of threats and risks. The academic relevance of this research is, that the research will help profiling security training and how this training impacts employee security behaviour, with a mixed methodology approach of qualitative and quantitative analysis. This will not only provide information on the essence of security training and on the expectations of the learning experts. Yet also provide insight in the perceptions of employees regarding the security training and impact of these perceptions on their productivity and effectiveness. Knowledge of this phenomena can be expanded and new exploratory insights can help create a better understanding of security training. This can support the shift to understanding the non-compliance of employees in order to create effective security. Instead of considering employees to be the problem or the weakest link, like referred to in many other studies (Aldawood & Skinner, 2018; Pahnila et al., 2007) and only focus on their compliance to security rules (Ifinedo, 2014; Woon & Kankanhalli, 2007).

The second contribution to the academic relevance of this research is by the creation of a new scale. Security behaviour has been a relevant scientific domain, where in several studies this behaviour still remains hard to define and measure. The models used in previous research give an inadequate or mediate fit to actual human behaviour (Ajzen, 2002; Rogers, 1975), where the focus on compliance appears to cut short on the analysis of this concept. Therefore, it is useful to examine a different way of analysing security behaviour and creating a theoretical framework combining relevant aspects from different previous studies.

1.3.2. Societal Relevance

The societal relevance evolves around the bigger picture, where reliability of the security of an organisation is crucial in the modern world. When an organisation deals with sensitive information and their security practices are not sufficient, this can have an enormous impact on society. The Global Risk Report of the World Economic Forum has concluded that cybersecurity has become an extensive global problem (McLennan, 2021). Cyber attacks have become common to critical infrastructures and mainly across sectors like transportation, healthcare and energy. Entities that perform cybercrime are joined forces and not likely to be caught. Cybercrime can have negative consequences in terms of cost, loss of reputation, or even causalities. For this reason, corporate leaders and governmental bodies are responsible for enhancing digital trust and global cybersecurity.

This research adds to the current societal goal to maintain safe and secure day to day practices within organisations. Specifically, the research focuses on the human component, whom are mostly considered to be the weakest link and also the primary defence when an organisation is subject to cyber attacks. The secure behaviour of employees is an important factor in protecting organisational assets and preventing losses.

This research will be beneficial for any organisation, who has to train or already educates their employees in being security aware. Therefore the outcomes of this research will contribute to the security of organisations and people whom interact with these organisations. The deliverables of this study will provide improvements to security training and help reaching an adequate level of security awareness amongst an organisation. Together this can protect the organisation's informational assets and prevent the endurance of possible losses.

1.3.3. Fit with CoSEM

In the Master Complex System Engineering and Management at the faculty Technology, Policy and Management, all the courses focus on solving problems within socio-technical systems. Where technology and humans are intertwined and are not to be analysed separately from each other. In this thesis project, the social and technical part of the system are respectively, the employee security behaviour and the security training itself. To adequately address this phenomenon of employee security behaviour, the interactions between the technological and social aspects of the system have to be analysed, subsequently creating a complexity to the research. Additionally, the goal of this study is to provide organisations with recommendations to improve the current security training, based on a case study of a global Professional Services Firm. In the CoSEM Master, a research study is usually finalised with recommendations for the institutional setting.

Within this Master, the track Information and Communication was chosen. This fit with this project is expressed by the focus on ICT and the human aspects connected to it. For instance, in order to be able to analyse security behaviour appropriately, a good understanding of the ICT aspects of security is required.

1.4. Outline

In this report, first the key concepts will be discussed in section two. After that, the literature review resulting in the theoretical framework of the research, will be illustrated in section three. A description of the research methodology, measures, data collection and data preparation is described in section four. In section five, the data analysis and a detailed description of the results is covered. Next, a discussion of the findings is provided in section six. Together, the conclusion and final recommendations are discussed in section seven. In addition, section eight will provide the limitations to the study and future research possibilities. Section nine, finally provides an illustration of the organisation chosen for this study and its organisational structure.

2
Key concepts

Before analysing security behaviour and the factors that impact this behaviour, the key concepts will be discussed. This chapter will elaborate the concepts cybersecurity, cybersecurity awareness and cybersecurity awareness training.

2.1. Cybersecurity

Concerns regarding protecting IT systems against attacks by unauthorised persons have been increasing over the past several years. Many experts and policy makers expect the number of attacks and their impact will increase over time, as people depend on the internet and connected systems more (Rainie, Anders, & Connolly, 2014). The operation of securing information systems and protecting the information assets, is called cybersecurity. Cybersecurity is a common term that has been defined in many different ways. Overall, the term cybersecurity concerns usually one or more of the following:

- A set of measures and activities in order to defend against threats, attacks and disruptions on computers, network related hardware and devices. Most of all, to protect the data and software that they transfer and contain.
- The quality of protection against these kind of attacks and threats.
- The overall picture of actually implementing and improving cybersecurity practices and security quality (Fischer, 2014).

Another term commonly used alongside cybersecurity is information security. To clarify the difference between these terms. Information security is primarily focused on the concepts of CIA: Confidentiality, Integrity and Availability. Where in information security the key assets to be protected are information and the information systems. A definition of information security is then also cited by 'Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities' (Von Solms & Van Niekerk, 2013).

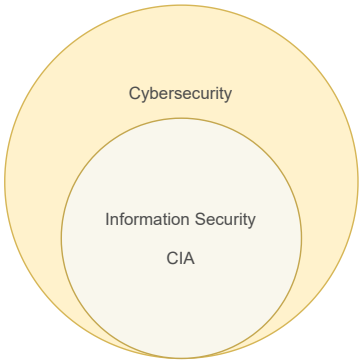

Figure 2.1: Information Security → Cybersecurity

This security is directed at protection of the technical layer, but threats and attacks do not only impact the technical part of an organisation. On top of this technical part is the socio-technical part, that is related to the actors that are exposed to cybersecurity risks of all domains when they carry out activities and function in cyberspace. Cybersecurity is different from information security, because it has more emphasis on the external effects of possible breaches to the physical world, more emphasis on human and organisational factors, rather than only cryptography and more emphasis on managing residual risks, rather than excluding risks. Fredrick Chang (2012), former Director of Research at the National Security Agency in the United States discusses the interdisciplinary nature of cybersecurity: 'A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed.'

This multi-disciplinary nature entails an increasing complexity when creating effective cybersecurity practices. Analysing and assessing cybersecurity risks and improving the cybersecurity in an interconnected world like we live in nowadays is very important. Security risks are defined as the equation of probability times impact. Acceptable levels of risk are determined by the business. Cyber teams use this outcome to design balanced preventive and repressive measures and align all these activities among different groups and layers. The following Bowtie Diagram presented in figure 2.2 provides a visualisation of this process. A good way to reduce risks caused by human errors and prevent incidents from happening is by enhancing cybersecurity awareness. This concept will be explained in the next section.

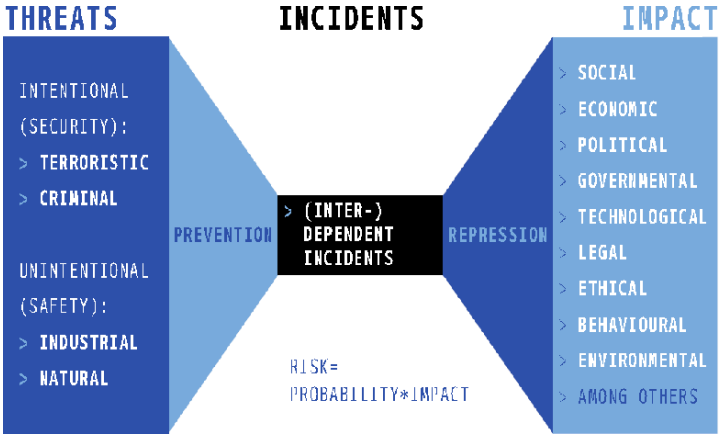

Figure 2.2: Bowtie Diagram

2.2. Cybersecurity Awareness

Awareness on itself entails being involved with the surroundings, over time, space and frequency. The concept of awareness is generally known in many disciplines, where security awareness includes attention at addressing the security, safety and sustainability of electric systems (Blasch et al., 2019). This concept is crucial at a personal level and on an organisational level in any information security program. Where absence of security awareness can result in risky behaviour like: using untrusted websites, revealing personal information, installing risky applications and sharing personal information with other parties (Liang, Xue, et al., 2010).

As mentioned in the introduction, security awareness can be defined as the level of understanding that users have of the information security best practices and of the relevance of cybersecurity for the organisation. Overall, in every organisation the level of security awareness varies among employees. Whom are progressively involved in all sorts of online activities, like conducting business and making deals, with a significant number of employees unaware of the security risks they are exposed to when they do so (Shaw et al., 2009). In organisations it seems like the awareness on the formal procedures and policies regarding security is limited. By the lack of a good communication channel, employees do not report issues or suggestions even though they might be willing to. In the real working world, managers should support their employees in behaving securely and give them the ability to make the right security decisions. Therefore, it is important that managers are security aware, since the security education and awareness that they advertise will be elucidated and arbitrated on a local scale. When it is the case that managers and their teams create their own understanding of their interplay to the security of information systems and data, caused by neglect of the organisation to awareness, the company can create security risks that have the ability to damage the organisation (Kirlappos et al., 2014).

The technology to secure and protect the organisation can be really solid. However, only a small error from the user part can easily weaken the technological defence in place. For any organisation, the employees play a fundamental role in securing their organisation. They can introduce risks to an organisation their information assets, especially employees whom have a low cybersecurity awareness (Sallai, 2016). Previous research sheds light on the impact of security awareness on compliance to information security policies by employees. The goal of raising security awareness among employees, is to provide them with the education and tools to be able to identify security risks and know their role and responsibilities regarding the security of their organisation (Bulgurcu et al., 2010). In addition, stated by the Information Security Forum (ISF, 2007), 'security awareness is a continual process of learning by which, trainees realise the importance of information security issues, the security level required by the organisation, and individuals their security duties.' This learning is commonly created by providing users with web-based security awareness training modules. The reasoning behind this way of generating awareness and what cybersecurity awareness training defines is discussed in the following section.

2.3. Cybersecurity Awareness Training

To create cybersecurity awareness amongst employees, the right cybersecurity awareness practices should be in place. Traditionally, cybersecurity is perceived as a service to be provided, this resulted in researchers primarily focusing on the technological part of cybersecurity rather than the socio-technical part (Al-Daeef, Basir, & Saudi, 2017).

Multiple researchers state that users view security as a secondary goal. For that reason it is needed to train employees and make them more aware and able to respond threats and detect deceptive activities. Previous research has shown that there is proof for good security training to increase security awareness and enhance security behaviour (Abawajy, 2014; Kumaraguru et al., 2009). An example, is SETA, short for Security Education, Training and Awareness, defined by Hight (2005) as a program of education that is intended to decrease the number of security breaches caused by human errors. This program is composed in order to inform employees of security issues and make them able to protect their organisations network, data and themselves. Security for employees within SETA is included in all their day-to-day activities: like reporting unusual emails or activities, logging of computers and using strong passwords. In addition, security awareness training is considered to be a critical approach in increasing security based on the security standards of the National Institute of Standards and Technology (NIST) and, the International Organisation for Standardisation (ISO Central Secretary, 2016; national institute of standards & technology, 2013).

In nearly all security programs implemented in organisations, the security awareness factor seems to be neglected. Training has proven to be an assuring method to increase user awareness and therefore reduce the negative effects of human errors. The overall goal of any security specific training program is to get users to preserve the knowledge required for an extensive period of time and in that way giving them the ability to translate this knowledge into their daily work. However, the implementation procedures and efficiency of current training methods fluctuate significantly. For example, some training programs are based on embedded concepts, whom are proven to enhance decision making processes of the user, and some are not (Al-Daeef et al., 2017). Due to the high importance of reaching effective security, is critical to find a way of providing security training in such a way that the user can get the knowledge required, hold on to it for an extensive amount of time and translate it to the environment. This is to be accomplished by providing a training process, that stimulates the user in behaving securely and that works alongside their normal work activities. In the next section, the literature review will elaborate on the factors influencing employee security behaviour and how this phenomenon is impacted by the security training in an organisational context. Finally, this will result in a theoretical framework as the foundation of the analysis. From now on in this report cybersecurity awareness training, will be referred to as security training.

3
Literature review

The main goal of security training is to create security awareness and make employees able to behave securely within the organisation. To achieve this goal and provide effective security training, employee security behaviour will be analysed in an organisational context.

3.1. Employee Security Behaviour

Employee security behaviour is defined as 'the behaviour of employees when using organisational information systems (including hardware, software, and network systems etc.), and such behaviour may have security implications' (Guo, 2013). Some examples of security behaviour are the use of network resources, how employees handle company data and manage their passwords. Based on most research, this security employee behaviour can be split into compliant and non-compliant behaviour. Where compliance is represented as conforming to the procedures, policies and norms of the organisation regarding security. When exploring the security behaviour in terms of compliance, an interesting approach is shown by Li, Pan, and Zhang (2019). This study examines how employees tend to react to security demands and how this influences their compliance to information security policies. This research solely relies on the compliance factor in analysing employee security behaviour. Another example of a related study is a research by Stanton, Mastrangelo, Stam, and Jolton (2004), that explores security behaviour in an organisational context based on motivational factors, like the commitment, role, type of organisation they work for and others. Together this entails an empirical study of personal and situational factors in relation to security behaviour. Subsequently, a constant comparative method of security countermeasures and organisational cultures by Yuryna Connolly, Lang, Gathegi, and Tygar (2017) resulted in insights on the impact of employee security behaviour in an organisational setting. The qualitative nature of this study based on grounded theories, has the implication that the research findings are not likely to be generalised to other organisational contexts.

On the other hand, there are also studies that focus on understanding why employees do not comply to security measures and try to provide a better foundation to effective security management. For instance, Kirlappos et al. (2014), share the vision that security training should be workable and fit into employees their daily work activities. Next to that, the compliance budget paper of Beautement et al. (2008) contributes to this view of effective security, by introducing a method to understand the perceptions of employees on the cost and benefits to compliance and to behaving secure. To provide different means for security managers to influence employee security behaviour. In addition, Beautement et al. (2016) provides a methodology to analyse employee security behaviour, where the effectiveness of security policies is assessed together with the impact of policies on employee security behaviour.

This study will contribute to these previous studies, by trying to identify why employees do not feel like they can comply to security procedures and how to introduce effective security that functionates alongside the business processes. Instead of just focusing on employees their compliance/non-compliance to security regulations.

3.2. Employee Self-Stated Security Behaviour

In this study, the employee self-stated security behaviour will be explored, this behaviour provides an indication of how employees view their security behaviour. There has been criticism on the use of self-stated behaviour and however it makes sense to be cautious, self-stated behaviour should not be overlooked. Workman (2007) shows in a research of social engineering, a strong relationship between objective measures of behaviour and self-stated behaviour, with a correlation of 0.89. From this relationship, it can be concluded that close to 80 percent of the variance in behaviour can be explained by

self-stated behaviour.

Moreover, it is relevant to acknowledge that there are problems regarding objective measurements of security behaviour. As an illustration, measurements of actual incidents are deficient, because systems do not always detect infiltration into the system. Subsequently for the detected ones, many are not reported. Next to that, to make sure responses of respondents are not biased, certain standards are in place. First, to remove any situational factors that could impact the answers of participants, the survey respondents are assured of anonymity and confidentiality. This will give them no indication to provide socially desirable answers and most likely result in a more adequate measure of behaviour (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

Next to this, leading articles on security behaviour like the HAIS-Q questionnaire of Parsons et al. (2017), the Security Behaviour Intention Scale of Egelman and Peer (2015), the article of Russell, Weems, Ahmed, and Richard III (2017) on 'Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors' and many others use self-stated behaviour to measure security behaviour.

3.3. Perceived Security Training

As explained in the key concepts, due to the high importance of raising security awareness amongst employees, it is critical to provide effective security training. In such a way that the user can get the knowledge required, hold on to it for an extensive amount of time and translate it into their day-to-day activities. This can be accomplished by providing security training, that stimulates the user in behaving securely and that works within their normal work activities. As a result, this research will measure the perceived security training, in other words the perceptions of employees on the security training modules of their organisation. These perceptions are required to consider if the security training provided is effective and to see if employees are able to include this training into their work activities, without the training putting pressure on their primary work tasks and work performance. To get a profound understanding of how these training modules are created and how quality and relevance of the content is assured, the team that creates this training will be interviewed. In addition, the learning team of the organisation will also be interviewed. To get a better vision on the effectiveness of the security training and the problems regarding compliance to security training. This will ensure accurate survey statements to measure the perceptions of employees on the security training and make them more likely to provide significant end-results.

3.4. Perceived Effectiveness of Security Behaviour

In the context of security behaviour, Culnan (2014) and Anderson (2005) researched perceived citizen effectiveness. Here perceived effectiveness is presented as the belief of an individual that distinctive actions can be of importance in securing actions on the Internet. Citizens with such perceptions are more probable to perform the right security behaviour (Anderson, 2005). When transferred to the context of security behaviour in organisations, employees are more likely to be compliant to security procedures and perform adequate security behaviour, when they believe their performance has an impact on the overall organisational security goal.

An employees believe is enhanced by their intrinsic motivation. Researchers have discussed the fact that 'no artificial incentive can ever match the power of intrinsic motivation' (Kohn, 1993). For instance, Benabou and Tirole (2003) show that intrinsic motivation is often quite rational and plays a central role in many economic and social interactions. The research of Davis, Schoorman, and Donaldson (1997) shows that intangible rewards that are intrinsic of nature, like self-realisation, reinforce individuals their motivation and work ethic. This self-realization refers to the concept of self-efficacy, which is defined as the ability or capability of users to perform the proposed behaviour. In this context, self-efficacy relates to the users ability to behave in such a way that they minimise security risks (Ifinedo, 2014). Self-efficacy is a near perseverance of human behaviour and a type of self-evaluation. Subsequently, self-efficacy relates to the belief of an individual that they are able to arrange their actions, based on cognitive resources and motivation. Computer related self-efficacy is connected to the judgement of users their competence to use computer resources in order to reach a particular end goal.

This self-efficacy presents computing behaviour, where effectiveness of behaviour lies in the belief of carrying out a task in the domain of computing (Safa, Von Solms, & Furnell, 2016).

In addition, Ardichvili, Page, and Wentling (2013) have found that individuals want what is best for their colleagues, the organisation and the community entirely. This results in the interest of the community and moral obligations to be of higher value, than self-interest. Employees are committed to the organisation and to the performance of the organisation. So, they engage in activities if they believe their efforts will improve the company outcomes. Hence, this brings us to the next two hypotheses:

H1: Perceived security training is positively related to the perceived effectiveness of employees in helping secure the organisation.

H2: Perceived effectiveness of an employee in helping secure the organisation is positively related to employee self-stated security behaviour.

However, next to employees feeling competent and believing that they can behave securely, there are also barriers to behaving securely and to being compliant to security procedures. Even though, employees might know the need for behaving securely and want to behave securely, certain aspects can still create an inconvenience around this behaviour. Especially, in a global operating company, with a lot of different departments, people, influences and more informational assets to protect. These barriers will be discussed in the following section.

3.5. Perceived Barriers to Security Behaviour

Perceived barriers to behaving securely or being compliant, are the negative elements of the action. Even though one might know that their behaviour is effective in reducing security risks, they can find performing that behaviour unpleasant or inconvenient (Rosenstock, 2015). For example, the costs of behaving securely and being compliant to security procedures can impact the productivity of employees. Where barriers can be that the current training is seen as a burden, irrelevant or even impossible to comply to (Kirlappos et al., 2014).

Additionally, perceived barriers arise due to an employees evaluation of the possible hurdles to overcome when behaving appropriately. In cybersecurity, these barriers are complementary to the low security skills of employees, that are caused by a deficiency of cybersecurity knowledge. Furthermore, the amount of effort it takes for users to comply to the organisations their security procedures and policies, forms a barrier and impacts user security behaviour. When operating securely takes too much time and effort, it will be less probable for employees to adhere to security rules. This together with the pressure of completing their work and competing against other employees in their close work environment (Humaidi & Balakrishnan, 2015). In this research, we define the perceived barriers as the employees time, efforts and feeling of inconvenience to completing security training and to behaving securely. Therefore, the interview with the learning team, observations in the work environment and an analysis of the company structure (Chapter 9) will help to define these barriers and translate them into the perceived security training statements.

3.6. Employee Cybersecurity Knowledge

As mentioned before, in order to protect an organisation against cyber threats, cybersecurity knowledge is necessary to acquire for all employees. Simultaneously, this cybersecurity knowledge can help employees protect their organisations information assets, impact their security behaviour and together reduce the number of security incidents. Experts define security knowledge in various ways. For example, Safa et al. (2016) define security knowledge as: 'Knowledge refers to the theoretical or practical aims to understand the fact, subject, value, information or skill collected through experience or education'. Where Kaur and Mustafa (2013) defines knowledge in the relationship of 'Knowledge refers to the focus of what an employee knows; attitude focuses on what an employee thinks; and behaviour is about what an employee does'. In order to reach secure behaviour of employees, a sufficient level of knowledge is a must regarding their responsibilities and roles within the security process. Subsequently, security knowledge has to be implemented and become a routine in employees their

day-to-day tasks. Enriching every employee's cybersecurity knowledge is critical in generating the aspired security behaviour (Mohamad Rashid, Zakaria, & Nabil Zulhemay, 2013). In the next section, some studies on the relationship between security knowledge and behaviour are discussed.

3.6.1. Security Knowledge and Security Behaviour

Among a range of studies on security knowledge and behaviour, Al Hogail (2015) introduces the information security culture and deduced a positive relationship between security knowledge and behaviour. In this study, security knowledge is necessary to create an effective security culture, since the shown significant impact of knowledge on security behaviour. Related to this, Mohamad Rashid et al. (2013) stressed that in order to protect the organisation and their information assets, the employee security awareness with respect to the significance of their cybersecurity knowledge is required.

To stimulate effective security behaviour, it is critical to educate employees and to infuse them with security knowledge. This knowledge will however only positively impact behaviour, when provided to employees in a way that does not put pressure on their work productivity. In relation to this, training, knowledge and behaviour need to be coordinated in order to align them and create a security posture that is effective. Hence, to hypothesise:

H3: Perceived security training is positively related to the perceived security knowledge of employees.

H4: Perceived security knowledge of employees is positively related to employee self-stated security behaviour.

The different types of knowledge regarding security in organisations, that are most relevant and how they relate to security behaviour will be explained in the following sections.

3.6.2. Knowledge of Security Threats

Employees within organisations form either an indirect or a direct threat to the performance of the organisation. This is due to an organisations information assets most of the time being vulnerable to cyber attacks and threats. In order to reduce the impact of threats and safeguard the organisation, a good knowledge of security threats is required. In a world of technology, the number, types and targets of threats are countless. There are different forms of cyber threats, like a threat in the form of malware (malicious software, often installed via email attachments or downloaded from the Internet), spam (unwanted e-mails), spyware (monitoring software), DDoS (denial of services attack, disabling computer resources to the users), social engineering (manipulating insiders to obtain confidential information) or phishing (consists of defrauding people by luring them to a fake website, which is a copy of the real website, to have them log in there - unsuspectingly - with their login name and password or their credit card number). The main purpose of the attacks is to abduct, change, monitor or disclose confidential information that can damage or form a risk for the user (Mahfuth, 2020).

In addition, activities that make employees and the data they held vulnerable to threats are: browsing risky websites, sharing passwords, downloading suspicious software, not complying to company policies, careless use of social media and phishing phone calls or scam emails (Arachchilage & Love, 2014). When avoiding security risks, knowledge of security threats shows importance. The provision of information on the negative consequences and the way to handle possible threats is useful in enhancing employee security behaviour.

More clearly, knowledge of security threats will in this research be referring to the perceived threat. This an indication of the employee perception to the danger of a threat and the risks in terms of negative consequences for the information assets and for the organisation itself.

3.6.3. Knowledge of Organisation Security Policies

Any policy within an organisation is created in order to regulate and define employee behaviour and their course of action. Policies are mostly very detailed and appear to be rather clear to understand, yet they still don't generate the desired end-result, particularly with respect to security policies (Mishra & Dhillon, 2016). Security policies are formal rules, guidelines, responsibilities and procedures that

employees have to conform to, in order to protect and handle information and technology resources of their organisation properly. These policies are in place to safeguard the security of an organisation and their information assets, by providing employees with guidance on how to handle information correctly and explain the consequences of misuse and threats connected to data handling (Lowry & Moody, 2015). However, research indicates that employees sometimes do not comply to the security policies and procedures. These are sometimes perceived as general guidelines or mere directions to follow, instead of hard standards (Lowry & Moody, 2015). This is why organisations struggle with managing employee security behaviour and more research is focusing on the behavioural intentions of employees to comply to these policies and procedures (Chan, Woon, & Kankanhalli, 2015).

Therefore it is of high importance to create acceptable policies, without demanding to much from employees. Policies should be in line with the business goals and should be comprehensible, if organisations want their employees to adhere to policies and safeguard the organisational environment against intentional an unintentional threats. As reported by Da Veiga and Eloff (2010), policies have to be altered in such a way that they direct and effect the changes required on an organisational level. Specifically, to create the desired security culture, it is needed to identify and enforce security components that align to this culture.

3.6.4. Knowledge of Security Risks

Similar to the other aspects of security knowledge, it is critical to help employees understand the risks in the organisational environment to enhance their interaction and behaviour with respect to the organisation's information assets. To set up an organisational information security culture that is effective. In order to achieve this, employees should be educated on the risks surrounding the information assets and the risks that can arise when they behave insecurely (Al Hogail, 2015).

Knowledge of security risks will enhance the ability of employees to recognise security risks and act applicable to minimise or even prevent losses (Blythe, Coventry, & Little, 2015). Providing risk awareness training is used to enhance employee security risk knowledge in most organisations, for example password risk awareness training to avoid deficient password management. Providing continuous training to employees, will improve their knowledge base and skills needed to handle information securely. A necessity for organisations is to distribute regular reports and information of security risks through different communication channels to employees. Think of e-mail, intranet, newsletters and workshops or campaigns (Ben-Asher & Gonzalez, 2015). Another important factor to be considered when analysing employee security behaviour is the impact on their productivity, which will be discussed in the following section.

3.7. Impact of Security Training on Productivity

Security training has the main goal to generate a working environment that includes security. Mostly, this is focused on employee compliance to security rules and procedures. However, an analysis of the impact on employee productivity and the balance between security and productivity within an organisation seems to be lacking.

3.7.1. Employee Productivity

In organisations employees constantly need to find a balance between working productively and behaving securely. When security is not easy to apply within their daily work activities and creates a burden, the security will be less effective, since they want to be productive (Beautement et al., 2008). Security is given and acknowledged to be needed, but the barriers to completing security training and behaving securely can result in problems. Where employees might perceive the barriers to behaving secure and being compliant bigger than the security gains. This than can result in a critical situation for the productivity and the security of an organisation, because of the clash between operational and security processes (Beautement et al., 2016).

Subsequently, when productivity is reduced by security measures, employees will not accept the meddling to the primary work tasks where they will eventually be judged on. They know the need for security, but are not going to create solutions themselves to security not fitting into their daily work.

Managers of security should seek for feedback on the interaction between security and productivity, in order to identify the conflicting situations and explore the behaviour of employees. Taking into account these clashing aspects and providing a security fit that works best for their organisational processes, will ultimately translate the knowing need for security to actual secure behaviour of employees (Kirlappos et al., 2014).

Still in many organisations, employees who go around security measures in order to keep their productivity high, are considered to be the root cause of security issues. Organisations respond to this 'problem', by educating employees and demanding secure behaviour instead of taking into account the probability that security is lacking and could be redesigned. Subsequently, experts on security are focused at securing the organisation by solely 'fixing' the human error. In busy organisational environments, employees will keep going around security actions that impact their primary work activities, because of the high workload and reduction of their productivity (Sasse, 2015).

As said, organisations have to protect their assets by deploying security training and policies and employees have to accustom their work operations to these elevated controls. Subsequently, employees often feel like they have to choose between working securely or working productively. The well known phenomenon this leads to is called non-malicious compliance (Posey, Roberts, Lowry, & Hightower, 2014), this is the bypass of security policies and procedures caused by the lack of balance between productivity and security behaviour. Hence, to hypothesise:

H5: Perceived security training is positively related to the perceived impact on productivity of employees. Where employees have a good perception of security training, will feel like being productive and secure at the same time is possible.

H6: Perceived impact of security training on productivity of employees is positively related to employee self-stated security behaviour. Where employees that feel like they can work productive and apply security measures at the same time, are more likely to behave securely overall.

Deriving out of these sections, it can be concluded that the perceived security knowledge, perceptions regarding security effectiveness, perceived impact of training on productivity, perceived barriers to behaving securely and being compliant, can only improve when we try to understand why these factors are sometimes not satisfactory. So, really comprehending why employees perceive training a certain way, feel like they can include the training into their work days, have more security knowledge or less than others and feel like their behaviour can effectively enforce company security goals, will be the eventual aim of this research.

Next to this, possible demographic variables that have an impact on security behaviour of employees will be explored. The factors included in the study and related research will be discussed next.

3.8. Demographic Profile

In a human environment, a number of different characteristics can be included in the demographic profiles of respondents. This research will assess the security behaviour of employees in a global Professional Services Firm and will focus on the following demographic characteristics: gender, age, department, function, if they are part of the technology consulting community, perform security related work and their deployment length. This subset is mostly generated based on related work, that also explored the correlation between demographics and employee security behaviour. For instance, studies on security behaviour show various differences and similarities based on demographics like gender or age. A role-playing phishing research acknowledges that women are more likely to open phishing emails and click on links, in the same way people between the age of 18 and 25 years seem to be more sensitive to phishing compared to individuals of an older age (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). On the other hand, studies present contradictory results when addressing security knowledge and awareness based on gender. The study by McCormac et al. (2017) presents a small favourable difference in significance for women, however A. Farooq, Isoaho, Virtanen, and Isoaho (2015) came to the conclusion that men are recognised to have a higher security knowledge and awareness. Regardless of using the same theoretical framework, these studies still presented conflicting results. Additionally, Beautement et al. (2016) found that young employees (25-34) rely more

on the organisations security structures and support, whereas older employees (50+) feel like they do not significantly influence the security process.

Other studies also emphasised the usefulness of tailoring security training to differences between individuals and groups. For example, a study by Proctor and Chen (2015) showed that every human has different absorption processes of information and decision-making practices with respect to security. Anwar et al. (2017) likewise pointed out the need for security training distinguished on gender, as a result of the gap in self-efficacy between men and women regarding security.

In the same way, security experience has an impact on employee awareness, the power to act securely and reducing security risks. Where in this research employees whom are working in the technology consulting community are expected to be more experienced in this field and are therefore likely to behave more secure. The demographics show relevance in previous research, therefore this research includes the following hypothesis:

H7: Demographics show a relationship to employee self-stated security behaviour.

How these factors are related will be evaluated in the data analysis in chapter five. The next section, provides an overview of the theoretical framework that resulted from this literature review and the connected hypotheses.

3.9. Theoretical Framework

As a result of previous findings it is expected for security training to be effective, when employees do not have to overcome barriers to complete training and to behave securely, they feel like behaving securely is effective, they can be productive at the same time and the training increases their security knowledge. This research is aimed to contribute to research that tries to understand why employees do not feel like they can comply and use this as a foundation to create recommendations for effective security within an organisational context. The theoretical framework, forming the conceptual model of this research, is presented in figure 3.1. This figure provides an overview of the impact of security training on the factors that impact employee security behaviour. Based on this theoretical framework, relevant interview questions have been generated and a survey has been constructed. Additionally, the framework functions as a supporting basis for the actual analysis of the research.

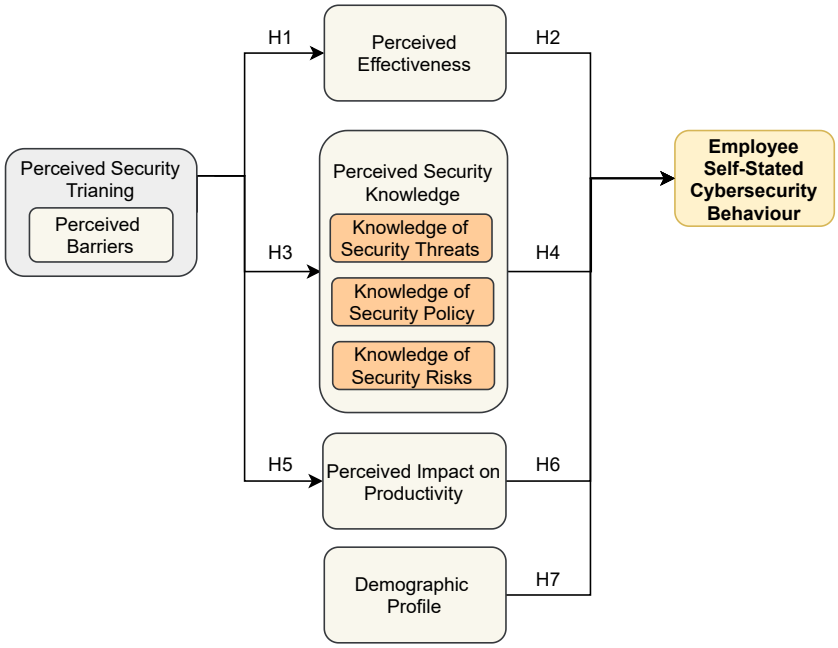

Figure 3.1: Theoretical Framework

4
Methodology

In this chapter, the research approach, research methods, measures and ways of collecting data for each sub-question will be discussed. Finalised by a description of the data preparation process for the actual data analysis.

4.1. Research Approach

The research question, as stated in the previous chapter, contains certain characteristics. The goal of the research is to provide organisations, based on the use case, with a detailed analysis of the security training, the perceptions of employees regarding this security training and the impact of these perceptions on employee security behaviour. This will require an in depth analysis of the company their security training modules, as well as an analysis of the perceptions of employees and their behaviour.

Secondly, the research question indicates an organisational culture that includes security, this will be analysed in the particular context of the company itself. Moreover, a number of aspects need to be taken into account when analysing the human factor in security. All these factors will influence the security of the company, because there is no 'one-size-fits all' solution.

This research aims to explain, describe and explore the aspects of employee security behaviour, within the specific group where the research will take place. That's why a case study approach will be adopted. A case study can be defined in several different ways, these differ in the emphasises and direction for performing the research. For instance, a case study can be defined technically, as a phenomenon for what we report and interpret only a single measure on any pertinent variable (Eckstein, 2000). Also, a case study can be an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2012). Lastly, a case study is a problem to be studied, that will reveal an in-depth understanding of a 'case' or bounded system, that involves understanding an event, activity, process, or one or more individuals (Creswell & Poth, 2016).

Performing a case study fits for this research approach, since it wishes to explore the aspects that influence security behaviour in order to generate an improved organisational culture that includes security. The research focuses on a 'how'-question and concentrates on a contemporary event. These facts are also indicators that a case study is an adequate research approach (Yin et al., 2003). Besides, case studies are grounded in 'lived reality' and strongly relate to the experiences of individuals, groups or organisations. In case studies it is possible to bring the research closer to the experiences of employees than with other types of research, since it includes the 'noise' of real life (Hodkinson & Hodkinson, 2001).

However, there are also limitations to applying a case study research approach. Designing case study evaluations, can be challenging on the validity and generalisation aspect. Mostly, because in many situations there are only a few cases available to be studied. The indicated can result in a different way of validating, then when there are considerably more cases available. This is mainly caused by the fact that the sample size has an impact on the significance of the results of the research (Yin, 2013). The next section will discuss the main phases a researcher passes through when performing a case study.

4.1.1. Case Study Phases

4.1.1.1. Defining the Case

When performing a case study, the first phase consists of defining the case. To define the case, important theoretical issues and existing literature are needed (Stake, 1995). Most important, the boundaries to define the scope, start and end of the case study should be pre-defined for each case. As well as, the organisation, interest area for the researcher, the social group that is of relevance, type of data to be collected and the way of data analysis and data collection (Yin, 1998). For this research the problem statement is already clear, so to yield an analytical framework a literature review has provided the information necessary.

4.1.1.2. Selecting the Case

Secondly, the selection of the case to be studied will need reflection and is very important in this research approach. Stake (1995) has had a significant influence on the scientific definition of the case study approach. Where he divides the case studies into three categories: intrinsic, instrumental and collective case studies. When learning about a particular phenomenon and using its uniqueness to distinguish it from other cases, typically an intrinsic case study will be selected. On the other hand, the instrumental approach makes use of one case to learn more and appreciates the broad issue or phenomenon. Lastly, when studying multiple cases at the same time, to also generate a broader understanding of a certain issue, a collective case study is performed. Based on these definitions, this research will be defined as an instrumental case study approach.

The selected site for the case study to take place, should give the researcher access to the organisation, individual or whatever else is contributing to the analysis of the study. That's why access is of substantial importance, since the researcher needs to get to know the case study environment and work in a cooperative manner with them (Stake, 1995). In this project, a global Professional Services Firm will be the site of the case study and their security training modules as well as their employees, the information security awareness team and the learning team will be included in the case.

Another important factor to consider before collecting the data, is the possible risks and burden of participation, to those who are included in the case study. As the researcher has the obligation to think about the ethical implications, before starting the research. Moreover, the need to ensure that participants have full information, to be able to make an informed decision to join the study (Sheikh et al., 2011). That's why a data management plan has been created and before starting data collection a form of informed consent has been signed by participants. These documents have been approved by the HREC (Human Research Ethics Committee).

4.1.1.3. Collecting the Data

In order to get a good understanding of the case, this approach typically adopts a range of quantitative and more commonly qualitative techniques to collect data. Like interviews, observations and expert consultations. To increase the validity of a case study, data triangulation or in other words using multiple data resources, is adopted (Mason, 2017). Next to the qualitative data collection methods, this research will also use quantitative research methods. To get a good understanding of the perspective of employees on security training and the impact on their security behaviour, a survey will be conducted.

Also, the different ways of collecting data is assumed to lead to similar conclusions and when the same issue is addressed from different perspectives, this can improve the development of an understandable picture of the phenomenon (Pinnock et al., 2008).

4.1.1.4. Analysing, Interpreting and Reporting Case Studies

The final step consists of the analysis and interpretation of the data and combinations of information. Integral to the analysing process is the reviewing of the data and sorting it. Data will be organised in such a way that it can be easily found at a later stage to address the key issues.

4.2. Research Method

In this chapter, first the main research question and the corresponding sub-questions will be provided. Second, the research methods and tools based on the sub-questions will be verified and explained. Finally, the data preparation phase will be discussed.

4.2.1. Research Question and Sub-questions

The main research question is:

> *How do employees perceive the security training of their organisation and what is the impact of that perspective on their security behaviour?*

To decide what material needs to be gathered or type of knowledge efficiency is sufficient and what type of research activity is required during the research project, some sub-questions have been conducted:

- SQ1: What are the organisations security policies and security training modules and how do they relate to each other?
- SQ2: How is compliance to the security training measured and what happens when employees don't comply to learning policy?
- SQ3: How do employees perceive this way of receiving security training?
- SQ4: What is the impact of security training on the employee self-stated security behaviour?
- SQ5: In light of the answers to the previous sub-questions, what aspects of security training can be improved within an organisational context?

4.2.2. Mixed Research Method

Multiple researchers have been investigating mixed method studies and evaluated their value. Hurmerinta-Peltomäki and Nummela (2016) found that mixed methods research contributed more in creating knowledge, since by informing the content of the second data source the validity of findings would increase. Authors have argued that studies using both qualitative and quantitative methods seem to gain a broader and deeper understanding of the phenomenon. Additionally, an advantage of using mixed methods in scientific research is the integration element. This results in more confidence in conclusions and results (O'Cathain, Murphy, & Nicholl, 2010). Some researchers even state, that in order to be certain of findings and interpretation, using mixed method in research is the only possible way (Coyle & Williams, 2011).

4.2.3. Qualitative Research Method

Qualitative methods provide the ability to get a full picture of an organisation and what is guiding the employee security behaviour. Where the primary advantage for qualitative methods is the ability to examine underlying assumptions, values and beliefs. Another huge advantage to a qualitative research approach is that the questions are open-ended, providing respondents with the possibility to raise points that are of high importance to them. For a qualitative researcher, the set of issues to be inspected is not likely to be finite or prejudiced (Yauch & Steudel, 2013).

However, qualitative research also has some disadvantages. ACAP's state that there are two downsides to qualitative data. First of all, the outcome can not be verified objectively. For the first problem, interpretations of researchers are always restricted. Knowledge and personal experiences will influence the conclusion and observations. Mainly, caused by the open-ended nature of qualitative research questions, that gives respondents the ability to control the essence of the data collected (Yauch & Steudel, 2013). Secondly, the analysis can be very intensive and interviewers need sufficient skills to conduct the primary data collection activities sufficiently (ACAPS, 2012). So, the mayor limitations to qualitative analysis are first, the fact that the critical issue could be missed and second, that the research process is very time-consuming.

4.2.3.1. Semi-structured Interviews

In this research, semi-structured interviews will be the first source of data collection together with the consultation and observation. Interviews provide a more detailed contextual analysis and will give insight in the topics of interest, because of their interactive nature (Beautement et al., 2016). The interviews will provide perspective on the security training modules and how they are created. Also, the interviews will give an indication of the expectations of the learning team to the employees, on how the team expects employees to implement the training into their daily activities. Since performance of security training is highly focused on the compliance of employees, it is interesting to consider how the teams perceive the impact on employee productivity and possible perceptions regarding the training provided. Therefore semi-structured interviews will be conducted to answer SQ1 and SQ2. These interviews will also provide information on the substance of the quantitative part of the research and are used as starting point for the survey statements.

4.2.4. Quantitative Research Method

Using a quantitative survey approach has two major strengths. Firs of all, this way of collecting data will provide the opportunity to determine the consensus or disagreement between different demographic profiles. That will allow the researcher to make comparisons between different responding groups easily. Secondly, administering and assessing the data can be done rather quickly. As the results can be transformed into tables within a relative short time frame (Yauch & Steudel, 2013).

On the other hand, these advantages can also create weaknesses, that have to be taken into account when conducting a research. Respondents lives are restricted to their immediate surroundings, that influence their identity, beliefs, perceptions and other significant characteristics. A profound understanding of this context is needed when translating these characteristics to relevant numbers. Moreover, to generate significant results, the sample size of the population researched is required to be rather large. This can be negatively affected by shortage of resources, resulting in impossibility of a large-scale and therefore more significant research (Dudwick, Kuehnast, Jones, & Woolcock, 2006).

4.2.4.1. Survey

SQ3 and SQ4 are directed at the perceptions of employees and how they impact the self-stated security behaviour. To get a good indication of the perceptions and make them comparative between different demographics, a survey is needed. Since, this can be easily distributed among employees of different departments. This indicates also a high number of respondents and higher chance to generate validated result to aim for greater generalisability (Kelly, 2011).

In addition, the different ways of collecting data is assumed to lead to similar conclusions and when the same issue is addressed from different perspectives, this can improve the development of an understandable picture of the phenomenon (Pinnock et al., 2008). A visualisation of the structure of the different research activities together with the frameworks created during this research, is shown in figure 4.1.

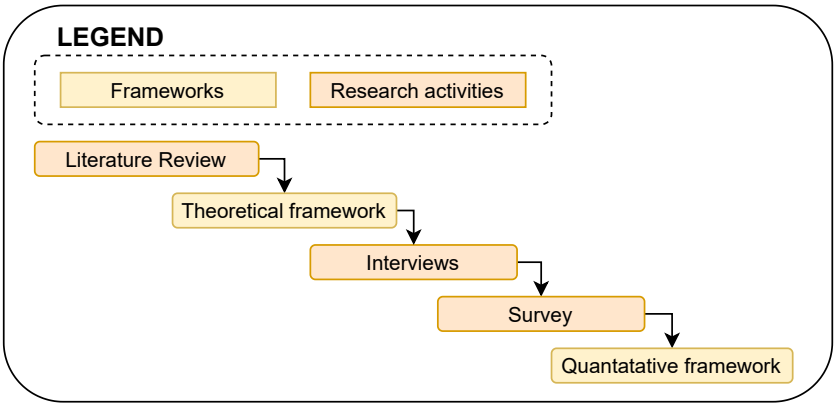

Figure 4.1: Research Activities

4.3. Applied Methodology and Statistical Tools

Within the quantitative survey research a combination of confirmatory factor analysis, exploratory factor analysis, structural equation modelling and regression analysis have been used to reach the research objective. This chapter will explain the concept of these quantitative methodologies and after that continues by explaining the measures to be used in the evaluation and presentation of the results.

4.3.1. Factor Analysis

For this research, the constructs in the first part of the survey (perceived effectiveness, perceived security knowledge, perceived productivity and perceived security training) are analysed by performing a confirmatory analysis. The employee security behaviour scale is explored by performing an exploratory factor analysis.

4.3.1.1. Confirmatory Factor Analysis

Confirmatory Factor Analysis is a way of modelling that takes into account the relationship between indicators and variables. This factor analysis has the goal of reaching the number of factors that clarify the variation and covariation between the observed measures. For a confirmatory factor analysis, the factors to be analysed and the number of items defining this factor are specified beforehand. Subsequently, the analysis will give an indication of how well the sample represents the pre-defined factor solution (Brown & Moore, 2012). In this analysis, the constructs perceived effectiveness, perceived security training, perceived security knowledge and perceived impact on productivity will be validated and tested for reliability. If these are sufficient, the variables can be included in the structural equation model.

4.3.1.2. Exploratory Factor Analysis

As the type of this analysis already describes, an exploratory factor analysis aims to explore the different dimensions represented within a set of items. This approach to factor analysis is data-driven and does not make assumptions to the pattern of the relationship or the number of common factors and their indicators. EFA aims to explore the number of measured variables that are good indicators for a construct, by determining the number of appropriate common factors (Brown & Moore, 2012). This type of factor analysis has been used to analyse the employee security behaviour scale and define the underlying constructs within this scale. As well as developing the scale that presents the employee security behaviour most accurately, based on the reliability of the scale and validity of the constructs.

4.3.2. Structural Equation Model

After the factor analysis, where the constructs have been validated, the relationships between constructs can be analysed. The basic idea of structural equation modelling is to test for causal theories within the data collected. The structural model is created to support the exploration of the depending relationships. Where path relations create networks and can be evaluated by using the multivariate data. In this research the structural equation model is used to analyse the hypothesised relationships within the theoretical framework of section 3.9. This structural equation model to be analysed, assuming that no constructs have to be deleted after the factor analysis, is presented in figure 4.2.

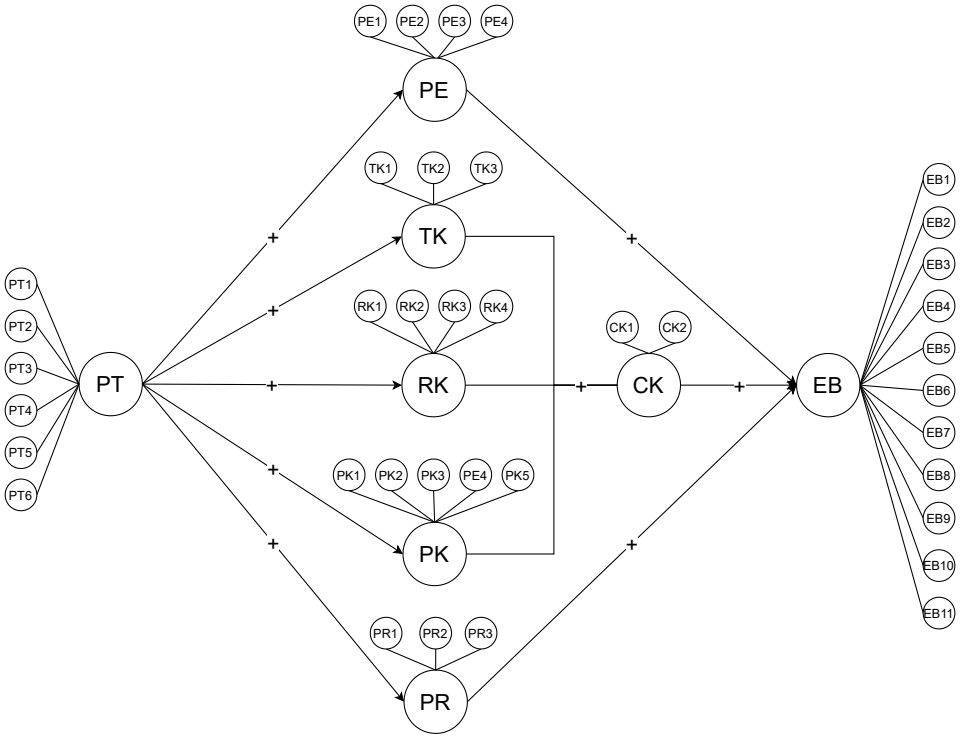

Figure 4.2: Structural Equation Model

4.3.3. Regression Analysis

When performing the structural equation model analysis, there is a possibility that one of the constructs their scale is not reliable and that the items do not represent the variable adequately. In this case, the separate items defining this construct will be regressed on the variables they have a causal relationship with. Next to that, not all the questions within the survey will be measured on a five point Likert scale and can therefore not be included in the factor analysis and SEM Model. Here regression analysis will also be performed to analyse the relationships between the items and other variables.

4.3.4. Statistical Tools

In order to carry out the analysis in this research, different statistical tools are available. For this particular research, IBM SPSS has been used to perform the overall statistical analysis. The AMOS software of SPSS has been used to analyse the relationships within the structural equation model, as described in section 4.3.2. These choices have been made particularly because of the accessibility of SPSS software for students of the TU Delft and the good interaction of AMOS and SPSS.

4.4. Measures

As mentioned before, first the information security awareness team and learning team of the company were interviewed. The information of the interviews is used in order to inform the content of the survey statements and get a better understanding of the organisational security structure. These interviews were conducted and transcribed manually, results of the interviews are shown in appendix A and B. In section 5.1 to 5.3 the first two sub-questions will be answered based on the interview outcomes and information gathered from the company intranet pages.

4.4.1. Survey Design

Now, in order to collect the quantitative data, survey statements have to be created and the survey has to be distributed amongst employees of the organisation.

4.4.1.1. Part 1: Communicated Information and Demographic Profile

The survey resides of two sections. The first part entails the an overall introduction to the survey together with the demographic profile questions.

The information in the **introduction** of the survey presented to respondents is:

Hello everyone,

First of all, I would like to thank you for filling in this survey and helping me complete my Master Thesis Project.

Cybersecurity awareness has been proven to be of high importance in organisations, especially in a global online operating organisation like you all work for. My Master Thesis Project aims to explore the impact of cybersecurity awareness training on your security behaviour and your perceptions with respect to the security training modules (WBLs) provided (think of the protecting mobile data and devices, phishing, handling information safely, password security, social engineering training).

The survey will cover the following topics:

- *Demographics*
- *Your cybersecurity knowledge*
- *How you perceive the security training*
- *How the training influences your productivity*
- *Employee security behaviour*

This will support the exploration of the factors that impact secure behaviour and provide possible improvements to training and organisational concepts from a user point of view. The survey should take around 15 minutes. The responses will be processed anonymously. Your answers will only be reported in the aggregate, individual responses are not shared.

If you have any questions regarding the survey or project, feel free to contact me

This survey is intended to give you the opportunity to voice your opinion. It is of importance that you read all questions attentively and take the time to answer them. Thank you again for participating and taking the time to answer the questions. By clicking next you agree to the conditions of the survey.

The inclusion of this introduction is aimed at informing the participants about the subject and the importance of the research. Next, explaining the structure of the survey to participants. Also, making participants attentive to the fact that all answers will be kept anonymous and that the survey will give them the opportunity to voice their opinion, which will remove the bias of socially desirable answers. Finally, to properly thank the participants for contributing to the research and explaining what will happen with end-results.

Next to this, the first part of the survey consists of questions regarding the **demographic profile** of the respondents, including:

- Gender
- Age
- Service line
- Part of TC (Technology Consulting)
- Security related work
- Function
- Deployment length

The inclusion of demographic profile questions is chosen based on results of previous research and to check generalisability of the results. This will provide the opportunity to analyse the relationship between different demographics and the security behaviour of employees. For that reason, the security related work and working in TC questions have been included. Considering the security and technology related backgrounds of these respondents. Also, gender, age, service line, function and deployment length might show differences in security behaviour and have therefore been admitted to the demographic questions.

4.4.1.2. Part 2: Measurable Items

Based on the theoretical framework, survey statements have been split into the categories: perceived security knowledge (which is split into risk knowledge, threat knowledge and policy knowledge), perceived security training, perceived effectiveness, perceived barriers, perceived impact on productivity and employee self-stated security behaviour. The items representing the constructs of the survey have been reviewed multiple times and previous research papers, interview outcomes and observations have been used to make sure the items will represent the constructs accurately.

To measure the items, a five-point Likert scale that indicates how much respondents agree to the statements has been adopted. The following numerical values are used to resemble the level of agreeability.

1 = Strongly Disagree
2 = Disagree
3 = Neutral
4 = Agree
5 = Strongly Agree

The Likert scale was embedded in the survey, since it provides practical results to analysed with the statistical tool SPSS. Next to that, five-point Likert has been chosen, since this is the most common and apparent scale to select from for respondents.

Items to measure variables

In this part the items that define the constructs used in the survey are described. Below every group of statements forming a construct, the development of the statements will be discussed. The particular statements have been chosen due to specific reasons and some of them were based on previous research.

To begin, the perceived security knowledge construct contains two overall knowledge statements and is then split up into threat knowledge, policy knowledge and risk knowledge as sub-constructs. In order to test perceived employee knowledge, questions involving words like 'know' or 'understand' or 'am familiar with' are used. The first two overall questions are focused at testing the existence of relevant security information or knowledge of respondents. Next to that, the items test if security behaviour is impacted by employees their competence in assessing risks and responding to them. Subsequently, the threat knowledge questions are focused on the employee knowledge of threats/attacks in terms of negative consequences that affect the organisation and the possible impact on their personal work. Secondly, the policy knowledge statements are focused at testing employees their understanding of

the security policies that apply to them and their role in putting these policies into practice. Then finally, the risk knowledge statements are used to measure the knowledge regarding risk and dangers to the organisation, caused by lack of security. Together with the risk that can arise as a consequence of employees their security behaviour. The following items have been used in the survey to measure employee security knowledge. After each group of items, the creation and formulation process of each statement will be elaborated.

Perceived Cybersecurity Knowledge

CK1: I am comfortable with computer technology and my company's security practices.
CK2: I know how to take action when I perceive a security risk in the workplace.

The first two items are, as mentioned, are directed at testing overall security knowledge of respondents. CK1 started with 'knowing what information security is' (a statement from ISO/IEC) and has been changed to feeling comfortable with computer technology and security practices of the company. This change has been performed to relate security knowledge to the security tasks of the organisation. The first form of the question would not be likely to result in any value, since 'knowing what information security is' is a vague statement. Next to that, the second statement has been added to measure an individual's skill at assessing risk.

Threat Knowledge

CTK1: I know the security threats that relate to my work on my company's information assets.
CTK2: I have an understanding of how my work depends on the IT systems of my company.
CTK3: If a security threat affected my company, we would still be able to continue our work.

CTK1 and CTK2, were extracted from the paper of Liang, Xue, et al. (2010) and adjusted in order to capture what we wanted to measure. For instance, threats that relate to my work instead of all threats on information assets, since it cannot be expected that an employee knows everything. This then relates to the dependability of work on the IT systems of the company. When developing CTK2, the question arose if employees then also think they can continue to work when threats affect the company and was therefore included.

Policy Knowledge

CPK1: I understand the content of the security policies that apply to me.
CPK2: I know my role with regard to the security policies that apply to me.
CPK3: I know how to put security policy into practice in order to comply.
CPK4: I know how and where to report security incidents.
CPK5: I find the security policies to be fitting to the mission of my company.

CPK2 and CPK4 are obtained from Hentea (2015) and adjusted to this particular context. Like adding 'that apply to me', since not all policies apply to everyone. Next to that, 'I know what to do when I detect a security violation', has been changed to 'I know where and when to report security incidents'. This one changed, since policies clearly state to report incidents and 'what to do' is quite vague. The other statements were self-developed and incorporated because of the aim to measure not only if employees know the policies, but also understand them. Additionally, to consider if understanding the policies also means that they can be put into practice and fit to the companies mission.

Risk Knowledge

CRK1: I know the security risks that exist in my work.
CRK2: I know the risk of not using a strong password.
CRK3: I know the risk of opening a link/attachment from an e-mail I do not trust.
CRK4: I know the risk of not keeping the software on my computer up-to date.

For the risk knowledge statements, the first item is extracted from a study by Hair, Black, Babin, Anderson, and Tatham (2010) and adapted 'work environment' to 'my work', to generate a question specifically related to the respondent's work activities. Based on interview outcomes and the companies security training topics, a subset of relevant risk specific questions have been added (CRK2, CRK3, CRK4). The first statement is used to see if respondents feel like they are aware of security risks. Subsequently, the other three statements are included to see if employees are aware of specific security risks.

Next to measuring security knowledge, the perceptions of employees regarding the security training, their effectiveness in behaving securely and the impact on their productivity have been integrated into the survey statements. Where perceived security training statements, measure the perspective on the current security training modules, in terms of quality, understandability and usability. This will also provide an explanation of the inconveniences or struggles to behaving securely and to completing the security training provided by the company. Secondly, the perceived effectiveness statements provide an indication of employees their belief to be able to behave securely. Next to that, perceived impact on productivity measures the feasibility of implementation of security into daily activities and the impact of compliance on productivity and performance of employees. The following items have been included in the survey to measure the perceptions of employees on security training.

Perceived security training

PT1: The security training that is provided is easy to put into practice, relative to other mandatory training.

PT2: Security training acts as a reminder of work-related security practices.

PT3: Security training is useful for providing me with security-related information that is new to me.

PT4: I discuss security related things with colleagues that are also in the training.

PT5: The learning application supports me in completing the security training.

PT6: The learning application supports the delivery of the security information in the training.

PT7: The security training modules are: Tick top 3 that apply.

To develop statements on the perceptions regarding security training in this particular environment, the interview outcomes and observations within the company were utilised. PT1 is included to see if respondents feel like the training can be applied, but easy to apply will only be of value when comparing to something else. Where the second and third item are included, because of the annual repetition of security training. In the interview with the learning team, the technical problems within the learning application were mentioned. So, to see if employees also find the learning application to contain glitches and not supportive to complete training, PT5 and 6 have been included. Finally, in order to capture a general view on the security training and relate this to the expectations of perceptions on training, PT7 provides the respondent with sixteen different security training characteristics to choose from. The characteristics have been extracted from the interviews. Next, the items to measure perceived effectiveness are presented and discussed.

Perceived effectiveness

PE1: If I follow the organisation's security training, I can work securely.

PE2: I can only feel that I am working securely, if everyone else is.

PE3: Security training has helped me manage unexpected and risky situations in work.

PE4: The security training provided to me, can be put into practice within my abilities.

The perceived effectiveness items have all been self-developed. First, item PE2 has been included to learn more about 'how much' responsibility respondents have compared to other employees in the organisation. PE3 is used to also cover the 'random' risks which might otherwise panic an employee, instead of the already mentioned 'day to day'. Now, the items forming the perceived impact on productivity construct are explained.

Perceived impact on productivity

PR1: Completing the security training takes a reasonable amount of time.

PR2: I feel like behaving in a secure manner, takes an appropriate amount of time.

PR3: I feel like following the security training, reduces the efficiency of completing my work.

Security training has an impact on productivity of employees, according to several papers (Beautement et al., 2016; Beautement et al., 2008; Kirlappos et al., 2014). In these papers the efficiency in completing work, the amount of time spend on training and to behave securely, were repeatedly mentioned problems regarding the balance of productivity and security. That's why PR1, 2 and 3 were included into the survey statements.

All together, the impact of the aforementioned constructs on the employee self-stated security behaviour will be analysed. In order to get a good indication of security behaviour, the statements to test this behaviour have been evaluated using multiple related studies. In these statements qualifiers have been avoided and to adequately measure the frequency of engaging in secure behaviour, a Likert scale from 'never,' 'rarely,' 'sometimes,' 'often,' to 'always' is used. The following items have been used in the survey to measure security behaviour.

Employee security behaviour

EB1: I don't open attachments to emails from an unfamiliar source.

EB2: I review and delete company business emails and attachments that I know are no longer required or to be retained.

EB3: I do not install non-standard software on company authorised or company provided systems or devices.

EB4: I use only the cloud data storage, processing and transfer services that are provided by my company for my work.

EB5: When creating a password for my work account, I use a passphrase that has no names, consecutive numbers or content of previous passwords.

EB6: My password that I use for business purposes is different to the one I use for personal purposes.

EB7: I use remember password features that are provided by company information systems and services.

EB8: I lock the device screen and secure the company laptop when stepping away from it.

EB9: I shut down or power off my company laptop before transporting it.

EB10: I will not allow anyone else to access the company technology that has been assigned to me.

EB11: I am keeping the computing devices that I use to conduct business activities up to date.

Regarding these behaviour statements, some are based on the company's security policies and some on other behaviour scales. EB5, EB6, EB8 and EB11 are based on the Security Behaviour Intention Scale of Egelman and Peer (2015). All the other behaviour statements are derived from company policies, where the most relevant ones have been chosen. For instance, EB9 might seem unnecessary and weird, but from observations it appeared that employees do not follow this rule since it is very time-consuming.

To make sure that participants will not provide socially desirable answers, two check questions have been included together with a request to read the questions attentively and take the time to answer them.

4.4.2. Survey Administration

These two parts have been wrapped together in a survey. To make sure no errors in measurements would occur, the layout of the survey, format of the questions and the order of the questions have been designed attentively. The survey is intended to look apparent and well arranged and contains a detailed introduction with fitting instructions. Also, to enhance credibility, the identifying information is clearly demonstrated on the survey.

For each item, a connected label is created, to make it easy for the researcher to link the items to the constructs. To make sure respondents do not get confused, the questions have been separated into sections, that are mentioned in the introduction statement of the survey. Before the actual distribution of the survey, a pilot survey has been send to two supervisors. Based on information of possible respondents, relevant academics and the feedback of these two supervisors, final adjustments have been made.

4.4.3. Data Collection and Response Rate

The aim of the collection process was to create a sample that is representative of the dynamic organisational culture. No employee of the company had to be excluded from the sample, since everyone who participates in security training could fill in the survey. In order to monitor the responding sample, the questions to determine the demographic profile were introduced. The results to these questions, which present the profiles of the participants, are presented in 5.4.1.

The data was collected utilising the email network within the company and employees from several departments have been contacted to help distributing the survey. Due to the university providing free access and the good user interface, Qualtrics has been chosen as a survey tool to collect the data. The survey has been presented via email to approximately 600 employees and Microsoft Teams was used to send reminders and engage employees to help completing this research project. Participation was not rewarded and the survey was open for two weeks. In the end, 105 employees filled in the survey, which results in a response rate of 17,5%. This is a sufficient rate for a thesis survey.

4.4.4. Data Preparation

In order to make sure only accurate responses are analysed, the collected data will first be prepared. To start, the following two check questions were presented to participants in two parts of the survey:

CH1: To check that you are paying attention please select Disagree in this question.

CH2: To check that you are paying attention please select Often in this question.

The respondents that did not answer Disagree and Often to these statements, were excluded from the data set to be analysed. The first check question was answered wrongly by six respondents and two of these respondents also didn't answer the second check question correctly. The respondents are excluded, to make sure that participants were paying attention and read the statements carefully. For this preparation it is not needed to exclude missing values, since the survey would not allow for questions not to be answered. Also, possible outliers were detected and excluded from the final data set. This all lead to a final data sample of 99 respondents to be analysed.

5
Data analysis

To get a better understanding of the current security training of the organisation and how they are developed, the global information security awareness team of the company has been interviewed. The information security awareness team is involved in different awareness practices like: managing the whole security program by providing campaigns, info-graphics and yammer posts, creating the WBL's (Web-Based Learning's) content based on hot topics, analysing data, actual phishing and the ambassador program. The ambassador program is created to get volunteers to distribute the material that is created by the security awareness team. By sending information within teams and creating events across all locations.

This interview along with information found on the companies network page, has been employed to answer the first sub-question:

- SQ1: What are the organisations security policies and security training modules and how do they relate to each other?

In this section, the organisation's security policies, the security training modules and the way these training modules are created will be discussed.

5.1. Organisation Cybersecurity Policies

In an organisation of this size and operating on global scale, a wide range of policies are required. The policies that are specified with regard to the cybersecurity of employees are the following:

- Acceptable Use of Technology: provides direction for personnel about the appropriate use of technology when conducting business. It supports the Global Code of Conduct regarding respecting intellectual capital, protecting personal data and client confidential information, and acting in accordance with applicable laws, regulations and professional standards.
- Global Information Security Policy (Code of Connection): the policy defines security controls, as well as roles and responsibilities for the protection of information and information systems integral to Information Security Management System regardless of the location. The purpose of this policy is to provide requirements and establish consistency for protecting information and information systems while striving to improve the companies overall security posture. The policy also sets forth requirements whereby compliance will be measured and audited.
- Information Security Management System Policy: defines information security management system of the company that includes the processes and roles and responsibilities for protection of information and information systems.
- Password Policy: defines security controls and attributes necessary for passwords created, used by, supported by, or provided by the company. Security controls are defined for each password type.
- Vulnerability Management Policy: to establish a single, consistent approach to managing security vulnerabilities through patch and configuration management at the company. This approach includes specific time frames for mitigating risks associated with vulnerabilities.
- Certificate Policy: to allow those associated with PKI to estimate the trustworthiness of certificates issued by the PKI, by specifying the requirements or provisions which must be met in various aspects of PKI operation. These include among other things, aspects such as issuance and vetting procedures, technical and physical security controls, revocation handling, and legal requirements.
- Information Classification Policy: define four classifications of Digital Information and the necessary controls to protect them.

- Logging Policy: Provide the minimum requirements for event logging for information systems, services and networks used by, supported by, or provided by the company.
- Prohibited and Non-standard Software Policy: to establish which category of software are prohibited by the company and are not to be installed on provisioned and managed end user Windows and macOS computers.
- Information Security Incident Response Policy: is a foundational document for the Cyber Defence program. It defines which events are considered incidents, defines roles and responsibilities , and lists the requirements for reporting cyber security incidents, among other items.
- Network and Internet Security Policy: designed to impose security controls that minimise the risk to the company arising from the use of networks and the internet without hindering the ability of the company to deliver value to clients.

It is unlikely that all the employees know every policy. For this reason, security policies are translated into security training modules. This is to increase knowledge regarding cybersecurity and the policies in place.

5.2. Organisations Web-Based Learning

The company has a learning page, where the employees can search training courses and complete them. On this page, 'Find Learning' is the search function where employees can browse the learning courses provided by the company. These are not only related to security, but there is a collection of different types of learning courses provided. In the 'Learning History and Compliance' page, the completed learning courses of the employee are listed, together with the credits and certificates that are linked to the courses. The tab named 'My Learning Assignments' provides an overview of the assignments that are overdue, due next or due later. This gives an indication of the work left to do or not completed in time. The company can assign curricula to employees, these will be summarised in the 'Curriculum Status' box. Each curriculum title links to the 'Curriculum Details' page, that includes a list of curriculum's items and 'Action' drop-down menus where employees can register for or request items. On this page employees can also view the sub-curricula associated with each curriculum and access information on learning items. Next, an overview of the security training modules provided on this learning page are discussed.

5.2.1. Organisations Security Training Modules

The organisation at hand has the following modules in place to raise security awareness and improve the security behaviour of their employees. To provide an illustration of these training practices, the names and focus of the modules are discussed.

- Defeating Social Engineers: with increasingly sophisticated technical defences for networks and computer systems, hackers often decide. It is much easier to simply go around these perimeter defences by attacking the end user. Hackers often use social engineering to gain access to sensitive and confidential information from end users through every day, common interaction. This course will teach employees how to identify and avoid giving away sensitive information to these hackers.
- Incident Reporting: this course covers the most important types of security events and incidents employees should report and how to report them.
- Password Security: this is an interactive learning course that provides useful tips for creating passphrases and other security best practices to prevent passwords from being compromised. The learning objectives entail: how can cyber-criminals guess employees passwords, best security practices for password management and tips for creating passphrases.
- Phishing: the phishing learning focuses instruction and simulations on combating phishing attempts. By mastering the information and experiencing the simulations presented in the course, employees will be able to defend the workplace data from phishing threats.
- Protecting Mobile Data and Devices: today's smartphones and tablets can not only act as a phone, but also as an email client, mobile Internet device, camera, GPS navigation system, entertainment console and platform for any number of applications, they can be exposed to many of the same risks as a desktop computer. This course uses high-quality video and real-world simulations to teach best practices for mobile security.

- Handling information safely: employees work through this course to find out what they need to know and do to handle information safely at all times. By the end of the course, employees should be able to recognise confidential information when they see it and know what they need to do to protect information from loss, theft, or inappropriate disclosure.

These modules are created by the global information security awareness team. How this team creates these Web-Based learning modules is discussed in the following section.

5.2.2. Creating Security Training Modules

During the creation of training modules on security, the team typically passes through the following phases:

1. First step is to define the topic of the security training module by considering feedback of different internal organisations. For instance: investigations, core reported incidents, leadership assessments, management assessments on current issues in the market and review reports on the most common breaches.
   Next to this, industry trends are used, where a lot of security training materials and presentations are based on what is currently happening. The team currently focuses on topics like personal email and working from home related to COVID. Working securely from home is also a mandatory security module at this moment, during a pandemic it is important to reinforce this. Adapt awareness around the new situation to working from home, since there are more distractions at home and other home responsibilities. The team checks what is happening inside the organisation and outside the organisation together, to pinpoint the most relevant topics for the security training modules.
2. Create a proposal with these topics. The team makes use of an external vendor, they review their catalog according to the catalog they want to pursue. Corresponding to this, there are two kind of proposals: mandatory ones for all employees and role-based security module proposals to focus on different people or areas.
3. Propose the security module to leadership, to get approval. Once it is approved, everything starts moving. Very slow, but in the end it gets implemented in the learning application of the company.

The cybersecurity policy information is used as a standard to translate into the vendors catalog. The catalog of the vendor is used as a starting point, according to the selected topic this catalog will be filled in accordingly. The vendor has a basic content, very-high level, which the team reviews. Starting by editing the text considering the organisations policies. First thing they do, is to validate the training based on company policy. After that, the training will be checked by technical stakeholders and will be changed according to their feedback.

In order to raise security awareness throughout the years, quarterly campaigns have been introduced by the information security awareness team. These campaigns are themed instead of topic driven, in order to combine multiple topics into one theme. For example, security awareness for different ages. Different topics for different ages, like senior vs kids. Collecting metrics on these topics, to help to analyse and find gaps and get more awareness around these gaps. The awareness is still quite new, for the awareness team it comes in three stages:

1. Statistical, any numbers to be collected. Collecting everything they can, like how many yammer posts, how many views, BeAware (the page with all security policies and info) hits.
2. Assumption, based on this metrics it can be assumed what is going on. Like people are more interested in phishing or have more knowledge with respect to another topic.
3. Holy grail: behaviour change metrics are really hard to prove. For these kind of metrics, they work together with the cyber defence team. By analysing their logs and actions they perform themselves, like the campaigns, trainings, mandatory trainings, they can see if there are changes in behaviour. Like when the amount of employees that click on phishing links increases, the effectiveness of training on this topic has to be reconsidered.

In addition, the learning team of the company has been interviewed, in order to evaluate the performance and compliance structure of the security training provided by the company. The next section will yield an overview of the results based on the answers of the interview in appendix B. Together this will answer the second research question:

- SQ2: How is compliance to the security training measured and what happens when employees don't comply to learning policy?

5.3. Compliance to Web-Based Learning

Overall, employees have to reach an amount of 120 points in three years, to be able to be compliant to global policy. This is split in technical and non-technical sections, with respect to assurance there are also some mandatory learning modules included for all employees. There are multiple policies involved, whom are different for each target group. Security training is for everyone, so will be applicable to all employees.

Employees receive points, called CE points, these are learning points. These points are based on the time spent on learning and the performance during the training. Points are inserted in their learning management system, based on participation registration these points are monitored. This is mostly done by the system itself, through the attendance based registration tool. Where every time unit is translated into a learning point.

When employees do not comply/do not reach the 120 points within three years, their service lines will be addressed by global. People are obliged to be 100% compliant. The service lines will monitor this closely and make sure that their employees reach the points required. It is not the case that people get accused on this, but the global team monitors the learning team closely to make sure learning points are fetched. So, employees will have make sure that they get the learning points required.

The learning team is responsible for deployment of the training modules and not directly for measuring compliance. So, measuring this compliance is the responsibility of the service lines themselves and the stakeholders involved. They just make sure that the training modules are provided, however they support the services lines by providing them with data on compliance of employees and by sending people reminders etc. But the real responsibility is embedded within the service lines.

Employees can either complete their learning modules during working hours or in their spare time, if working hours won't allow it. Everyone in the business has to reach their productivity of work, so how employees make this work doesn't matter as long as they do. That is why employees just make sure that they complete the 120 hours. Still it is a combination, employees have to complete training and that is included in the plan. Ofcourse, the plan takes into account the productivity of employees and does not want to lower this. So, not all learning will be done in spare time, however there are a lot of different training modules available. The service lines indicate that they don't want their people spending too much time on these learning plans, because for one, it lowers the productivity of employees and secondly, every training costs money which the learning department will collect from the service lines.

In addition, because security training is regulated globally, the training modules are not designed differently for different target groups. The global team operates very far from the working field and don't experience the actual day to day practices within the offices. Externals do not have access to the system, while the learning team would actually like them to run through the learnings as a basis before they work with clients of the company. In addition, the number of modules assigned to new joiners is quite much. Also, when performing extra learning there is not an extra reward received by employees or anything to enhance this.

Together, this all results in employees viewing these training modules as a hassle to complete, some of them are general and employees don't think they need the modules provided to them. Especially the mandatory ones, that they have to repeat annually and are seen as a burden and a waste of time. Often the technology is also not that user-friendly, there are a lot of bugs in the closing of the training modules. This results in employees having to do the training again or get articles send to them with

next steps. Now people take a screenshot when they have completed the training, so they can proof that they have done it and get it switched to compliant. However, this is again extra work, since this has to be sent to the learning team and that team has to fill in a form, which is send to Global. Global then has to approve this, then it goes to system support and they have to change the status to compliant. Which goes per unit, and they have 5000 employees. Which is not making the completion of training modules very popular amongst employees.

Next, these findings have been used to inform the survey statements and will be linked to the outcomes of the data analysis of the survey. This will be discussed in section 5.4.

5.4. Survey

Through a survey that is distributed among different departments of the company, SQ3 and SQ4 are answered. The content of the survey has been split into demographics, perceived security knowledge, how employees perceive the security training, how the training influences their productivity and employee security behaviour. To start, the demographic profile of the population sample will be discussed in section 5.4.1.

5.4.1. Demographic Profile

The data collection resulted in 105 respondents from different departments, deployment lengths and different backgrounds with security related projects. After the data preparation, as described in 4.4.4, six respondents were removed and this resulted in a sample of 99 participants, for who the demographics are shown in table 5.1. As the table shows, the amount of male respondents is twice the amount of female respondents. Next to that, the age group between 25 and 35 years is the largest within the sample, which makes sense within a constantly evolving company like this. The majority of the respondents are part of the consulting service line and have either an intern, junior or senior function. In addition, the sample covers a nice spread over respondents being part of Technology Consulting or not, if they perform security related work and over the deployment periods of the employees. An overview of the descriptive statistics of the demographic questions is provided in Appendix D.

Demographic variable (N=99)	*Frequency*	*Percentage*
Gender		
Male	64	64,6%
Female	32	32,2%
Other	0	0
Prefer not to say	3	3,0%
Age		
18 - 25 Years	9	9,1%
25 - 35 Years	68	68,7%
35 - 45 Years	12	12,1%
45 - 55 Years	7	7,1%
55 - 65 Years	3	3,0%
Department		
Assurance	26	26,3%
Tax	2	2,0%
Strategy	0	0%
Consulting	58	58,6%
CBS	13	13,1%
Technology Consulting		
Yes	37	37,4%
No	62	62,6%
Security Related Work		
Yes	47	47,5%
No	52	52,5%
Function		
Intern, Junior or Senior	65	65,7%
Manager, Senior Manager or Partner	34	34,3%
Deployment period		
< 1 year	21	21,2%
1 - 2 years	21	21,2%
3 - 5 years	31	31,3%
6 - 10 years	14	14,1%
> 10 years	12	12,1%

Table 5.1: Demographic Profile of Participants

5.4.2. Common Method Bias

Before focusing on the construct validity and reliability within the model, the items measured in the survey had to be checked for common method bias using the Harmon's one-factor test. Common method bias is caused by the method of measuring responses in a study. For instance, the introduction at the beginning of the survey can stir the answers provided by different participants to the same overall direction, which can result in indicators having a valid amount of common variation. This can also be caused by providing social desirable answers, introduced by respondents wanting to answer in a particular way. (Aguirre-Urreta & Hu, 2019). In this survey, social desirability could result in answers that give the impression like the participants behave securely, while maybe really they don't.

Not considering common method bias in empirical research has two major negative impacts. First of all, the estimated validity and reliability of the measures used in the research can be biased, because of the common method effects enforcing a systematic variance in these measures. Secondly, this variance can affect the testing of hypotheses and can result in biased estimates of the relationships between constructs (MacKenzie & Podsakoff, 2012).

As said, in this study the Harmon's one-factor test to check for common method bias has been performed. This test is based on the use of the confirmatory factor analysis to load all observed variables. Where the unrotated factor outcome, will provide the amount of factors needed to be able to justify for the greater part of the variance existing in the collected data. The test will check if the first extracted factor has the ability to explain more than 50 percent of variance. According to Harmon, this single factor extracted, should not have the ability to explain more than 50 percent of this variance to proceed the research (Aguirre-Urreta & Hu, 2019). The test is extracted using SPSS and resulted in a total of 20,5% of the total variance (See appendix E). Thus, it can be concluded that common method bias will not be a problem when analysing this particular set of data and the research can proceed.

5.4.3. Factor Analysis

In this analysis, several items are used to measure one construct. The validity of each construct is essential to make sure that the different items predict the construct in the same way. In addition, reliability is directed at the dependability, meaning that the different items produce consistent results and do not differ based on the measurement process. To test the reliability of the items, Cronbach's Alpha reliability coefficient is used. Cronbach's Alpha should be at least 0,7, for the items to reach internal consistency. Nonetheless, in an exploratory study like this, a minimum value of 0,6 is also acceptable (McKinley, Manku-Scott, Hastings, French, & Baker, 1997). In table 5.2, the Cronbach's alpha values are shown for the different constructs. Since, perceived effectiveness is only measured by four items, a value above 0,5 is enough for significance (Egelman & Peer, 2015). However, the items that predict perceived productivity are not significant and should therefore be left out of the structural equation model. The rest of the variables met the required criteria to be reliable and can be included in the structural equation model, which will be analysed using SPSS AMOS. First, the confirmatory factor analysis to test the validity of the data will be further explained. All the results of the reliability and validity tests are provided in appendix F.

5.4.4. Confirmatory Factor Analysis

When performing a factor analysis different types of rotations can be preferred. Regarding the first part of the data, including the constructs perceived security knowledge, perceived security training, perceived effectiveness and perceived impact on productivity, it is likely that these correlate with each other. That is why a direct oblimin rotation has been chosen to perform the factor analysis.

The outcome of Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0,705 and Barlett's test of sphericy has a significance of 0.000. These two tests give an indication of the suitability of the data to detect structures. A high number indicates that a factor analysis might be useful when analysing this particular set of data, since it signifies the part of variance that is caused by underlying factors. When this value is lower than 0,5, the results of the factor analysis are not likely to be significant (Fabrigar, Wegener, MacCallum, & Strahan, 1999). The outcome of the test shows that a factor analysis can be valuable and will be carried out using SPSS.

Together this resulted in the loadings of the items within the constructs, which are next to the Cronbach's Alpha values provided in table 5.2.

Constructs and Items	*Loading*	α
Cybersecurity Knowledge (CK)		
CK1: I am comfortable with computer technology and my company's security practices.	0,743	
CK2: I know how to take action when I perceive a security risk in the workplace.	0,494	
Threat Knowledge (CTK)		
CTK1: I know the security threats that relate to my work on my company's information assets.	0,480	
CTK2: I have an understanding of how my work depends on the IT systems of my company.	0,751	
CTK3: If a security threat affected my company, we would still be able to continue our work.	0,822	
Policy Knowledge (CPK)		
CPK1: I understand the content of the security policies that apply to me.	0,850	
CPK2: I know my role with regard to the security policies that apply to me.	0,826	
CPK3: I know how to put security policy into practice in order to comply.	0,877	
CPK4: I know how and where to report security incidents.	0,654	
CPK5: I find the security policies to be fitting to the mission of my company.	0,509	
Risk Knowledge (CRK)		
CRK1: I know the security risks that exist in my work.	0,449	
CRK2: I know the risk of not using a strong password.	0,921	
CRK3: I know the risk of opening a link/attachment from an e-mail I do not trust.	0,572	
CRK4: I know the risk of not keeping the software on my computer up-to date.	0,659	0,842
Perceived Security Training (PT)		
PT1: The security training that is provided is easy to put into practice, relative to other mandatory training.	0,772	
PT2: Security training acts as a reminder of work-related security practices.	0,773	
PT3: Security training is useful for providing me with security-related information that is new to me.	0,568	
PT4: I discuss security related things with colleagues that are also in the training.	0,961	
PT5: SuccessFactors supports me in completing the security training.	0,836	
PT6: SuccessFactors supports the delivery of the security information in the training.	0,891	
PT7: The security training modules are: Tick top 3 that apply.		0,753
Perceived Effectiveness (PE)		
PE1: If I follow the organisation's security training, I can work securely.	0,771	
PE2: I can only feel that I am working securely, if everyone else is.	0,496	
PE3: Security training has helped me manage unexpected and risky situations in work.	0,761	
PE4: The security training provided to me, can be put into practice within my abilities.	0,602	0,553
Perceived Productivity (PR)		
PR1: Completing the security training takes a reasonable amount of time.	0,744	
PR2: I feel like behaving in a secure manner, takes an appropriate amount of time.	0,754	
PR3: I feel like following the security training, reduces the efficiency of completing my work.	0,506	0,381

Table 5.2: Constructs and Items

5.4.5. Employee Security Behaviour Scale

Concerning the security behaviour scale, the outcome of the KMO test was 0,650 and Barlett's test of sphericy has a significance of 0.000. This gives an indication that the data is correlated and measured common factors are accounted for. To extract components within the scale, an exploratory principal component analysis has been performed. Based on the criterion of Kaiser (where components with an eigenvalue > 1 are retained) components are extracted. As the scree plot in figure 5.1 shows, the Kaiser test signifies that we should keep four components.

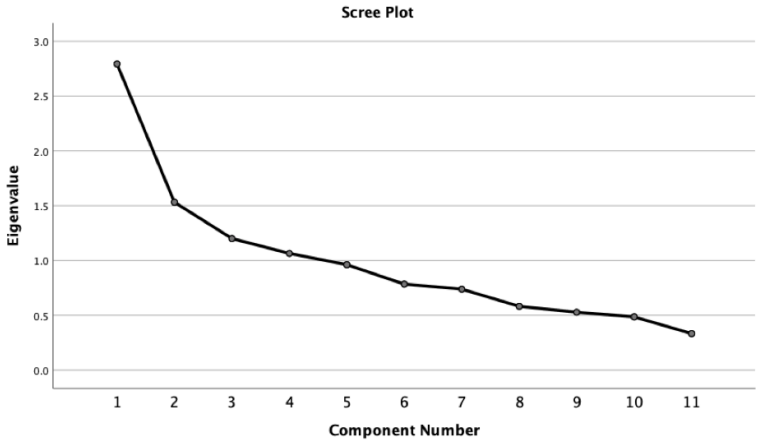

Figure 5.1: Scree Plot Eigenvalues Employee Security Behaviour Scale

The reliability of the scale has been examined in different ways. First the Cronbach's Alpha for the full scale was computed at a value of 0,654. The item-total statistics shows that deleting EB7 results in a value for Cronbach's Alpha of 0,672. This item is therefore deleted and next the item loadings will be calculated. It can be concluded that the data set is in line with the metric by McKinley et al. (1997): 'a multi-component scale is reliable if α > 0.6 for all sub-scales'.

Next to this test, a Varimax rotation was applied and factor loadings per security behaviour item were calculated. The items to be considered had to fulfil two conditions. Specifically, a factor loading should have a value above 0,5 and adhere to Saucier's criterion of only including an item in the scale, when the loading of that item is twice as much as the loading on other components (Saucier, 1994). Using these requirements, EB2 had to be removed as well. The factor analysis has been performed again without the items EB2 and EB7. This resulted in the scree plot shown in figure 5.2, that displays three components extracted to keep. Also, this analysis resulted in a KMO and Barlett's test of 0,646 with 0,000 significance, so still above the threshold value.

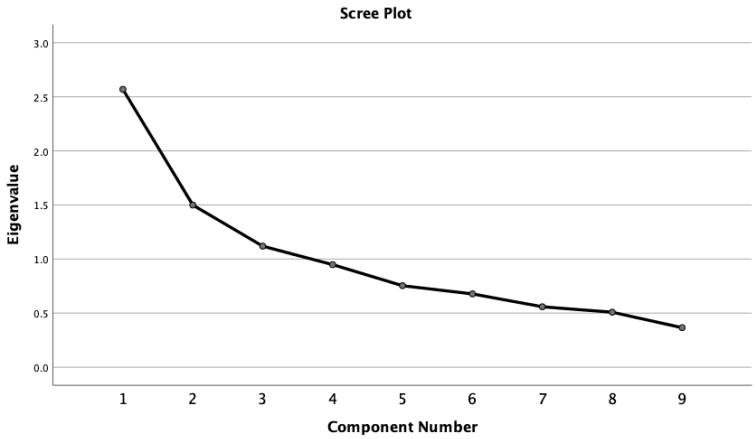

Figure 5.2: Scree Plot Eigenvalues Employee Security Behaviour Scale

As said, the factor analysis shows that three components have an eigenvalue above one and should be kept to analyse the security behaviour scale. The three components that resulted from this analysis predicted 57,6% of variance. Where component 1 accounted for 28,5%, component 2 for 16,7% and component 3 for 12,4% of variance. The scale for security behaviour can therefore be divided in three sub-scales. Based on the items in these scales the three components can be themed as follows: password security (creating strong passwords, using different passwords for work and social accounts), security awareness (not opening attachments from unfamiliar sources, not installing unauthorised software, not allowing access to computing devices by other people), device security (updating devices, shutting down before transporting company laptop, only using software provided and authorised by the company).

In addition, the inter-item correlation per construct was calculated. Inter-item is the correlation between the item and the average of all other items in their component. These values are presented in the first row of table 5.3. All items exceeded the threshold of 0,2, suggested by Everitt and Skrondal (2002). The Item Total Correlation is the average inter-item correlation per sub-scale, shown in the right column of table 5.3. This value is defined as extensive, when the correlation value is between 0,20 and 0,29. When this value is higher than 0,30 the item is described as exemplary. EB5, EB6, EB8, EB9, EB10 and EB11 exceed 0,3 and are exemplary. Items EB1, EB3 and EB4 have a value between 0,20 and 0,29, which is between the ranges and defined as extensive. All of these reliability measures and loadings are shown in table 5.3, and the full analysis in SPSS is shown in appendix G.

	Component 1	*Component 2*	*Component 3*	
IIC	0,371	0,360	0,381	ITC
EB6	0,798			0,385
EB5	0,762			0,431
EB8	0,630			0,344
EB1		0,745		0,270
EB3		0,696		0,253
EB10		0,770		0,368
EB11			0,743	0,436
EB9			0,674	0,345
EB4			0,654	0,263

Table 5.3: Factor Loadings, Inter-Item Correlations and Item Total Correlations

5.4.6. The Analysed Model

As mentioned before, the perceived productivity construct and two of the employee security behaviour items failed the reliability test. The items EB2 and EB7 were deleted from the analysis, since the scale for security behaviour is more reliable without them and will still contain enough items to verify the construct. Perceived productivity items will be analysed by performing an linear regression analysis, described in section 5.4.10. However, the perceived productivity construct was not reliable and could therefore not be included in the structural equation model.

After completing the reliability analysis for the constructs, the structural model has been adjusted. The new model is shown in figure 5.3, together with the hypothesised relationships among variables. The small circles define the survey statements, in other words the items that identify each construct. The larger circles define the following variables in the model.

- Perceived Security Training (PT)
- Perceived Effectiveness (PE)
- Threat Knowledge (TK)
- Risk Knowledge (RK)
- Policy Knowledge (PK)
- Cybersecurity Knowledge (CK)
- Employee Security Behaviour (EB)
  - Password security (EBP)
  - Security awareness (EBA)
  - Device security (EBD)

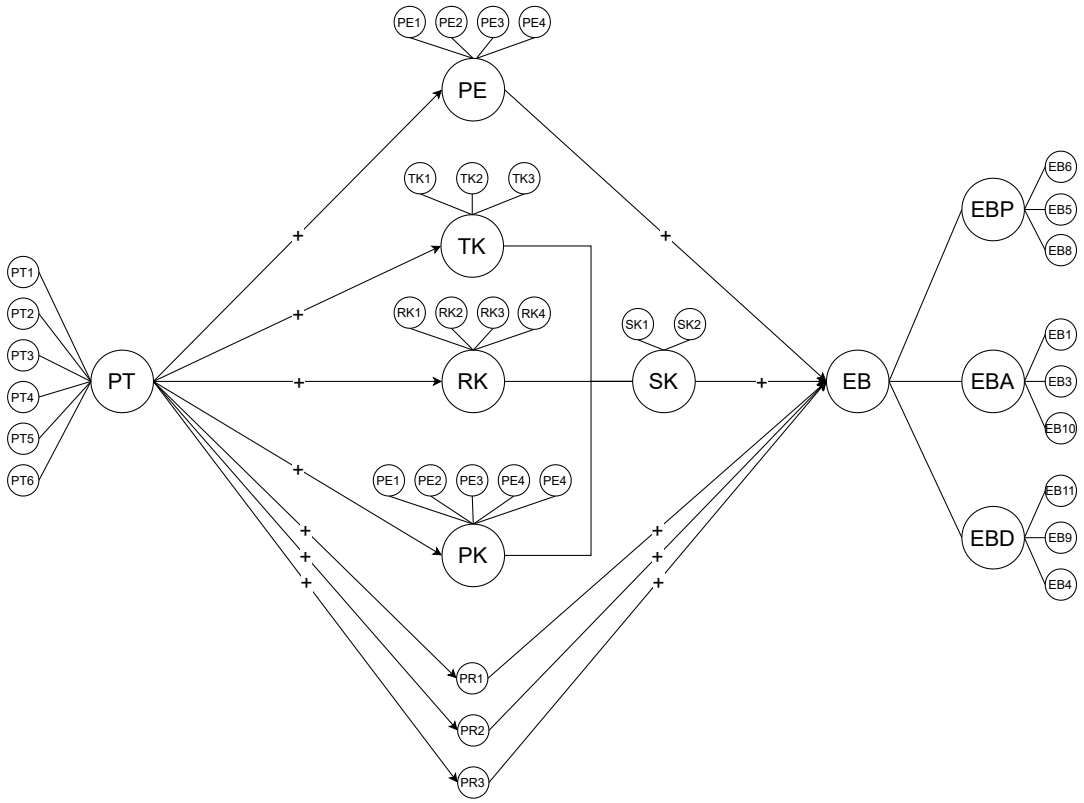

Figure 5.3: The Analysed Structural Model

5.4.7. AMOS Analysis

To generate the structural equation model and test the interactions presented in figure 5.3, SPSS AMOS has been employed. SPSS AMOS is used to analyse the relationships within the structural equation model, between unmeasured latent variables or directly measured variables. To analyse this particular model, summated scales have been used. Creating summated scales is done by summing the items that define a construct and then dividing it by the number of items. This can reduce the impact of multicollinearity on the estimated coefficients when performing the regression analysis (R. Farooq & Shankar, 2016).

In this analysis, first the groups of items indicating a construct, for instance PT1, PT2, PT3, PT4, PT5 and PT6, were summated into one variable using SPSS. This variable defines the oval of the construct in AMOS. Also, the error variance of the summated variables were calculated and inserted in the AMOS model. The higher the scale reliability, the lower the error variance. That is another reason why a high Cronbach's Alpha, as mentioned before, is of importance.

Now the structural equation model is ready for analysis and the results of the estimated model are provided in the next section.

5.4.8. The Estimated Model

This section will address the descriptive statistics of the estimated variables and tested hypotheses with the structural equation model analysis in SPSS AMOS.

5.4.8.1. Descriptive Statistics

In table 5.4, for each variable of the structural equation model, the mean and standard deviation is calculated. Next to that, the significant correlations between the variables are presented, with a threshold value of $p < 0,05$. The full AMOS output is shown in appendix H.

Variable	*Mean*	*SD*	*PT*	*PE*	*TK*	*RK*	*PK*	*CK*	*EB*
PT	3,39	0,62	-	0,785	0,304	0,395	0,530	0,319	0,300
PE	3,44	0,59	0,785	-	0,234	0,434	0,442	0,180	0,284
TK	3,74	0,52	0,304	0,234	-	0,847	0,567	0,645	0,643
RK	4,29	0,49	0,395	0,434	0,847	-	0,572	0,708	0,799
PK	3,73	0,64	0,530	0,442	0,567	0,572	-	0,672	0,573
CK	3,91	0,60	0,319	0,180	0,645	0,708	0,672	-	0,730
EB	3,99	0,61	0,300	0,284	0,643	0,799	0,573	0,730	-

Table 5.4: Descriptive Statistics for the Analysed Model

The statistics above show that the mean for risk knowledge is the highest among the sample, with a value of 4,29 on a five point Likert scale. Still, all of the variables have a mean value above average (neutral) on the five-point Likert scale. This indicates that the average respondent of the sample have a relatively positive perception of the training and their effectiveness. Next to that, they have an above average security knowledge, based on risks, threats and policies and they state that their behaviour is strongly secure.

In addition, the highest positive correlations have a value of 0,785; 0,847; 0,708; 0,799 and 0,730. These are subsequently the correlations between perceived training and perceived effectiveness, between threat knowledge and risk knowledge, risk knowledge and cybersecurity knowledge, risk knowledge and employee security behaviour and cybersecurity knowledge to employee security behaviour. Interesting is that correlations between threat knowledge, cybersecurity knowledge and perceived effectiveness are relatively low.

5.4.9. Hypotheses Testing: Structural Equation Model

The following table contain the path coefficients connected to each of the hypothesis of the theoretical framework, together with the corresponding p-value and the tested end-result. A hypothesis is approved, when the p-value is lower than 0,05 and the relationship is directed as expected (positive/negative).

Hypothesis	*Path Coefficient*	*P-value*	*Result*
PT → PE (+)	0,542	0,001	Approved
PT → RK (+)	0,336	0,001	Approved
PT → TK (+)	0,229	0,022	Approved
PT → PK (+)	0,571	< 0,001	Approved
PT → CK (+)	0,426	< 0,001	Approved
PE → EB (+)	0,184	0,069	Rejected
CK → EB (+)	0,501	< 0,001	Approved

Table 5.5: Hypothesis Testing in the Analysed Model

All hypotheses visualised in the theoretical framework of section 3.9 are supported, except for the relationship between perceived effectiveness and employee security behaviour. The significance of this relationship is above the threshold value of p < 0,05. In addition, the rest of the hypothesis even comply to the significance level of 0,01.

To visualise this, the values corresponding to the relationship are presented in figure 5.4.

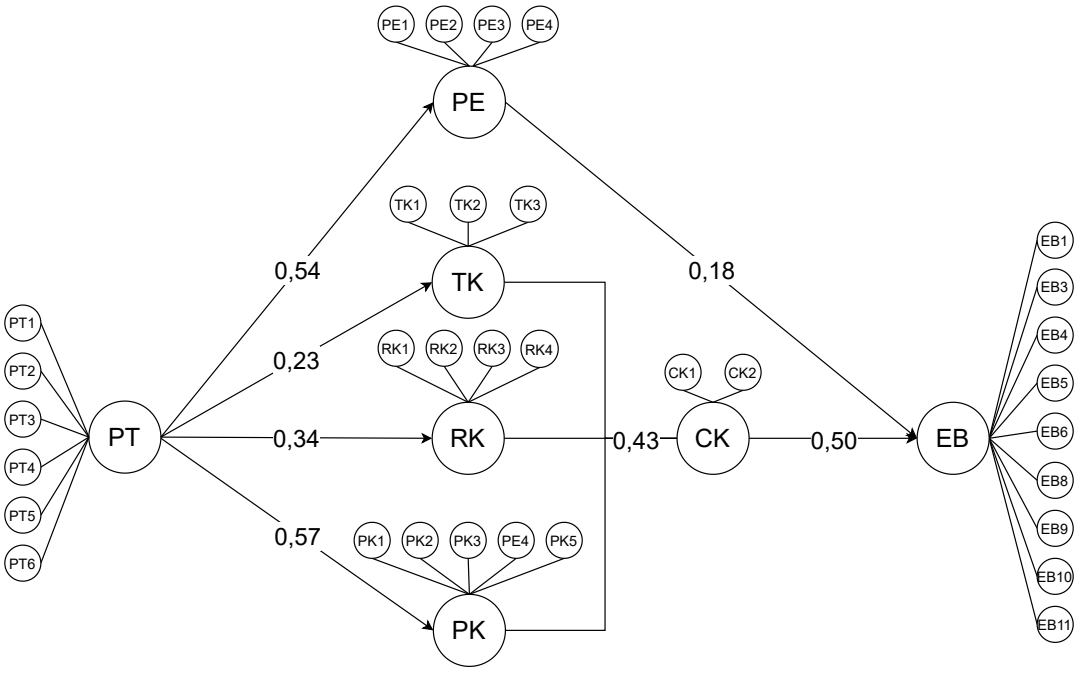

Figure 5.4: Analysed Model Including Effects

5.4.10. Regression Analysis

As mentioned before, the confirmatory factor analysis revealed that the items forming the construct perceived productivity were not significant and cannot be included in the structural equation model analysis. The explanation for this insignificance is possibly caused by the construct being predicted by only three items. This results in a lower probability to predict the construct correctly. However, the perceived productivity items should not be excluded from the research, since we want to use all data collected. So, an extra regression analysis was performed, as discussed in 5.4.10.2. Besides, the perceived effectiveness construct showed an insignificant relationship to the employee security behaviour. This insignificance is also explored, therefore the impact of the separate items for perceived effectiveness were tested using regression, shown in 5.4.10.3.

Next to that, the survey question regarding the security training characteristics, where respondents were asked to tick the top three boxes that applied, wasn't included in the the structural equation model analysis. This is because of the answers not being divided on a Likert scale. This question will be included to be analysed by first describing the data collected, then combining the multiple answers given by respondents and after that exploring the relationship to other variables. Subsequently, the relationship between this question and the security knowledge, perceived effectiveness, perceived productivity and employee security behaviour will be analysed.

5.4.10.1. Descriptive Statistics

First of all, the PT7 (Perceived Training Characteristics) question, will be analysed. The respondents were provided with sixteen choices and asked to tick the top three that applied to the security training of their organisation. These sixteen options are presented below and all of the characteristics have a corresponding opposite value shown in the options. The full SPSS analysis of this question is presented in appendix I.

- 1 = Informative
- 2 = Entertaining
- 3 = Visual
- 4 = Time consuming
- 5 = Easy to understand
- 6 = Easy to apply
- 7 = Fresh
- 8 = Specific
- 9 = Irrelevant
- 10 = Boring
- 11 = Text-heavy
- 12 = Hard to find time for
- 13 = Difficult to understand
- 14 = Difficult to apply
- 15 = Repetitive
- 16 = General

Utilising SPSS, the results to this question have been analysed. Starting with a basic description of the frequencies and percentages per security training characteristic in table 5.6.

Security Training Characteristic (N=99)	*Frequency*	*Percentage*
Informative	52	52,5%
Entertaining	0	0%
Visual	16	16,2%
Time consuming	20	20,2%
Easy to understand	49	49,5%
Easy to apply	24	24,2%
Fresh	3	3,0%
Specific	4	4%
Irrelevant	2	2,0%
Boring	30	30,3%
Text-heavy	13	13,1%
Hard to find time for	17	17,2%
Difficult to understand	0	0%
Difficult to apply	3	3,0%
Repetitive	32	32,3%
General	32	32,3%

Table 5.6: Frequencies Security Training Characteristics

An overview of the differences between these characteristics is visualised in the bar chart represented in figure 5.5. The green bars represent the positive security training characteristics and the red bars the negative characteristics.

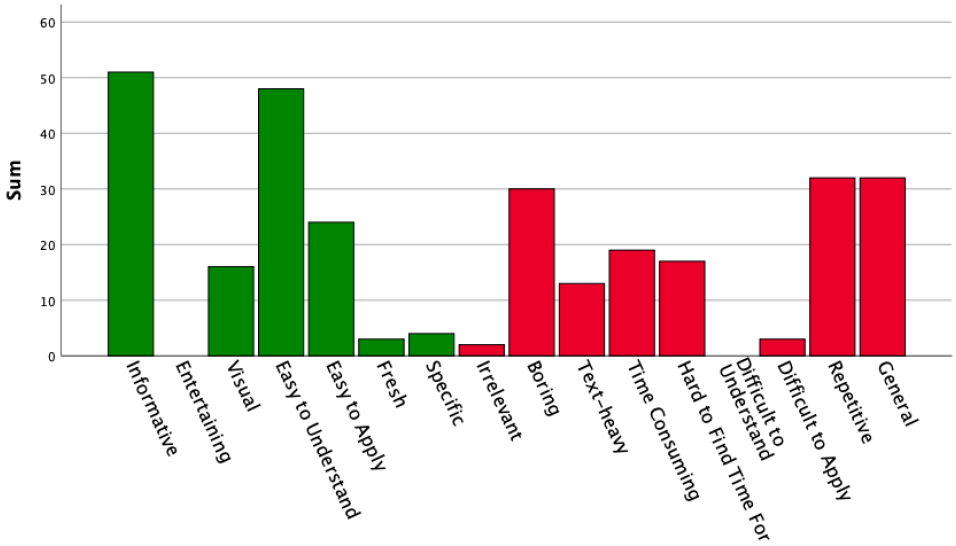

Figure 5.5: Perceived Training Characteristics Bar Chart

This figure shows that around half of the respondents chose for the security training to be informative and easy to understand. However, a third of the respondents chose the characteristics general, boring and repetitive. Also, around twenty percent of the respondents found the modules to be time consuming and hard to find time for, but also easy to apply. Further, visual has been chosen a few times more than text-heavy, but are almost equal. An interesting characteristic, which is chosen by more than twenty percent of respondents, is easy to apply. As from observations within the company, it was found that some of the security rules are quite hard to apply and are sometimes not applied. However, there is always the bias of what respondents say and what they actually do. In addition, interesting is that entertaining and difficult to understand were not chosen by respondents.

Moreover, to get a view of how employees generally perceive the security training modules, the multiple response sets have been analysed and the most common combinations of answers are provided in table 5.7

Security Training Characteristic	*Combined Characteristic*	*Combined Characteristic*
Informative	Easy to understand (33)	Easy to apply (14)
Entertaining	-	-
Visual	Informative (11)	Easy to understand (9)
Time consuming	Boring (9)	Repetitive (7)
Easy to understand	Informative (33)	Easy to apply (16)
Easy to apply	Easy to understand (16)	Informative (14)
Fresh	Informative (3)	Easy to understand (2)
Specific	Informative (3)	Easy to apply (1)
Irrelevant	Boring (1)	Hard to find time for (1)
Boring	Repetitive (14)	Time consuming (9)
Text-heavy	General (5)	Time consuming (5)
Hard to find time for	Boring (6)	Informative (6)
Difficult to understand	-	-
Difficult to apply	Hard to find time for (2)	Text-heavy (1)
Repetitive	Boring (14)	General (13)
General	Repetitive (13)	Informative (12)

Table 5.7: Combination of Security Training Characteristic Responses

The values in the table show the different combinations of characteristics and the number of times these combinations occurred in the multiple response set. Entertaining and difficult to understand have not been chosen by respondents and have therefore no combination characteristic. The results show that generally respondents combine either positive characteristics or negative characteristics. Interesting is that general and informative have been combined by twelve respondents. As well as the combination of informative and hard to find time for. This one is still rather explainable, since the employees do not have much time next to their work. However, employees belief security training is needed and think the modules are providing the necessary information to behave securely. Generally speaking, employees have either a positive perception to the security training modules or a negative one.

Next to these findings, the relationships between the training characteristics and the perceived effectiveness, perceived security knowledge, perceived impact on productivity and employee security behaviour is analysed. The correlations between these variables are provided in table 5.8 and in appendix I, analysed performing Pearson correlations. Entertaining and difficult to understand are not chosen by any participant and are therefore left out of this analysis. In addition, the items representing the construct perceived productivity were not significant, as shown in section 5.4.3. Therefore, the correlation between the security training characteristics and each item of perceived productivity separately have been analysed and are presented in table 5.8.

Variable	*PE*	*CK*	*EB*	*PR1*	*PR2*	*PR3*
Informative	**0,303**	0,105	0,006	0,106	0,120	0,040
Text-heavy	-0,076	**-0,330**	**-0,209**	0,088	-0,045	**-0,201**
Time consuming	**-0,251**	**-0,194**	**-0,197**	-0,001	-0,062	**-0,379**
Easy to understand	**0,349**	**0,226**	0,134	0,079	**0,191**	**0,0275**
Difficult to apply	0,018	-0,74	-0,020	0,079	-0,143	-0,065
Fresh	-0,008	0,063	0,002	-0,112	-0,143	0,048
General	**-0,171**	0,036	-0,005	-0,095	-0,076	-0,006
Irrelevant	**-0,262**	0,042	-0,012	**-0,350**	-0,065	0,085
Boring	**-0,169**	-0,036	-0,042	-0,014	-0,010	-0,116
Visual	**0,173**	-0,091	0,009	0,058	0,160	**0,207**
Hard to find time for	**-0,218**	-0,165	0,009	-0,066	-0,117	-0,065
Easy to apply	0,147	0,137	0,142	-0,002	0,053	0,063
Repetitive	-0,088	0,009	0,077	-0,025	**-0,170**	0,077
Specific	-0,044	-0,071	0,014	-0,001	0,132	-0,027

Table 5.8: Correlations between Security Training Module Characteristics and Other Variables

In the table, the significant correlations between the characteristics and variables are presented in bold. As said, the correlations of the characteristics and perceived productivity are analysed per item, since the summated scale for perceived productivity was not reliable.

The correlations show that informative, easy to understand and the visual show a positive interaction to the perceived effectiveness of employees. These relationships are explainable, since informative, visual and understandable training modules should have the impact of giving employees the feeling that they are contributing to the security of the company and can apply the security module contents. Next to that, the negative relationships to perceived effectiveness are, time consuming, general, irrelevant, boring and hard to find time for. This is also easy to explain, since boring, time consuming, irrelevant and general modules will not give employees the perception that the training is effective.

Secondly, the significant relationships to cybersecurity knowledge are represented by the characteristic variables text-heavy, time consuming and easy to understand. Where the perceived security knowledge of employees is negatively impacted by the training modules to be seen as text-heavy and time consuming and positively by easy to understand.

In addition, the employee security behaviour correlations, that are significant, are to text-heavy and to time consuming. The two correlations are negative, that indicates the negative impact of text-heavy and time consuming perceived training modules on the security behaviour of employees. The behaviour is sensibly less secure when employees are less engaged to do the training and find them heavy and time absorbing. This will result in the information of the training not being translated into actual secure behaviour.

The three perceived productivity statements are:

PR1: Completing the security training takes a reasonable amount of time.
PR2: I feel like behaving in a secure manner, takes an appropriate amount of time.
PR3: I feel like following the security training, reduces the efficiency of completing my work.

Since the third statement is negatively framed oppositely to the first two statements, this statement has been reverse computed. To start, employees who perceive the security training as irrelevant, do also find completing them not to be taking a reasonable amount of time. Further, training modules that are perceived as easy to understand, increases PR2, so the feeling that behaving securely takes an appropriate amount of time. Where on the other hand the repetitive nature of the training modules has a negative impact on the PR2 item.

Lastly, training modules being perceived as text-heavy and time consuming, having a negative impact on the efficiency of employees in completing their work. However, the perceived understandability and visual representation of the training modules have a positive impact on employees their efficiency in completing their work.

As mentioned, the perceived productivity construct was not included in the SEM. However a regression analysis of the separate items defining this construct with the variable employee security behaviour is still executed. This in order to find out why the items did not provide a reliable scale and to evaluate the relationships between the items and the employee security behaviour.

5.4.10.2. Regression Analysis with Excluded Construct Perceived Productivity

To begin, the descriptive statistics of the perceived productivity items are calculated and presented in table 5.9. The results of these descriptive statistics and regression analysis of the PR items in SPSS are presented in appendix J.

Perceived Productivity Item	*Mean*	*S.D.*
PR1	3,25	0,930
PR2	3,42	0,926
PR3	3,38	1,047

Table 5.9: Perceived Productivity Item Statistics

The mean values of the items are above average (neutral) and the highest mean is the second item, which indicates that overall employees feel like behaving in a secure manner takes an appropriate amount of time the most. In table 5.10 the results of the regression analysis between the perceived productivity items and employee security behaviour are calculated.

Item	*R Square Adjusted*	*Standardized Beta*	*T-value*	*P-value*	*95% Confidence*
PR1 $\rightarrow$ **EB**	-0,007	0,032	0,316	0,752	Rejected
PR2 $\rightarrow$ **EB**	0,030	0,234	2,348	0,021	Approved
PR3 $\rightarrow$ **EB**	0,076	0,328	3,420	0,001	Approved

Table 5.10: Results Regression Perceived Productivity on Employee Security Behaviour

The results in this table indicate, that when behaving securely takes an appropriate amount of time and when employees feel like they can work efficiently, this has a positive interaction with employee security behaviour. Furthermore, the PR1 item did not show a significant relationship when regressed on employee security behaviour and is therefore rejected. This can also be the explanation for the construct perceived productivity not being reliable. Since the scale is composed of only three items and one of the items is significant in relationship with the employee security behaviour.

Next to that the PT construct has also been regressed on the productivity items separately. This resulted in the outcomes presented in table 5.11.

Item	*R Square Adjusted*	*Standardized Beta*	*T-value*	*P-value*	*95% Confidence*
PT → PR1	0,187	0,432	4,719	0,000	Approved
PT → PR2	0,071	0,284	2,914	0,004	Approved
PT → PR3	0,041	0,225	2,275	0,025	Approved

Table 5.11: Results Regression Perceived Training on Perceived Productivity Items

5.4.10.3. Regression Analysis with the Rejected Construct Perceived Effectiveness

The hypothesis of perceived effectiveness having a positive effect on the security behaviour of employees was rejected by the structural equation model analysis, since this value was positive but not significant. The separate perceived effectiveness items have been regressed on employee security behaviour, to see why this insignificance was created. First, the descriptive statistics of the items are presented in table 5.12. The full SPSS output of this regression and descriptive statistics are presented in appendix J.

Perceived Effectiveness Item	*Mean*	*S.D.*
PE1	3,66	0,797
PE2	3,34	1,099
PE3	2,98	0,915
PE4	3,79	0,746

Table 5.12: Perceived Effectiveness Item Statistics

The content of the four perceived productivity items in the survey is:

PE1: If I follow the organisation's security training, I can work securely.
PE2: I can only feel that I am working securely, if everyone else is.
PE3: Security training has helped me manage unexpected and risky situations in work.
PE4: The security training provided to me, can be put into practice within my abilities.

The fourth item has highest mean, and thenceforth the second and third item. PE3 is also the only item with a mean slightly below neutral. This indicates that respondents find that they can put the security training into practice within their abilities the most and do not really feel like the security training modules are actually helping them manage risky situations in their work.

Now, in order to explain the insignificant relationship between the constructs perceived effectiveness and employee security behaviour, the separate items representing perceived effectiveness have been regressed on employee security behaviour. The values were calculated and are presented in table 5.13.

Item	*R Square Adjusted*	*Standardized Beta*	*T-value*	*P-value*	*95% Confidence*
PE1 → EB	-0,010	-0,022	-0,222	0,825	Rejected
PE2 → EB	0,007	0,132	1,314	0,192	Rejected
PE3 → EB	0,014	0,155	1,547	0,125	Rejected
PE4 → EB	0,038	0,218	2,196	0,031	Approved

Table 5.13: Results Regression Perceived Effectiveness on Employee Security Behaviour

Based on the results of this regression analysis, it can be concluded that only one of the perceived effectiveness items shows a significant relationship to employee security behaviour. Therefore, the insignificance between the perceived effectiveness construct and the employee security behaviour scale can be explained. Three items were rejected because of the high p-value and the item approved had a relatively small but positive value (β = 0,218).

Finally, the analysis of this research will be completed by analysing the relationship between the demographic variables and employee security behaviour, discussed in the next section.

5.4.11. Demographic Analysis

The overall goal of this analysis is capture if demographics have an impact on the employee security behaviour. First, the descriptive statistics of the demographic variables will be discussed. In SPSS the gender male has been coded as 2 and female as 1, that is why the mean is 1,65 (65% male). This also applies to the variables Technology Consulting, Security Related Work and Function. Age is a numerical variable, the Service Line variable has been split into four categories and Deployment Length into five categories. Table 5.14 describes the mean, standard deviation and the correlations of the demographic variables to the perceived security training and to employee security behaviour.

5.4.11.1. Descriptive Statistics

Variable	*Mean*	*SD*	*Correlation with PT*	*Correlation with EB*
Gender	1,65 (65% Male)	0,66	-0,125	-0,960
Age	32	8,75	0,242	0,136
Service Line	3,30 (Consulting)	1,453	-0,103	-0,013
Technology Consulting	1,63 (63% not)	0,49	-0,076	-0,011
Security Related Work	1,53 (53% not)	0,50	-0,092	-0,248
Function	1,34 (34% Manager, Senior Manager or Partner)	0,48	0,072	0,134
Deployment Length	2,75 (3-5 years)	0,48	-0,111	0,060

Table 5.14: Results Regression Perceived Productivity on Employee Security Behaviour

The two negative correlations with gender signify that within this sample female respondents have a better perception of the security training modules and state their behaviour as more secure. Positive correlations between age and the two variables, show that people of an age above 32 (the average) have a better perception of security training and behave more securely. Regarding respondents that are involved in security related projects and are part of the technology consulting community, their perception on training and their stated security behaviour is a little bit better than when this is not the case. In addition, the positive correlation of employee function to the variables show that employees in higher positions have better perceptions on the training modules and behave more securely than employees in an earlier function.

5.4.11.2. Regression Analysis Demographic Profile

Next to this, the demographic variables have been regressed on the security behaviour. To analyse if there is a significant relationship to consider. The results of this analysis are presented in table 5.15.

Item	R Square Adjusted	Standardized Beta	T-value	P-value	95% confidence
Gender	-0,001	-0,096	-0,946	0,346	Rejected
Age	0,008	0,136	1,348	0,181	Rejected
Service Line	-0,010	-0,013	-0,131	0,896	Rejected
Technology Consulting	-0,010	-0,011	-0,107	0,915	Rejected
Security Related	0,052	-0,248	-2,519	0,013	Approved
Function	0,008	0,134	1,335	0,185	Rejected
Deployment Length	-0,007	0,060	0,594	0,554	Rejected

Table 5.15: Results Regression Demographics and Employee Security Behaviour

The results of this regression analysis indicate a significant interaction between employees who perform security related work and their security behaviour. This relationship is however as expected,

since a negative value (yes is the lower value) defines that security focused employees state that their security behaviour is better than employees whom are not involved in security related projects.

6
Discussion

The purpose of this thesis is to gain a better understanding of the perceptions of employees on security training within their organisation and the impact of these perceptions on their security behaviour. First, an overview of the policies, security training modules and how these modules are created was gathered by conducting semi-structured interviews. This information is used in order to inform the quantitative part of the research. Overall, the cybersecurity policies are translated into WBL (Web Based Learning) modules, like Defeating Social Engineers, Incident Reporting, Password Security, Phishing, Protecting Mobile Data and Devices and Handling Information Safely. These training modules are created by the information security awareness team and the check for compliance as well as the provision of the modules is carried out by the learning team. The interview with the information security awareness team and the learning team provided input for the content of the survey statements. Additionally, the interviews provided the opportunity to consider the perspectives of the creators and deliverers of the security training in the company. On the other hand, the survey sheds light on the user perspective on security training of the organisation. Together, this thesis research project will examine where these perspectives do not align and provide recommendations to the possible improvements of security training in the organisation.

The quantitative part of this research aimed to explain the relationship between the perceptions of employees regarding security training and the impact on their behaviour. This was examined in order to see if the security policies and mechanisms are effective within the organisation. More detailed, the study aimed to reach the research objective by composing a structural equation model based on the theoretical framework created in the literature review. This structural model contained the variables perceived security training, perceived effectiveness, perceived security knowledge, perceived impact on productivity and employee security behaviour. In addition, to validate the hypotheses presented in the theoretical model, structural equation modelling in SPSS AMOS has been used to analyse the results. To perform this analysis, first a scale reliability test and confirmatory factor analysis have been carried out. The results showed that the scale for perceived security knowledge (α = 0,84), the perceived security training scale (α = 0,75), perceived effectiveness scale (α = 0,55) and also the employee security behaviour scale (α = 0,65) were significant. This indicated that the items are a good representation of the construct and can be included in the structural equation model. However, the items representing perceived impact on productivity (α = 0,38) were not significant and had to be analysed separately. Next to that, the question regarding the security training characteristics was not measured on a Likert scale and is therefore not to be included in the SEM analysis. The results to these questions have been analysed using regression separately.

Before analysing the model, the test for common method bias (20,5%) showed that the hypothesised model does not show to much common variation and the analysis could proceed. After performing the confirmatory factor analysis, to validate the reliability of the constructs and of the employee security behaviour scale, it is concluded that the employee security behaviour scale should be explored further. To achieve this, an exploratory factor analysis has been carried out. First, the factor analysis would result in four components with an eigenvalue above one. However, the reliability test showed that the removal of EB7 would result in a higher Cronbach's Alpha (α = 0,67). So, this item was deleted and the factor analysis was performed again. This resulted in a pattern matrix where the loadings had to fulfil two requirements: factor loadings should be above 0,5 and adhere to Saucier's criterion of only including an item in the scale when the loading of that item is twice as much as the loading on other components. This resulted in EB2 also to be removed from the analysis. The final exploratory factor analysis, resulted in the extraction of three components, that together explained 57,6% of variance. The components are respectively themed as Password Security (28,5% of variance), Security Aware-

ness (16,7% of variance) and Device Security (16,7% of variance). Finally, the inter-item correlations and the item-total correlations were calculated, which resulted in all the items being extensive and even 6 items being labeled as exemplary (ITC > 0,3).

All together, the estimated model contained all the indicators, except for two employee behaviour items and the perceived productivity items. In addition, the results of the model show the correlations between the variables presented in the structural equation model and the path coefficients between constructs. These results suggest a strong significant positive effect between the perceptions on training modules on the perceived effectiveness (β = 0,54) and on the policy knowledge of employees (β = 0,54). These two relationships indicate, that employees whom appreciate the training more also feel like they can effectively behave secure and have more knowledge of the policies (which are translated into the training modules). This is in line with the discussion findings in the compliance budget paper of Beautement et al. (2008), that concludes that effective training can build confidence and competence to using security systems. Further, the perceptions on the training modules showed a positive significant effect on the risk knowledge (β = 0,34), threat knowledge (β = 0,23) and overall cybersecurity knowledge (β = 0,43) of employees. Also, as predicted the security knowledge of employees show a rather high positive significant effect (β = 0,50) to the employee security behaviour. This is in line with Al Hogail (2015), who deduced a positive relationship between security knowledge and behaviour. However, the relationship between perceived effectiveness and the self-stated security behaviour resulted in an insignificant outcome and this hypotheses was therefore rejected. So, all together every hypothesis in the analysed model is supported by the SEM procedure, except for perceived effectiveness on employee self-stated security behaviour.

The second part of the analysis focused on the effect of the perceptions on training modules (defined by characteristics) on the constructs perceived effectiveness, perceived security knowledge, employee security behaviour and on the perceived productivity items. First, the distribution of the security training characteristics chosen by the respondents have been specified. Most chosen where the options informative (52,5%), easy to understand (49,5%), general (32,3%), repetitive (32,3%) and boring (30,3%). Next to that, respondents also found the security modules to be easy to apply (24,2%), time consuming (20,2%) and hard to find time for (17,2%). As mentioned in the interview, it is likely for the respondents to find the security training modules boring, time consuming and hard to find time for, since the company is not structured to provide them with 'free' time to complete these modules. Additionally, the fact that the modules probably provide interesting information but not in an engaging way (like for instance a security game would do). The information security awareness team spends a lot of time picking topics and building the training modules, to provide all employees with educational security information. This could therefore be the reason that participants identify the modules to be informative. In addition, the participants find the security training modules easy to understand, this can be explained by the security training being the same for all employees within the organisation and not differ per target group (as said in the interview). Subsequently, this will have impact of the specificity of the training and for that reason general has been chosen by respondents more than specific. Next to that, the mandatory security training modules get repeated every year, as mentioned in section 5.3, therefore it is likely for respondents to find the training repetitive. In addition, interesting but explainable is that entertaining and difficult to understand were not chosen. In the interviews, it appeared that most employees found security training to be boring, so not entertaining and since the training is distributed company wide, the modules should be easy to understand.

Now, the combinations of chosen security training characteristics have been analysed, to get a general view of how the respondents perceive security training in their organisation. The multiple response set was evaluated by utilising cross-tabulation in SPSS. This resulted in the finding, that overall respondents who chose one positive characteristic, would also choose the other two options to be positive. This also applied to the negative aspects of the security training, whom were mostly combined with other negative characteristics. An interesting combination of characteristics, that is corresponding with the results of the interview, is the combination between hard to find time for and informative. Employees know that the security training is necessary for the safety of their company and the information security awareness team invests a lot of time and thought into the content of the training for it to be informative. However, the structure of the company does not allow employees to complete the all the

training during working hours. This aligns with the perspective in the productivity paper of Beautement et al. (2016), where individuals know the benefits to the company of behaving securely, but find the costs of compliance to be higher than these benefits acquired.

Next to this, the correlations of the chosen training characteristics to the constructs perceived effectiveness, perceived security knowledge, employee security behaviour and the perceived impact on productivity items have been analysed. As expected, informative, easy to understand, relevant and visual showed a positive correlation to the perceived effectiveness variable. On the contrary, time consuming, general, boring and hard to find time for, negatively effected the perceived effectiveness of employees. Further, the security knowledge of employees was positively correlated to easy to understand and negatively to security modules being time consuming and text-heavy. Importantly, employee security behaviour is negatively impacted by the security modules being time consuming and text-heavy. Moreover, training modules that are perceived as easy to understand, increase the feeling that behaving securely takes an appropriate amount of time. Where on the other hand the repetitive nature of the training modules has a negative impact on the second productivity item. This is incoherence with security training modules having to be repeated annually, as mentioned in the interview. Lastly, training modules being perceived as text-heavy and time consuming, having a negative impact on the efficiency of employees in completing their work. This is also discussed in the interview with the learning department. Since, employees don't find like they have the time to complete the modules and have the feeling that the performance of their daily work will reduce when completing training during working hours. This contributes to the employee behaviour towards compliance as described by Beautement et al. (2016), where security mechanisms and policies that interfere their primary tasks and reduce productivity are perceived as 'more time wasted by security'.

Besides, the items for the perceived impact on productivity construct were regressed on the employee security behaviour. This analysis revealed that two items of perceived productivity (PR2: β = 0,23, PR3: β = 0,33) had a relatively small, but positive effect on the employee security behaviour. This shows that respondents whom feel like behaving securely takes an appropriate amount of time and think that the security training does not reduce the efficiency of their work, state their behaviour to be more secure. On the other hand, one of the items showed an insignificant relationship (p = 0,75) to the employee security behaviour and was therefore rejected.

Due to the relationship between perceived effectiveness and employee security behaviour being insignificant, this insignificance was explored by performing a regression analysis per perceived effectiveness item. The results of the regression analysis explained the insignificance of the relationship between the two constructs. Specifically, only one of the four perceived effectiveness items showed a significant relationship to employee security behaviour. This relationship entails a small positive effect between the ability of an employee to put security training into practice and their security behaviour. Together, the insignificance of the other three items explains why the relationship of the whole construct to employee security behaviour was not significant.

Finally, the demographic variables were regressed on the employee security behaviour construct. The choice to include this regression is due to, as mentioned in the literature review, other research show significant relationships between demographics and security behaviour. The descriptive statistics showed that within this response set, females perceive the security training to be better and state that they behave more securely. This is in line with the study by McCormac et al. (2017), that reveals a small significant favourable difference for females in behaving securely. Further, the demographic analysis showed that overall employees with an age between 25 and 35 perceive the security training to be better and behave more securely. This aligns to the findings by Beautement et al. (2016), who found that young employees (25-34) rely more on the organisations security structures than older employees. For the respondents that are involved in security related projects and the technology consulting community, their perception on security training and their stated security behaviour is a little bit better than when this is not the case. In addition, the positive correlation of employee function show that employees in higher positions have better perceptions on the security training modules and state their behaviour to be more secure than employees in an earlier functions. However, only one of the seven demographic variables, when regressed on employee security behaviour, showed a relationship of significant nature.

Particularly, when employees are involved in security related projects they state their behaviour to be more secure.

7 Conclusion and Recommendations

7.1. Conclusion

Utilising a combination of qualitative and quantitative research techniques, this study was aimed at exploring the perceptions of employees on security training and the impact of that perception on their security behaviour within an organisational context. This study has been conducted in a global Professional Services Firm and included their employees, their information security awareness team, learning team and the security training modules provided by the company. The research question to be answered is:

How do employees perceive the security training of their organisation and what is the impact of that perception on their security behaviour?

To answer this question, the relationships between the variables within the theoretical framework have been analysed and will be explained based on figure 7.1.

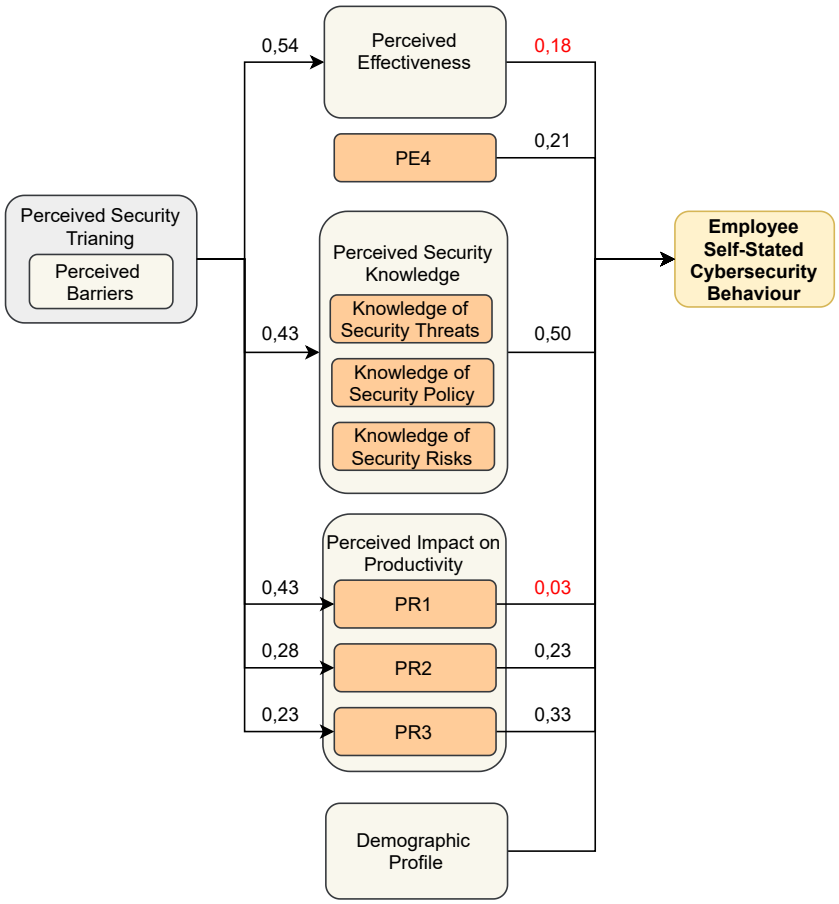

Figure 7.1: Theoretical Framework with Values

First of all, the results of the analysis confirmed a strong positive relationship (0,54) between the perceptions to security training and perceived effectiveness of employees. Employees whom perceive the security training modules to be informative, easy to understand and visual, have the feeling that they can work securely and put the training into practice within their abilities. The other relationship revealed that perceptions of security training are positively related (0,43) to the security knowledge (mainly policy knowledge) and this knowledge also has a relatively big positive relationship (0,50) with employee security behaviour. This indicates that when employees are positive towards the security training, they gain more security knowledge and especially policy knowledge (this makes sense, since the policies are translated into the security training modules) and state their behaviour to be more secure. Aligning to the findings of Al Hogail (2015), who found a positive relationship between security knowledge and security behaviour. This knowledge can however also indicate that employees know the policies and are aware of the expected security behaviour, but in reality do not perform this behaviour. This is a risk introduced by measuring self-stated behaviour and perceptions, that will be explained in the limitations section.

Within the perceived security training construct, some specific characteristics of security training and the relationship to the other constructs have been analysed. This resulted in the conclusion that employees who find security modules informative and easy to understand also perceive security training as effective within the company. On the other hand, employees find training modules time consuming, irrelevant and hard to find time for, which reduces the effectiveness of security training. The security behaviour of employees is negatively impacted by security training being text-heavy and time consuming. In addition, the impact of the training modules on productivity showed that mainly because employees find training time consuming and including a lot of text, they feel like security training reduces their efficiency in completing their work. Further, employees perceive the training to be irrelevant and therefore do not think that behaving securely takes an appropriate amount of time.

Next to this, the analysis confirmed that employees either have a general positive view of the security training or a negative one. The only opposite combination, that has been chosen often by employees, is the combination between informative and hard to find time for. As the learning team explained in the interview, employees do not have time to complete security training even though they are eager to learn more and know the security risks to their organisation. This is in line with the conclusion of the compliance budget paper by Beautement et al. (2008), that indicates the costs of compliance to be higher than the benefits gained in terms of security.

Further, this research project aimed to analyse the perceived impact of security training on the productivity of employees. Additionally, how this relates to their perceptions on security training and how the impact on productivity influences their security behaviour. The first interaction analysed is between the perceived security training and PR1 (0,43). This defines the interaction of good perceptions on security training on the feeling that hours spend on security training are reasonable. Next to that, these perceptions also positively relate to PR2 (0,28) and PR3 (0,23). Showing a positive interaction to the feeling that behaving securely takes an appropriate amount of time and does not reduce employees their efficiency in completing their work. From this it can be concluded, that good training (as perceived by respondents) can make the time spend on training feel reasonable.

Additionally, this resulted in the outcome that when behaving securely takes an appropriate amount of time, the security behaviour of employees will increase slightly (0,23). Next to that, a positive interaction (0,33) was revealed between the feeling of employees to be able to work efficiently and their security behaviour. This indicates that employees find it important that their work efficiency is not impacted by security training and will behave more securely if they feel like their efficiency is not reduced. This is supported by the findings in the paper by Kirlappos et al. (2014), whom stated that employees are motivated to secure the organisation if this does not take an unreasonable amount of time and does not demand to much effort.

Also, an insignificant interaction that resulted from the structural equation model, was between perceived effectiveness and employee security behaviour. However, through linear regression this insignificance could be explained. Since, three of the four items did not show a significant relationship. Only the feeling of employees that they can put the training into practice within their abilities showed a small positive interaction (0,21) to their security behaviour.

Lastly, the demographic analysis resulted in negative correlations between gender and perceptions of security training and their security behaviour. This indicates that in this sample female respondents have a better perception of security training and state to behave more secure. Positive correlations between age and these two constructs, show that people of an age above 32 (the average) have a better perception of security training and behave more securely. For the respondents that are involved in security related projects and are part of the technology consulting community, their perception on training and their stated security behaviour is a bit higher than when this is not the case. In addition, the positive correlation of employee function to the variables, show that employees in higher positions have a better perception of security training and state to be behaving more secure than employees in an earlier functions. Finally, employees who are involved in security related projects, state their behaviour to be more secure than employees whom are not. This can be related to their more advanced cybersecurity knowledge and better understanding of the policies they are expected to adhere to and how to put these policies into practice.

Together, the two most apparent interactions show, that first of all well designed training can increase the feeling for employees that secure behaviour is effective. Also, well designed training enhances the perception that employees can work securely and that they can put training into practice within their abilities. The feeling that training can be put into practice, reinforces the security behaviour of employees. Secondly, the security knowledge of employees is an important stimulant for their security behaviour, especially policy knowledge. Employees can only pick up this knowledge when security training is designed in such a way that it is informative, easy to apply and when they have time to complete this training. The time spend on training tailors back to the productivity of employees, where pressure on their primary tasks is causing them to be less eager to engage in security and be compliant.

7.2. Recommendations

The takeaway from this research is, first of all the perception of employees on security training of their organisation is either generally positive or negative. That perception of security training impacts employees their effectiveness, security knowledge, productivity and security behaviour. Where employees whom perceive training modules to be time consuming, hard to find time for and boring are also not feeling like they can be productive, do not see the training as effective, have less security knowledge and behave less secure. On the other hand, good perceptions on the training have a positive effect on all of these factors.

As stated in the interview with the information security awareness team, the security training is created by the global team and is aimed to train every employee within the organisation. This team refreshes the training every year and spends time and effort in perfecting the content and topics of the training. However, because the training is created for all employees, the content should be understandable for every single employee. This causes the security training to feel general and for some employees even to be irrelevant. Mainly because some of the employees already know the largest part of the content (like the cybersecurity team). To address this problem, it is recommended for the company to look into specifying the training content per target group and creating training that is role-based instead of general and relatively easy. The targeting of security training contributes to the conclusion drawn by Beautement et al. (2016). This research found that providing security interventions targeted to groups, will free employees of being included in training that is not needed for them and having to determine if the training even applies to them.

In terms of creating training that is more specific, the constructs of this research can be used as a vision line to improve security training. Where training can be made more effective, by redesigning it into the limitations that appeared. For instance, some employees find security training informative and easy to understand, but still feel like they are not able to put the training into practice. Redesigning training to be easy to put into practice and help employees manage unexpected and risky situations, will improve the perceived effectiveness of employees. Also, recommended when redesigning training is to not add extra training hours, but to make the training fit within busy working situations. This will give employees the feeling that they spend an appropriate amount of time on training and can work efficiently, which will improve their perceived productivity.

Next to that, the security awareness team devotes plenty of time to the design of security training. The content of the security training is therefore mostly perceived as informative. However, the time spend on completing security training should not effect employees their work (the cost of compliance should not be higher than the benefits gained) (Beautement et al., 2008). The interview with the learning team showed that the application contains technical glitches. Technical glitches, as they are called, are still occurring too often. It is recommended to make sure that things run smoothly and to make the application more user-friendly. The system should make the training at least easy to follow and not make it even more of a burden. This contributes to the recommendation to honour the commitment of employees to security training and helping them, instead of making them jump through hoops. In addition, since the global team creates the training and manages the learning application, it should be possible to provide the global team with feedback on security training. It is recommended to introduce a good feedback loop, not only between the learning team and global, but also for employees separately. So, employees do not feel unheard or far away from the team creating the training for them.

Also, the employees find security training time consuming, hard to find time for and boring and this impacts their productivity and belief in the effectiveness of security training. The training should support these aspects and not lower them. That's why it is really important to address the fact that employees do not feel like they have time to complete the training. Likewise Kirlappos et al. (2014) approaches barriers to compliance, by managing security in a way that it fits into the work activities of users and use a more participative approach. An important aspect, also discussed with the learning team, is the fact that employees are very busy and are likely to have to complete the training in their spare time. Mostly caused by training hours reducing the productivity of employees and employees already spending a full work week on their normal day-to-day tasks. Completing the training in spare time is not having a positive impact on the effectiveness of the security training and reduces the security knowledge and secure behaviour of employees. It is therefore recommended to find a solution where employees are provided with time to complete security training within working hours, without putting pressure on their work productivity. In addition, as extra motivation, rewards could be introduced for employees who reach the highest security training score within a team or overall behave the most secure (based on clicking on phishing links or reporting suspicious emails).

Another recommendation would be for the organisation to be very clear and transparent about the rules regarding security procedures and hours expected to be spend on learning. Make sure that every employee knows from the moment they start, why they are completing the training and when they are expected to do this. By introducing hours to complete the modules and rewarding those who complete training sooner/better, the training perceptions will increase and therefore the effectiveness of security training, the security knowledge, productivity and the security behaviour of employees will also increase.

8
Limitations and Future Work

8.1. Limitations

First of all, the most important limitation in a study of this nature, is the measurement of employee security behaviour. Behaviour is a concept which is extremely hard to measure and research is lacking in this area. Mainly, because of the gap between people having the intention to act a kind of way and actually behaving in a certain way. Important is to see why this behaviour exists and what the factors are that influence intentions and behaviour the most in this particular organisational context. The information security awareness team of the company also mentioned, that the most challenging task for them is the measurement of employee security behaviour. They mostly try to capture this behaviour by technical measures, like the amount of money spend on cybersecurity or hits on yammer posts and clicks on phishing links. However, it is unclear what you are exactly measuring when using these technical measures. Is this representative for day-to-day work and makes this that employees understand and live the policy?

Next to this behaviour, the perceptions of employees regarding their effectiveness, productivity, knowledge and security training of the organisation are measured and correlations between these opinions are analysed. When using perceptions in a survey, the measurements do not objectively define the constructs. This is caused by perceptions being subjective and employees having different mental states and perceiving situations each in a certain way. During the gathering of perceptions, the trustworthiness of outcomes can be constrained by different cultural, social, historical and political factors. There is no 'perfect way' of performing a perception study, due to their complex nature. However, when explicitly discussing the design choices and translating research goals into the design, perception studies can provide the opportunity to capture extra value on studying specific problems (DeCamp, Enumah, O'Neill, & Sugarman, 2014). This thesis project captures opinions of employees regarding security training and correlations between these opinions and their security behaviour.

In addition, the theoretical framework and model to be analysed is created based on information gathered from the literature review. Hypotheses are stated and relationships are predicted to be tested within the analysed model. However, there can be extra factors influencing the variables in this framework and other relationships that are also interesting to research. Although, due to defining a scope to the research and time constraints of a thesis project, only the hypotheses in chapter two are tested and no extra factors or effects are analysed.

Next to this, a limitation to this study is the fact that it is conducted within one global Financial Services Firm and focuses solely on their security training modules and employees. Therefore, the results can be generalised to similar competition driven services organisations like this, but will not be applicable to small companies. They won't have all these different service lines, cultures and a global team creating security training for a big amount of employees.

Also, a major part of the respondents was male, between the age of 25 and 35 and part of the service line consulting. While the age group is accounted for by the type of organisation, the gender and service line are not equally distributed among respondents. However, a demographic analysis was only performed to compare the responses to previous research and was not a major part of the analysis. A larger and better representative sample, results in outcomes with a better representation for the organisation itself.

Concerning the data collection, the items representing the construct perceived productivity could have been designed better. Since, now they did not reach an internal reliability to significantly represent this construct. A higher quantity of productivity items could have been a good improvement for the design of the survey. Next to that, three items of the perceived effectiveness construct showed an insignificant relationship to employee security behaviour. While other variables revealed high significant relationships to this construct. The separate connections between the perceived effectiveness items and the behaviour items could have been improved.

8.2. Future Work

This research project was conducted within a global Professional Services Firm and the survey was distributed amongst their employees within different departments in the Netherlands. Therefore, performing this study within other similar organisations, could enhance the generalisability of the results. Interesting would be to perform this study in similar organisations within the Netherlands and compare the outcomes. Also, performing the research in the other countries where this specific services organisation operates, could provide perspective on how different cultures impact the perceptions of employees on security training and their security behaviour.

Also, security training is not the only training provided by the organisation. Therefore, in future work, it would be interesting to study the perceptions on other training modules and compare the outcomes to the perceptions on the security training modules. This can then be done likewise within different countries, similar companies and compared between those.

Future research could also extend the theoretical framework, by including extra contextual factors and analysing all interdependencies. In this study, the conceptual framework predicts certain relationships, which are tested and explained. This does not mean that other relationships are not of relevance.

9 Case Description

9.1. Organisation

The company is an internationally operating service company active in the field of assurance, tax advice and consulting. The company is an international alliance of local member firms. Based in London, the headquarters ensures unity in the policies of all member firms and monitors the quality of service. This global headquarter does not provide services to clients, the member firms do.

The mission of the company is to help digital pioneers in a fast changing world in their protection of data privacy, help governments in cash-flow crises, use data analytics to unravel new medical treatments and together provide high quality audits to generate trust in the financial business and markets. In short, solving critical challenges by working together with companies, entrepreneurs and countries as a whole.

Via the four integrated services lines together with deep sector knowledge, the organisation assists their clients to exploit new possibilities and assess and manage risk to reach effective growth. The teams are multidisciplinary and high-performing, in order to help clients comply to regulatory requirements, inform investors and together match stakeholder needs.

9.1.1. Organisational Structure

An organisation is a collaboration of people. In fact, it is the people who determine the performance of an organisation. This indicated the importance to consider how people interact with each other; in this context studies speak of the culture in an organisation. This is not so much about the formal side of things, but rather the informal side. In this context is referred to the so-called soft controls. One concept that makes sense is identity, especially corporate identity or corporate culture. Today, more and more organisations are using their corporate identity to distinguish themselves from the competition.

It was Quinn and Cameron (1999) in particular who elaborated on this pursuit of an organisational culture. They describe the culture from an integration perspective, which is about achieving a unity culture with shared values and norms. The power of culture lies mainly in its ability to bring people together, along with the ability to prevent fragmentation as much as possible. A homogeneous, consistent and comprehensive organisational culture optimises mutual communication. Half a word is often enough and it takes little time to come to an agreement with each other about the situation people are facing at that moment. Quinn and Cameron distinguish the following four typologies of cultures:

- The family culture
- The adhocracy
- The hierarchical culture
- The market culture

The company where this research is conducted is a typical example of a market culture. Namely, this culture was incorporated as competition became more and more important. Oliver Williamson and Bill Ouchi in particular found the functioning of an organisation comparable to the functioning of the market. As with the market, a lot of attention is paid to what happens outside the organisation. The result is a result-oriented working environment. The leaders are adamant producers and competitors. They are tough and demanding. The binding agent that holds the organisation together is the emphasis on winning. The long-term concerns are competitive action and the achievement of ambitious goals. Success is defined in terms of market share and market penetration. Leaving the competitor behind and becoming the market leader is the most important.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248.

ACAPS, M. (2012). Qualitative and quantitative. research techniques for humanitarian needs assessment. an introductory brief.

Aguirre-Urreta, M. I., & Hu, J. (2019). Detecting common method bias: Performance of the harman's single-factor test. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *50*(2), 45–70.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of applied social psychology*, *32*(4), 665–683.

Al Hogail, A. (2015). Cultivating and assessing an organizational information security culture; an empirical study. *International Journal of Security and Its Applications*, *9*(7), 163–178.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, *29*(4), 432–445.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 ieee international conference on teaching, assessment, and learning for engineering (tale)* (pp. 62–68). IEEE.

Anderson, C. (2005). Creating conscientious cybercitizen: An examination of home computer user attitudes and intentions towards security. In *Conference on information systems technology (cist)/informs, san francisco, california*.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Ardichvili, A., Page, V., & Wentling, T. (2013). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of knowledge management*.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth symposium on usable privacy and security ({soups} 2016)* (pp. 253–270).

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop* (pp. 47–58).

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61.

Benabou, R., & Tirole, J. (2003). Intrinsic and extrinsic motivation. *The review of economic studies*, *70*(3), 489–520.

Blasch, E., Sabatini, R., Roy, A., Kramer, K. A., Andrew, G., Schmidt, G. T., … Fasano, G. (2019). Cyber awareness trends in avionics. In *2019 ieee/aiaa 38th digital avionics systems conference (dasc)* (pp. 1–8). IEEE.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh symposium on usable privacy and security ({soups} 2015)* (pp. 103–122).

Brown, T. A., & Moore, M. T. (2012). Confirmatory factor analysis. *Handbook of structural equation modeling*, 361–379.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523–548.

Chan, M., Woon, I., & Kankanhalli, A. (2015). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of information privacy and security*, *1*(3), 18–41.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of is security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31.

Coyle, J., & Williams, B. (2011). An exploration of the epistemological intricacies of using qualitative data to develop a quantitative measure of user views of health care. *Journal of Advanced Nursing*, *31*(5), 1235–1243.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Culnan, M. (2014). Bentley survey on consumers and internet security: Summary of findings. *available at:[WWW document] http://legacy. bentley. edu/events/iscw2004/survey_findings. pdf (accessed 19 May 2012)*.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1997). Toward a stewardship theory of management. *Academy of Management review*, *22*(1), 20–47.

DeCamp, M., Enumah, S., O'Neill, D., & Sugarman, J. (2014). Perceptions of a short-term medical programme in the dominican republic: Voices of care recipients. *Global public health*, *9*(4), 411–425.

Dudwick, N., Kuehnast, K., Jones, V. N., & Woolcock, M. (2006). Analyzing social capital in context. *A guide to using qualitative methods and data*, 1–46.

Eckstein, H. (2000). Case study and theory in political science. *Case study method*, 119–164.

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

Everitt, B., & Skrondal, A. (2002). *The cambridge dictionary of statistics*. Cambridge University Press Cambridge.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological methods*, *4*(3), 272.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. In *2015 ieee trustcom/bigdatase/ispa* (Vol. 1, pp. 352–359). IEEE.

Farooq, R., & Shankar, R. (2016). Role of structural equation modeling in scale development. *Journal of Advances in Management Research*.

Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief. Congressional Research Service.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242–251.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2010). Multivariate data analysis upper saddle river: Pearson prentice hall. *Links*.

Hentea, M. (2015). A perspective on achieving information security awareness. *Issues in Informing Science & Information Technology*, *2*.

Hight, S. D. (2005). The importance of a security, education, training and awareness program, november 2005. *Security*, *27601*, 1–5.

Hodkinson, P., & Hodkinson, H. (2001). The strengths and limitations of case study research. In *Learning and skills development agency conference at cambridge* (Vol. 1, pp. 5–7).

Humaidi, N., & Balakrishnan, V. (2015). The moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science*, *28*(2), 70–92.

Hurmerinta-Peltomäki, L., & Nummela, N. (2016). Mixed methods in international business research: A value-added perspective. *Management International Review*, *46*(4), 439–459.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

ISF. (2007). The standard of good practice for information security. *Security Standard*.

ISO Central Secretary. (2016). *Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) – Part 1: Overview* (Standard No. ISO/IEC TR 29110-1:2016). International Organization for Standardization. Geneva, CH. Retrieved from https://www.iso.org/standard/62711.html

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on sme. In *2013 international conference on research and innovation in information systems (icriis)* (pp. 286–290). IEEE.

Kelly, A. P. (2011). Social research methods. *London: London School of Economics and Political Science*.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "shadow security": Why understanding non-compliance provides the basis for effective security.

Kohn, A. (1993). Why incentive plans cannot work. SUBSCRIBER SERVICE, PO BOX 52623, BOULDER, CO 80322-2623.

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1-3), 72–77.

Kumaraguru, P., Cranshaw, J., Acquisti, R., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). A real-word evaluation of anti-phishing training.

Li, Y., Pan, T., & Zhang, N. A. (2019). From hindrance to challenge. *Journal of Enterprise Information Management*.

Liang, H., Xue, Y. L. et al. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 1.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433–463.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of retailing*, *88*(4), 542–555.

Mahfuth, A. A. A. (2020). *An investigation on the relationship between security knowledge constructs and employee behaviour in organisations* (Doctoral dissertation).

Marett, K., Biros, D. P., & Knode, M. L. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. In *International conference on intelligence and security informatics* (pp. 187–200). Springer.

Mason, J. (2017). *Qualitative researching*. Sage.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156.

McKinley, R. K., Manku-Scott, T., Hastings, A. M., French, D. P., & Baker, R. (1997). Reliability and validity of a new measure of patient satisfaction with out of hours primary medical care in the united kingdom: Development of a patient questionnaire. *Bmj*, *314*(7075), 193.

McLennan, M. (2021). The global risks report 2021 16th edition.

Mishra, S., & Dhillon, G. (2016). Information systems security governance research: A behavioral perspective. In *1st annual symposium on information assurance, academic track of 9th annual nys cyber security conference* (pp. 27–35). ACSAC New York, USA.

Mohamad Rashid, R., Zakaria, O., & Nabil Zulhemay, M. (2013). The raltionship of information security knowledge (isk) and human factors, challenges and solution. *Journal of Theoretical & Applied Information Technology*, *57*(1).

national institute of standards, & technology. (2013). *Security and privacy controls for federal information systems and organizations* (tech. rep. No. NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015). doi:10.6028/NIST.SP.800-53r4

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review*, *79*(6), 895–904.

O'Cathain, A., Murphy, E., & Nicholl, J. (2010). Three techniques for integrating data in mixed methods studies. *Bmj*, *341*.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards is security policy compliance. In *2007 40th annual hawaii international conference on system sciences (hicss'07)* (156b–156b). IEEE.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (hais-q): Two further validation studies. *Computers & Security*, *66*, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & security*, *42*, 165–176.

Peković, J., Zdravković, S., & Pavlović, G. (2019). Social media influencers as a predictor of consumer intentions. *Marketing*, *50*(3), 207–216.

Pinnock, H., Huby, G., Powell, A., Kielmann, T., Price, D., Williams, S., … Sheikh, A. (2008). The process of planning, development and implementation of a general practitioner with a special interest service in primary care organisations in england and wales: A comparative prospective case study. *Report for the National Co-ordinating Centre for NHS Service Delivery and Organisation R&D (NCCSDO)*.

Ponnusamy, V., Selvam, L. M. P., & Rafique, K. (2020). Cybersecurity governance on social engineering awareness. In *Employing recent technologies for improved digital governance* (pp. 210–236). IGI Global.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management*, *51*(5), 551–567.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace. *Human factors*, *57*(5), 721–727.

Qin, T., & Burgoon, J. K. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *2007 ieee intelligence and security informatics* (pp. 152–159). IEEE.

Quinn, R. E., & Cameron, K. S. (1999). *Onderzoeken en veranderen van organisatiecultuur: Gebaseerd op het model van de concurrerende waarden*. Academic Service economie en bedrijfskunde.

Rainie, L., Anders, J., & Connolly, J. (2014). Cyber attacks likely to increase. *Digital Life in*, *2025*.

Rheea, H.-S., Kimb, C., & Ryuc, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *computers & security*, *28*(8), 816–826.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93–114.

Rosenstock, I. M. (2015). Why people use health services. *The Milbank Quarterly*, *83*(4).

Russell, J. D., Weems, C. F., Ahmed, I., & Richard III, G. G. (2017). Self-reported secure and insecure cyber behaviour: Factor structure and associations with personality factors. *Journal of Cyber Security Technology*, *1*(3-4), 163–174.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70–82.

Sallai, G. (2016). Social engineering audit and security awareness programme. *KPMG: Amstelveen, The Netherlands*.

Sasse, A. (2015). Scaring and bullying people into security won't work. *IEEE Security & Privacy*, *13*(3), 80–83.

Saucier, G. (1994). Mini-markers: A brief version of goldberg's unipolar big-five markers. *Journal of personality assessment*, *63*(3), 506–516.

Schneier, B. (2015). *Secrets and lies: Digital security in a networked world*. John Wiley & Sons.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100.

Sheikh, A., Cornford, T., Barber, N., Avery, A., Takian, A., Lichtner, V., … Robertson, A., et al. (2011). Implementation and adoption of nationwide electronic health records in secondary care in england: Final qualitative results from prospective national evaluation in "early adopter" hospitals. *Bmj*, *343*.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 373–382).

Stake, R. E. (1995). *The art of case study research*. sage.

Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. *AMCIS 2004 proceedings*, 175.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97–102.

Woon, I. M., & Kankanhalli, A. (2007). Investigation of is professionals' intention to practise secure development of applications. *International Journal of Human-Computer Studies*, *65*(1), 29–41.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315–331.

Yauch, C. A., & Steudel, H. J. (2013). Complementary use of qualitative and quantitative cultural assessment methods. *Organizational research methods*, *6*(4), 465–481.

Yin, R. K. (1998). The abridged version of case study research: Design and method.

Yin, R. K. et al. (2003). Design and methods. *Case study research*, *3*.

Yin, R. K. (2012). Case study methods.

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321–332.

Yuryna Connolly, A., Lang, M., Gathegi, J., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information and Computer Security*, *25*(2), 118–136.

A

Interview Information Security Awareness Team

Subject	Question and answer
Cyberawareness practices	*When talking about cybersecurity awareness among employees of your company, what are the practices your team is involved in?* • Managing the whole cybersecurity program: providing campaigns, infographics and yammer posts. • Creating the WBL's (Web-Based Learning's) content based on hot topics. • Analysing data and actual phishing. • Ambassador program, to get volunteers to distribute the material that is created from awareness. Sending within teams, creating events across all locations. The volunteers take some of their daily activities on helping the team promote their awareness programs.
Cybersecurity training	*When you create a cyber awareness training, what design phases do you typically go through?* First step is to define the topic of the WBL: • Consider feedback of different internal organisations, for instance: investigations, core reported incidents, leadership assessments, management assessments on current issues in the market. External situations. Review reports on the most common breaches, most hot topics. • Industry trends are also used, a lot of materials and presentations are based on what is happening. We are talking about personal email, working at home related to the COVID. Working securely from home is also a mandatory WBL at this moment, during a pandemic it is important to reinforce that. Adapt awareness around the new situation to working from home, more distractions at home and home responsibilities. • Check what's happening inside the organisation and outside the organisation.
Cybersecurity training	Create a proposal with those topics: • Use an external vendor, review their catalog according to the catalog we want to pursue. • ToC approval, to approve the proposal (phishing WBL to increase phishing awareness, create a proposal, included is the objective of the WBL, which are the governed risks within the company, what are the benefits of completing the WBL) • Two kind of proposals: 1. For all employees, mandatory 2. Role-based WBL proposals (Changed every year, to focus on different people or areas) • Propose the WBL to leadership. • Once it is approved, everything starts moving. Very slow, but in the end it gets implemented in in the learning application.
Relation to policy	*How do the training modules map to the cybersecurity policies?* • The vendor has a basic content, very-high level, which we review. We start editing the text considering the organisations policies. • First thing they do, is to validate the training against company policy.

Cybersecurity training	*What are the most important factors in raising security awareness training* Raising security awareness throughout the years, quarterly campaigns to raise awareness. Themed instead of topic driven, in order to combine multiple topics into one theme. For example, security awareness for the ages. Different topics for different ages, like senior vs kids. Collecting metrics on these topics, to help to analyse and find gaps and get more awareness on these gaps. The awareness is still quite new, for us it comes in three stages. 1. Statistical, any numbers to be collected. Collecting everything they can, like how many yammer posts, how many views, BeAware hits. 2. Assumption, based on this metrics it can be assumed what is going on. Like people are more interested in phishing or have more knowledge on another topic. 3. Holy grail: Behaviour change metrics, really hard to prove. For these kind of metrics, they work together with the cyber defence team. By analysing their logs and based of the things they perform themselves, like the campaigns, trainings, mandatory trainings, they can see if there are changes in behaviour. Like are employees falling for phishing links, then the campaigns are not working or the other way around.
Cybersecurity training	*Do you use your own knowledge when creating these modules or are there certain standards you have to adhere to when creating the trainings?* • The cybersecurity policy information is used as a standard to get into the vendors catalog. We then use the catalog of the vendor to fill this in further, according to the selected topic. • After that the training will be checked by technical stakeholders and will be changed according to their feedback.
Cybersecurity training	*Do you create different trainings for different target groups, or do you have one training set for all employees?* • There is mandatory training for all employees . • There is also role-based training based on different people and areas.
Training evaluation	*How do you evaluate your cybersecurity trainings?* • We share data analysis with stakeholders that we have from different groups, like risk management, global organisations. Technical stakeholders can provide their feedback, the team is not technical. Meetings to discuss to see if they agree or not, all the necessary and minor changes to align to the policies and get stakeholders feedback for 100% review. Then the training goes back to the vendor for customisation. • Employee assessments after all the campaigns and trainings, like questionnaires and surveys, to see if what they are doing is actually working and if they are reading it. • Tools to measure employee behaviour, analysing logs. Money or revenue, if EY is spending more money on combatting security risks than the awareness practices are likely not to be working and if they are spending less money than the security awareness practices are working. Harder in big companies to get measurements, since the awareness team doesn't have access to all logs and technical checks due to confidentiality. In smaller companies IT people have access to almost all data.
Re-occurence of training	*How often do employees have to complete cyber awareness training, do they only do this when they get started or do they have to repeat this after a certain time? (Do you think this should be done more often by employees?)* • Annual WBL's are to be completed every year Employees have 60 dates to complete it. • Other optional WBL's, whom aren't assigned, that employees can do themselves. • There are 5 WBL's for new joiners, when they come aboard. • Current employees, we assign annual WBL's to be completed in 60 days. • No refresher WBL's up to now, but the idea is that we work all together with the team to refresh topics. • Infographics, campaigns and yammer post to refresh all the topics throughout the year. Information on the Be.Aware page.

Training expectations	*How do you expect employees to adapt the training in their day-to-day activities?* • The main purpose is to change the security behaviour of employees. The WBL is created and the idea is to refresh all the content and create a security mindset. • Short WBL's to keep people engaged and not get them bored. • Different ways of sharing information to keep employees interested, some might hate trainings but like the yammer posts. • There is no one size fit's all in security awareness, so any angle they can use they grab to make sure the awareness increases amongst all employees.

Table A.1: Transcribed Interview Results Information Security Awareness Team

B

Interview Learning Team

Subject	Question and answer
Performance/Compliance activities	*What are the activities that your team is involved in regarding the compliance and performance of employees with respect to the learning modules?* • The learning team is involved in the deployment of training modules and making sure everyone is compliant to global policy.
Compliance	*What does it mean when an employee is compliant?* • Overall people have to reach an amount of 120 points in three years, to be able to be compliant to global policy. First requirement is to comply to this global CE policy. This is split in technical and non-technical sections, for assurance there are also some mandatory learnings included for all employees. • There is a global policy and a policy that applies to accountants and tax consultants. So, a regional and a global policy, everyone has to comply to the global policy. There are multiple policies involved, whom are different for each target group. Cybersecurity in this case is for everyone, so will be applicable to all target audiences.
Measure of performance	*How do you measure performance?* • People get points, called CE points, these are learning points. These points are based on the time spent on learning and the performance during the training. Points are inserted in their learning management system, based on participation registration these points are monitored. This is mostly done by the system itself, by the attendance based registration tool. Where every time unit is translated into a learning point.
Perceived measure of performance	*Do you think that the performance measured by the learning application is a good indication of actual performance?* 1. Not really, often employees complete the learning module and write down their answers and then do it again focusing on the questions they didn't know for sure. Since, when you try again you get exactly the same set of questions as before. This means that they just want to get it done and are not really paying attention to the content of the training and therefore the performance measurement will not be a good indication of actual performance.

Compliance	*What happens when employees do not comply/do not complete the modules?* • When employees do not comply/do not reach the 120 points within three years, their service lines will be addressed by global. People are obliged to be 100% compliant. The service lines will monitor this closely and make sure that their people reach the points required. • It is not the case that people get accused on this, but Global monitors the learning team closely to make sure the points are fetched. So, you make sure that you get the points required. • In practice, for accountants and tax advisors there is the risk that they are not allowed to exercise their profession any longer. • The learning team is responsible for deployment of the security training and not directly for measuring compliance. So, measuring this compliance is the responsibility of the service lines themselves and the stakeholders involved. They just make sure that the training modules are provided, however they support the services lines by providing them with the data to see where they are at and by sending people reminders etc. But the real responsibility is embedded in the service lines.
Compliance	*When are employees expected to complete their training modules and does this affect their productivity?* Employees can either do their learnings during working hours or in their spare time if working hours won't allow it. Everyone in the business has to reach their productivity of work, so how you make it work doesn't matter as long as you do. So employees just make sure that they complete the 120 hours. Still it is a combination, employees have to learn and that is included in the plan. Ofcourse, the plan takes into account the productivity of employees and does not want to lower this. So, not all learning will be done in spare time, however there are a lot of training modules available. The service lines indicate that they don't want their people spending too much time on these learnings, because for one it takes time in productivity of employees and secondly every training costs money which the learning department will collect from the service lines.
Perceived compliance impact	*What do you think employees think of this way of receiving learning and receiving rewards?* • Annual WBL's are to be completed every year Employees have 60 dates to complete it. • Other optional WBL's, whom aren't assigned, that employees can do themselves. • There are 5 WBL's for new joiners, when they come aboard. • Current employees, we assign annual WBL's to be completed in 60 days. • No refresher WBL's up to now, but the idea is that we work all together with the team to refresh topics. • Infographics, campaigns and yammer post to refresh all the topics throughout the year. Information on the Be.Aware page.

Table B.1: Transcribed Interview Results Learning team

C
Survey Questions

Demographics:
1. What is your gender? (Male/Female/Other/Prefer not to say)
2. How old are you? (Number)
3. What department do you work for? (Assurance, Tax, Strategy, Consulting)
4. Are you part of Technology Consulting (TC)? (Yes/No)
5. Does your work include any security related projects? (Yes/No)
6. What is your position/function? (Intern, Junior, Senior, Manager, Senior Manager, Partner, Other)
7. How long do you work for your company? (< 1 year, 1-2 years, 3-5 years, 6-10 years, > 10 years)

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. I am comfortable with computer technology and my company's security practices.
2. I know how to take action when I perceive a security risk in the workplace.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. I know the security threats that relate to my work on my company's information assets.
2. I have an understanding of how my work depends on the IT systems of my company.
3. To check that you are paying attention please select Disagree in this question.
4. If a security threat affected my company, we would still be able to continue our work.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. I understand the content of the security policies that apply to me.
2. I know my role with regard to the security policies that apply to me.
3. I know how to put security policy into practice in order to comply.
4. I know how and where to report security incidents.
5. I find the security policies to be fitting to the mission of my company.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. I know the security risks that exist in my work.
2. I know the risk of not using a strong password.
3. I know the risk of opening a link/attachment from an e-mail I do not trust.
4. I know the risk of not keeping the software on my computer up-to date.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. The security training that is provided is easy to put into practice, relative to other mandatory training.
2. Security training acts as a reminder of work-related security practices.
3. Security training is useful for providing me with security-related information that is new to me.
4. I discuss security related things with colleagues that are also in the training.
5. SuccessFactors supports me in completing the security training.
6. SuccessFactors supports the delivery of the security information in the training.
7. The security training modules are: Tick top 3 that apply: informative, irrelevant, entertaining, boring, text-heavy, visual, time consuming, hard to find time for, easy to understand, difficult to understand, difficult to apply, easy to apply, fresh, repetitive, general, specific.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]
1. If I follow the organisation's security training, I can work securely
2. I can only feel that I am working securely, if everyone else is.
3. Security training has helped me manage unexpected and risky situations in work.
4. The security training provided to me, can be put into practice within my abilities.

Please indicate if you agree or disagree with the following statements:
[1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree]

1. Completing the security training takes a reasonable amount of time.
2. I feel like behaving in a secure manner, takes an appropriate amount of time.
3. I feel like following the security training, reduces the efficiency of completing my work.

Please indicate if you perform the actions in the following statements on the scale of 'Never to Always'
[1: Never; 2: Rarely; 3: Sometimes; 4: Often 5: Always]

1. I don't open attachments to emails from an unfamiliar source.
2. I review and delete company business emails and attachments that I know are no longer required or to be retained.
3. To check that you are paying attention please select Often in this question.
4. I do not install non-standard software on company authorised or company provided systems or devices.
5. I use only the cloud data storage, processing and transfer services that are provided by my company for my work.
6. When creating a password for my work account, I use a passphrase that has no names, consecutive numbers or content of previous passwords.
7. My password that I use for business purposes is different to the one I use for personal purposes.
8. I use remember password features that are provided by company information systems and services.
9. I lock the device screen and secure the company laptop when stepping away from it.
10. I shut down or power off my company laptop before transporting it.
11. I will not allow anyone else to access the company technology that has been assigned to me.
12. I am keeping the computing devices that I use to conduct business activities up to date.

D

Descriptive Statistics Demographics

Frequency Table

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	64	64.6	64.6	64.6
	Female	32	32.3	32.3	97.0
	Prefer not to say	3	3.0	3.0	100.0
	Total	99	100.0	100.0	

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 25 years	9	9.1	9.1	9.1
	25 - 35 years	68	68.7	68.7	77.8
	35 - 45 years	12	12.1	12.1	89.9
	45 - 55 years	7	7.1	7.1	97.0
	55 - 65 years	3	3.0	3.0	100.0
	Total	99	100.0	100.0	

Department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Assurance	26	26.3	26.3	26.3
	Tax	2	2.0	2.0	28.3
	Consulting	58	58.6	58.6	86.9
	CBS	13	13.1	13.1	100.0
	Total	99	100.0	100.0	

Technology Consulting

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	37	37.4	37.4	37.4
	No	62	62.6	62.6	100.0
	Total	99	100.0	100.0	

Security related work

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	47	47.5	47.5	47.5
	No	52	52.5	52.5	100.0
	Total	99	100.0	100.0	

Function

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Intern, Junior or Senior	65	65.7	65.7	65.7
	Manager, Senior Manager or Partner	34	34.3	34.3	100.0
	Total	99	100.0	100.0	

Deployment lenght

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	< 1 year	21	21.2	21.2	21.2
	1 - 2 years	21	21.2	21.2	42.4
	3 - 5 years	31	31.3	31.3	73.7
	6 - 10 years	14	14.1	14.1	87.9
	> years	12	12.1	12.1	100.0
	Total	99	100.0	100.0	

Figure D.1 Descriptive Statistics Demographic Questions

E

Common Method Bias

Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	8.477	22.308	22.308	7.780	20.474	20.474
2	3.302	8.690	30.998			
3	2.078	5.469	36.467			
4	1.985	5.223	41.690			
5	1.873	4.929	46.619			
6	1.694	4.459	51.078			
7	1.577	4.151	55.229			
8	1.358	3.573	58.802			
9	1.235	3.251	62.053			
10	1.196	3.147	65.200			
11	1.104	2.904	68.105			
12	.992	2.610	70.715			
13	.938	2.469	73.185			
14	.895	2.354	75.539			
15	.884	2.326	77.864			
16	.791	2.082	79.947			
17	.738	1.942	81.888			
18	.682	1.794	83.683			
19	.628	1.653	85.336			
20	.613	1.614	86.950			
21	.543	1.429	88.379			
22	.529	1.393	89.772			
23	.431	1.133	90.905			
24	.413	1.086	91.992			
25	.377	.992	92.984			
26	.337	.887	93.871			
27	.316	.832	94.703			
28	.291	.765	95.468			
29	.271	.713	96.182			
30	.253	.665	96.847			
31	.231	.609	97.456			
32	.213	.562	98.018			
33	.188	.494	98.512			
34	.152	.401	98.912			
35	.122	.322	99.234			
36	.117	.308	99.542			
37	.101	.267	99.809			
38	.073	.191	100.000			

Extraction Method: Principal Axis Factoring.

Figure E.1 Harmon's One-factor Test

F

Construct Reliability and Validity Results

Scale: Knowledge scale

Case Processing Summary

		N	%
Cases	Valid	99	100.0
	Excluded[a]	0	.0
	Total	99	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.842	.846	14

Item Statistics

	Mean	Std. Deviation	N
CK1	4.01	.647	99
CK2	3.82	.861	99
CTK1	4.08	.710	99
CTK2	4.19	.710	99
CTK3	2.94	.946	99
CPK1	3.87	.816	99
CPK2	3.82	.850	99
CPK3	3.80	.880	99
CPK4	3.41	.892	99
CPK5	3.74	.723	99
CRK1	4.02	.728	99
CRK2	4.44	.798	99
CRK3	4.55	.594	99
CRK4	4.15	.973	99

Figure F.1 Scale Reliability Test Cybersecurity Knowledge

Scale: Perceived Training Scale

Case Processing Summary

		N	%
Cases	Valid	99	100.0
	Excluded[a]	0	.0
	Total	99	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.753	.769	6

Item Statistics

	Mean	Std. Deviation	N
PT1	3.65	.747	99
PT2	3.84	.738	99
PT3	3.51	.952	99
PT4	2.45	1.072	99
PT5	3.43	1.032	99
PT6	3.48	.983	99

Figure F.2 Scale Reliability Test Perceived Security Training

Scale: Perceived Effectiveness Scale

Case Processing Summary

		N	%
Cases	Valid	99	100.0
	Excluded[a]	0	.0
	Total	99	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.553	.571	4

Item Statistics

	Mean	Std. Deviation	N
PE1	3.66	.797	99
PE2	3.34	1.099	99
PE3	2.98	.915	99
PE4	3.79	.746	99

Figure F.3 Scale Reliability Test Perceived Effectiveness

Scale: Perceived Productivity Scale

Case Processing Summary

		N	%
Cases	Valid	99	100.0
	Excluded[a]	0	.0
	Total	99	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.393	.401	3

Item Statistics

	Mean	Std. Deviation	N
PR1	3.25	.930	99
PR2	3.41	.926	99
PR3	2.62	1.047	99

Figure F.4 Scale Reliability Test Perceived Productivity

Pattern Matrix[a]

	Component			
	1	2	3	4
CPK3	.852			
CPK2	.823			
CPK1	.783			
CPK4	.720			
CK2	.555		-.358	
CRK1	.449	.330		
CRK2		.921		
CRK4		.659		
CRK3		.572		.502
CTK3			.779	
CPK5	.461		.574	
CTK2				.802
CTK1				.624

Extraction Method: Principal Component Analysis. Rotation Method: Oblimin with Kaiser Normalization.[a]

a. Rotation converged in 16 iterations.

Figure F.5 Loadings Perceived Security Knowledge

Pattern Matrix[a]

	Component 1	Component 2
PT6	.886	
PT5	.822	
PT1	.796	-.329
PT2	.779	
PT3	.560	
PT4		.957

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.[a]

a. Rotation converged in 4 iterations.

Component Matrix[a]

	Component 1
PE1	.771
PE3	.761
PE4	.602
PE2	.496

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Component Matrix[a]

	Component 1
PR2	.754
PR1	.744
PR3	-.506

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Figure F.6: Loadings PT, PE and PR

G

Employee Security Behaviour Scale

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.650
Bartlett's Test of Sphericity	Approx. Chi-Square	173.083
	df	55
	Sig.	.000

Figure G.1 KMO and Barlett's Test EB Scale

Scale: Employee Security Behaviour Scale

Case Processing Summary

		N	%
Cases	Valid	99	100.0
	Excluded[a]	0	.0
	Total	99	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.646	.670	11

Item Statistics

	Mean	Std. Deviation	N
EB1	3.95	1.431	99
EB2	2.36	1.173	99
EB3	3.54	1.272	99
EB4	4.06	1.096	99
EB5	3.24	1.478	99
EB6	4.31	1.075	99
EB7	2.79	1.402	99
EB8	4.46	.799	99
EB9	3.62	1.361	99
EB10	4.30	1.208	99
EB11	4.46	.760	99

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
EB1	37.15	32.538	.270	.282	.632
EB2	38.74	33.890	.273	.196	.629
EB3	37.57	33.636	.253	.203	.634
EB4	37.04	34.407	.263	.189	.631
EB5	37.86	29.837	.431	.309	.594
EB6	36.79	33.067	.385	.309	.610
EB7	38.31	35.687	.080	.101	.672
EB8	36.64	35.091	.344	.256	.622
EB9	37.48	31.844	.345	.281	.615
EB10	36.80	32.469	.368	.347	.611
EB11	36.64	34.519	.436	.381	.612

Figure G.2 Scale Reliability Test Employee Security Behaviour

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.646
Bartlett's Test of Sphericity	Approx. Chi-Square	143.942
	df	36
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.569	28.544	28.544	2.569	28.544	28.544	1.773	19.702	19.702
2	1.499	16.660	45.204	1.499	16.660	45.204	1.756	19.516	39.219
3	1.119	12.434	57.638	1.119	12.434	57.638	1.658	18.419	57.638
4	.948	10.537	68.175						
5	.754	8.373	76.548						
6	.678	7.532	84.081						
7	.559	6.209	90.290						
8	.509	5.650	95.940						
9	.365	4.060	100.000						

Extraction Method: Principal Component Analysis.

Rotated Component Matrix[a]

	Component		
	1	2	3
EB1		.745	
EB3		.696	
EB4			.654
EB5	.762		
EB6	.798		
EB8	.630		.304
EB9			.674
EB10		.770	
EB11		.306	.743

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 5 iterations.

Figure G.3 Factor Analysis Security Behaviour Scale

Number of distinct sample moments:	594
Number of distinct parameters to be estimated:	120
Degrees of freedom (594 - 120):	474

Result (Default model)

Minimum was achieved
Chi-square = 788,092
Degrees of freedom = 474
Probability level = ,000

Group number 1 (Group number 1 - Default model)

Estimates (Group number 1 - Default model)

Scalar Estimates (Group number 1 - Default model)

Maximum Likelihood Estimates

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
PT1	<---	PT	1,000				
PT2	<---	PT	,984	,178	5,516	***	
PT3	<---	PT	,845	,219	3,856	***	
PT4	<---	PT	,374	,238	1,570	,116	
PT5	<---	PT	1,873	,267	7,011	***	
PT6	<---	PT	1,916	,264	7,269	***	
PE1	<---	PE	1,000				
PE2	<---	PE	,459	,267	1,720	,085	
PE3	<---	PE	1,026	,251	4,080	***	
PE4	<---	PE	,902	,210	4,299	***	
CTK3	<---	TK	,128	,188	,683	,495	
CTK2	<---	TK	,659	,150	4,401	***	
CTK1	<---	TK	1,000				
CRK1	<---	RK	1,336	,278	4,806	***	
CRK2	<---	RK	1,000				
CRK3	<---	RK	,793	,196	4,039	***	
CRK4	<---	RK	1,614	,352	4,582	***	
CPK1	<---	PK	1,000				
CPK2	<---	PK	1,175	,128	9,192	***	
CPK3	<---	PK	1,173	,132	8,850	***	
CPK4	<---	PK	,772	,143	5,405	***	
CPK5	<---	PK	,581	,116	4,991	***	

			Estimate	S.E.	C.R.	P	Label
EB1	<---	EB	1,000				
EB3	<---	EB	,623	,543	1,147	,252	
EB4	<---	EB	1,382	,775	1,784	,074	
EB5	<---	EB	2,131	1,159	1,839	,066	
EB6	<---	EB	1,536	,837	1,835	,066	
EB8	<---	EB	1,279	,682	1,875	,061	
EB9	<---	EB	2,048	1,104	1,855	,064	
EB10	<---	EB	1,456	,826	1,763	,078	
EB11	<---	EB	1,620	,832	1,948	,051	
CK2	<---	CK	1,000				
CK1	<---	CK	,327	,124	2,640	,008	

Standardized Regression Weights: (Group number 1 - Default model)

			Estimate
PT1	<---	PT	,638
PT2	<---	PT	,635
PT3	<---	PT	,423
PT4	<---	PT	,166
PT5	<---	PT	,865
PT6	<---	PT	,928
PE1	<---	PE	,612
PE2	<---	PE	,204
PE3	<---	PE	,548
PE4	<---	PE	,591
CTK3	<---	TK	,078
CTK2	<---	TK	,531
CTK1	<---	TK	,806
CRK1	<---	RK	,761
CRK2	<---	RK	,520
CRK3	<---	RK	,554
CRK4	<---	RK	,688
CPK1	<---	Pk	,778
CPK2	<---	PK	,878
CPK3	<---	PK	,846
CPK4	<---	PK	,549
CPK5	<---	PK	,510
EB1	<---	EB	,223
EB3	<---	EB	,156
EB4	<---	EB	,403
EB5	<---	EB	,460
EB6	<---	EB	,456
EB8	<---	EB	,511

Covariances: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
PT	<-->	TK	,082	,037	2,229	,026	
PT	<-->	PK	,159	,044	3,610	***	
PT	<-->	RK	,077	,030	2,582	,010	
TK	<-->	RK	,199	,052	3,820	***	
RK	<-->	PK	,149	,045	3,288	,001	
TK	<-->	PK	,204	,054	3,790	***	
PE	<-->	EB	,044	,033	1,342	,180	
PT	<-->	PE	,181	,048	3,753	***	
PE	<-->	TK	,067	,044	1,522	,128	
PE	<-->	RK	,087	,036	2,411	,016	
PE	<-->	PK	,136	,048	2,802	,005	
CK	<-->	TK	,243	,064	3,773	***	
CK	<-->	EB	,153	,083	1,837	,066	
CK	<-->	PK	,281	,068	4,126	***	
CK	<-->	RK	,193	,056	3,443	***	
CK	<-->	PE	,058	,054	1,080	,280	
PK	<-->	EB	,115	,064	1,805	,071	
CK	<-->	PT	,100	,045	2,214	,027	
PT	<-->	EB	,045	,030	1,506	,132	
RK	<-->	EB	,105	,058	1,793	,073	
TK	<-->	EB	,116	,064	1,816	,069	

Correlations: (Group number 1 - Default model)

			Estimate
PT	<-->	TK	,304
PT	<-->	PK	,530
PT	<-->	RK	,395
TK	<-->	RK	,847
RK	<-->	PK	,572
TK	<-->	PK	,567
PE	<-->	EB	,284
PT	<-->	PE	,785
PE	<-->	TK	,243
PE	<-->	RK	,434
PE	<-->	PK	,442
CK	<-->	TK	,645
CK	<-->	EB	,730
CK	<-->	PK	,672
CK	<-->	RK	,708
CK	<-->	PE	,180
PK	<-->	EB	,573

Standardized Total Effects (Group number 1 - Default model)

	EB	PK	RK	TK	PE	PT	CK
CK2	,000	,000	,000	,000	,000	,000	,772
CK1	,000	,000	,000	,000	,000	,000	,336
EB11	,680	,000	,000	,000	,000	,000	,000
EB10	,385	,000	,000	,000	,000	,000	,000
EB9	,480	,000	,000	,000	,000	,000	,000
EB8	,511	,000	,000	,000	,000	,000	,000
EB6	,456	,000	,000	,000	,000	,000	,000
EB5	,460	,000	,000	,000	,000	,000	,000
EB4	,403	,000	,000	,000	,000	,000	,000
EB3	,156	,000	,000	,000	,000	,000	,000
EB1	,223	,000	,000	,000	,000	,000	,000
CPK5	,000	,510	,000	,000	,000	,000	,000
CPK4	,000	,549	,000	,000	,000	,000	,000
CPK3	,000	,846	,000	,000	,000	,000	,000
CPK2	,000	,878	,000	,000	,000	,000	,000
CPK1	,000	,778	,000	,000	,000	,000	,000
CRK4	,000	,000	,688	,000	,000	,000	,000
CRK3	,000	,000	,554	,000	,000	,000	,000
CRK2	,000	,000	,520	,000	,000	,000	,000
CRK1	,000	,000	,761	,000	,000	,000	,000
CTK1	,000	,000	,000	,806	,000	,000	,000
CTK2	,000	,000	,000	,531	,000	,000	,000
CTK3	,000	,000	,000	,078	,000	,000	,000
PE4	,000	,000	,000	,000	,591	,000	,000
PE3	,000	,000	,000	,000	,548	,000	,000
PE2	,000	,000	,000	,000	,204	,000	,000
PE1	,000	,000	,000	,000	,612	,000	,000
PT6	,000	,000	,000	,000	,000	,928	,000
PT5	,000	,000	,000	,000	,000	,865	,000
PT4	,000	,000	,000	,000	,000	,166	,000
PT3	,000	,000	,000	,000	,000	,423	,000
PT2	,000	,000	,000	,000	,000	,635	,000
PT1	,000	,000	,000	,000	,000	,638	,000

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	120	788,092	474	,000	1,663
Saturated model	594	,000	0		
Independence model	66	1663,617	528	,000	3,151

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,526	,472	,736	,692	,723
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	,898	,472	,649
Saturated model	,000	,000	,000
Independence model	1,000	,000	,000

NCP

Model	NCP	LO 90	HI 90
Default model	314,092	240,780	395,294
Saturated model	,000	,000	,000
Independence model	1135,617	1016,297	1262,519

FMIN

Model	FMIN	F0	LO 90	HI 90
Default model	8,042	3,205	2,457	4,034
Saturated model	,000	,000	,000	,000
Independence model	16,976	11,588	10,370	12,883

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,082	,072	,092	,000
Independence model	,148	,140	,156	,000

AIC

Model	AIC	BCC	BIC CAIC
Default model	1028,092	1155,592	
Saturated model	1188,000	1819,125	
Independence model	1795,617	1865,742	

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	10,491	9,743	11,319	11,792
Saturated model	12,122	12,122	12,122	18,563
Independence model	18,323	17,105	19,618	19,038

HOELTER

Model	HOELTER .05	HOELTER .01
Default model	66	69
Independence model	35	36

Execution time summary

Minimization:	,042
Miscellaneous:	1,093
Bootstrap:	,000
Total:	1,135

Figure H.1 AMOS Output Structural Equation Model

Frequency Table

PT_Informative

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	47	47.5	47.5	47.5
	1.00	52	52.5	52.5	100.0
	Total	99	100.0	100.0	

PT_Entertaining

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	99	100.0	100.0	100.0

PT_Text_heavy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	86	86.9	86.9	86.9
	1.00	13	13.1	13.1	100.0
	Total	99	100.0	100.0	

PT_TimeConsuming

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	79	79.8	79.8	79.8
	1.00	20	20.2	20.2	100.0
	Total	99	100.0	100.0	

PT_Relevant

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	97	98.0	98.0	98.0
	1.00	2	2.0	2.0	100.0
	Total	99	100.0	100.0	

PT_Boring

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	69	69.7	69.7	69.7
	1.00	30	30.3	30.3	100.0
	Total	99	100.0	100.0	

PT_Visual

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	83	83.8	83.8	83.8
	1.00	16	16.2	16.2	100.0
	Total	99	100.0	100.0	

PT_HardToFindTimeFor

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	82	82.8	82.8	82.8
	1.00	17	17.2	17.2	100.0
	Total	99	100.0	100.0	

PT_EasyToUnder

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	50	50.5	50.5	50.5
	1.00	49	49.5	49.5	100.0
	Total	99	100.0	100.0	

PT_DiffToApply

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	96	97.0	97.0	97.0
	1.00	3	3.0	3.0	100.0
	Total	99	100.0	100.0	

PT_Fresh

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	96	97.0	97.0	97.0
	1.00	3	3.0	3.0	100.0
	Total	99	100.0	100.0	

PT_General

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	67	67.7	67.7	67.7
	1.00	32	32.3	32.3	100.0
	Total	99	100.0	100.0	

PT_DiffToUnder

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	99	100.0	100.0	100.0

PT_EasyToApply

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	75	75.8	75.8	75.8
	1.00	24	24.2	24.2	100.0
	Total	99	100.0	100.0	

PT_Repetitive

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	67	67.7	67.7	67.7
	1.00	32	32.3	32.3	100.0
	Total	99	100.0	100.0	

PT_Specific

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	95	96.0	96.0	96.0
	1.00	4	4.0	4.0	100.0
	Total	99	100.0	100.0	

Figure I.1 Frequency Tables Perceived Training Characteristics

$PTall*PT_Informative Crosstabulation

			PT_Informative		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	0	52	52
	PT_Text_heavy	Count	11	2	13
	PT_TimeConsuming	Count	16	4	20
	PT_EasyToUnder	Count	16	33	49
	PT_DiffToApply	Count	1	2	3
	PT_Fresh	Count	0	3	3
	PT_General	Count	20	12	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	23	7	30
	PT_Visual	Count	5	11	16
	PT_HardToFindTimeFor	Count	11	6	17
	PT_EasyToApply	Count	10	14	24
	PT_Repetitive	Count	25	7	32
	PT_Specific	Count	1	3	4
Total		Count	47	52	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Entertaining Crosstabulation

			PT_Entertaining	
			.00	Total
PTCharacteristics[a]	PT_Informative	Count	52	52
	PT_Text_heavy	Count	13	13
	PT_TimeConsuming	Count	20	20
	PT_EasyToUnder	Count	49	49
	PT_DiffToApply	Count	3	3
	PT_Fresh	Count	3	3
	PT_General	Count	32	32
	PT_Irrelevant	Count	2	2
	PT_Boring	Count	30	30
	PT_Visual	Count	16	16
	PT_HardToFindTimeFor	Count	17	17
	PT_EasyToApply	Count	24	24
	PT_Repetitive	Count	32	32
	PT_Specific	Count	4	4
Total		Count	99	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Text_heavy Crosstabulation

			PT_Text_heavy		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	50	2	52
	PT_Text_heavy	Count	0	13	13
	PT_TimeConsuming	Count	15	5	20
	PT_EasyToUnder	Count	47	2	49
	PT_DiffToApply	Count	2	1	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	27	5	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	26	4	30
	PT_Visual	Count	16	0	16
	PT_HardToFindTimeFor	Count	14	3	17
	PT_EasyToApply	Count	24	0	24
	PT_Repetitive	Count	28	4	32
	PT_Specific	Count	4	0	4
Total		Count	86	13	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_TimeConsuming Crosstabulation

			PT_TimeConsuming		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	48	4	52
	PT_Text_heavy	Count	8	5	13
	PT_TimeConsuming	Count	0	20	20
	PT_EasyToUnder	Count	46	3	49
	PT_DiffToApply	Count	2	1	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	27	5	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	21	9	30
	PT_Visual	Count	15	1	16
	PT_HardToFindTimeFor	Count	14	3	17
	PT_EasyToApply	Count	22	2	24
	PT_Repetitive	Count	25	7	32
	PT_Specific	Count	4	0	4
Total		Count	79	20	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_EasyToUnder Crosstabulation

			PT_EasyToUnder		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	19	33	52
	PT_Text_heavy	Count	11	2	13
	PT_TimeConsuming	Count	17	3	20
	PT_EasyToUnder	Count	0	49	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	1	2	3
	PT_General	Count	23	9	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	22	8	30
	PT_Visual	Count	7	9	16
	PT_HardToFindTimeFor	Count	12	5	17
	PT_EasyToApply	Count	8	16	24
	PT_Repetitive	Count	22	10	32
	PT_Specific	Count	3	1	4
Total		Count	50	49	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_DiffToApply Crosstabulation

			PT_DiffToApply		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	50	2	52
	PT_Text_heavy	Count	12	1	13
	PT_TimeConsuming	Count	19	1	20
	PT_EasyToUnder	Count	49	0	49
	PT_DiffToApply	Count	0	3	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	32	0	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	30	0	30
	PT_Visual	Count	16	0	16
	PT_HardToFindTimeFor	Count	15	2	17
	PT_EasyToApply	Count	24	0	24
	PT_Repetitive	Count	32	0	32
	PT_Specific	Count	4	0	4
Total		Count	96	3	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Fresh Crosstabulation

			PT_Fresh		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	49	3	52
	PT_Text_heavy	Count	13	0	13
	PT_TimeConsuming	Count	20	0	20
	PT_EasyToUnder	Count	47	2	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	0	3	3
	PT_General	Count	31	1	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	30	0	30
	PT_Visual	Count	16	0	16
	PT_HardToFindTimeFor	Count	17	0	17
	PT_EasyToApply	Count	24	0	24
	PT_Repetitive	Count	32	0	32
	PT_Specific	Count	4	0	4
Total		Count	96	3	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_General Crosstabulation

			PT_General		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	40	12	52
	PT_Text_heavy	Count	8	5	13
	PT_TimeConsuming	Count	15	5	20
	PT_EasyToUnder	Count	40	9	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	2	1	3
	PT_General	Count	0	32	32
	PT_Irrelevant	Count	1	1	2
	PT_Boring	Count	21	9	30
	PT_Visual	Count	14	2	16
	PT_HardToFindTimeFor	Count	14	3	17
	PT_EasyToApply	Count	20	4	24
	PT_Repetitive	Count	19	13	32
	PT_Specific	Count	4	0	4
Total		Count	67	32	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Irrelevant Crosstabulation

			PT_Irrelevant		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	52	0	52
	PT_Text_heavy	Count	13	0	13
	PT_TimeConsuming	Count	20	0	20
	PT_EasyToUnder	Count	49	0	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	31	1	32
	PT_Irrelevant	Count	0	2	2
	PT_Boring	Count	29	1	30
	PT_Visual	Count	16	0	16
	PT_HardToFindTimeFor	Count	16	1	17
	PT_EasyToApply	Count	24	0	24
	PT_Repetitive	Count	32	0	32
	PT_Specific	Count	3	1	4
Total		Count	97	2	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Boring Crosstabulation

			PT_Boring		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	45	7	52
	PT_Text_heavy	Count	9	4	13
	PT_TimeConsuming	Count	11	9	20
	PT_EasyToUnder	Count	41	8	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	23	9	32
	PT_Irrelevant	Count	1	1	2
	PT_Boring	Count	0	30	30
	PT_Visual	Count	15	1	16
	PT_HardToFindTimeFor	Count	11	6	17
	PT_EasyToApply	Count	23	1	24
	PT_Repetitive	Count	18	14	32
	PT_Specific	Count	4	0	4
Total		Count	69	30	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_Visual Crosstabulation

			PT_Visual		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	41	11	52
	PT_Text_heavy	Count	13	0	13
	PT_TimeConsuming	Count	19	1	20
	PT_EasyToUnder	Count	40	9	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	30	2	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	29	1	30
	PT_Visual	Count	0	16	16
	PT_HardToFindTimeFor	Count	16	1	17
	PT_EasyToApply	Count	20	4	24
	PT_Repetitive	Count	30	2	32
	PT_Specific	Count	3	1	4
Total		Count	83	16	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_HardToFindTimeFor Crosstabulation

			PT_HardToFindTimeFor		
			.00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	46	6	52
	PT_Text_heavy	Count	10	3	13
	PT_TimeConsuming	Count	17	3	20
	PT_EasyToUnder	Count	44	5	49
	PT_DiffToApply	Count	1	2	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	29	3	32
	PT_Irrelevant	Count	1	1	2
	PT_Boring	Count	24	6	30
	PT_Visual	Count	15	1	16
	PT_HardToFindTimeFor	Count	0	17	17
	PT_EasyToApply	Count	23	1	24
	PT_Repetitive	Count	30	2	32
	PT_Specific	Count	3	1	4
Total		Count	82	17	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_DiffToUnder Crosstabulation

			PT_DiffToUnder .00	Total
PTCharacteristics[a]	PT_Informative	Count	52	52
	PT_Text_heavy	Count	13	13
	PT_TimeConsuming	Count	20	20
	PT_EasyToUnder	Count	49	49
	PT_DiffToApply	Count	3	3
	PT_Fresh	Count	3	3
	PT_General	Count	32	32
	PT_Irrelevant	Count	2	2
	PT_Boring	Count	30	30
	PT_Visual	Count	16	16
	PT_HardToFindTimeFor	Count	17	17
	PT_EasyToApply	Count	24	24
	PT_Repetitive	Count	32	32
	PT_Specific	Count	4	4
Total		Count	99	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_EasyToApply Crosstabulation

			PT_EasyToApply .00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	38	14	52
	PT_Text_heavy	Count	13	0	13
	PT_TimeConsuming	Count	18	2	20
	PT_EasyToUnder	Count	33	16	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	28	4	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	29	1	30
	PT_Visual	Count	12	4	16
	PT_HardToFindTimeFor	Count	16	1	17
	PT_EasyToApply	Count	0	24	24
	PT_Repetitive	Count	27	5	32
	PT_Specific	Count	3	1	4
Total		Count	75	24	99

Percentages and totals are based on respondents.

$PTall*PT_DiffToUnder Crosstabulation

			PT_DiffToUnder .00	Total
PTCharacteristics[a]	PT_Informative	Count	52	52
	PT_Text_heavy	Count	13	13
	PT_TimeConsuming	Count	20	20
	PT_EasyToUnder	Count	49	49
	PT_DiffToApply	Count	3	3
	PT_Fresh	Count	3	3
	PT_General	Count	32	32
	PT_Irrelevant	Count	2	2
	PT_Boring	Count	30	30
	PT_Visual	Count	16	16
	PT_HardToFindTimeFor	Count	17	17
	PT_EasyToApply	Count	24	24
	PT_Repetitive	Count	32	32
	PT_Specific	Count	4	4
Total		Count	99	99

Percentages and totals are based on respondents.

a. Dichotomy group tabulated at value 1.

$PTall*PT_EasyToApply Crosstabulation

			PT_EasyToApply .00	1.00	Total
PTCharacteristics[a]	PT_Informative	Count	38	14	52
	PT_Text_heavy	Count	13	0	13
	PT_TimeConsuming	Count	18	2	20
	PT_EasyToUnder	Count	33	16	49
	PT_DiffToApply	Count	3	0	3
	PT_Fresh	Count	3	0	3
	PT_General	Count	28	4	32
	PT_Irrelevant	Count	2	0	2
	PT_Boring	Count	29	1	30
	PT_Visual	Count	12	4	16
	PT_HardToFindTimeFor	Count	16	1	17
	PT_EasyToApply	Count	0	24	24
	PT_Repetitive	Count	27	5	32
	PT_Specific	Count	3	1	4
Total		Count	75	24	99

Percentages and totals are based on respondents.

Figure I.2 Crosstabs Multiple Responses Perceived Training Characteristics

Correlations

		PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
PE	Pearson Correlation	1	.303**	-.076	-.251**	.349**	.018	-.008	-.171*	-.262**	-.169*	.173*	-.218*	.147	-.088	-.044
	Sig. (1-tailed)		.001	.226	.006	.000	.432	.470	.045	.004	.047	.044	.015	.073	.192	.335
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Correlations

		PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
CK	Pearson Correlation	1	-.330**	-.194*	.226*	-.074	.063	.036	.042	-.036	.091	-.165	.137	.009	-.071
	Sig. (1-tailed)	.151	.000	.027	.012	.232	.269	.363	.339	.361	.186	.052	.088	.463	.245
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Correlations

		EB	PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
EB	Pearson Correlation	1	.006	-.209*	-.197*	.134	-.020	.002	-.005	-.012	-.042	.009	.009	.142	.077	.014
	Sig. (1-tailed)		.477	.019	.026	.093	.423	.494	.479	.454	.340	.465	.465	.080	.224	.446
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Correlations

		PR1	PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
PR1	Pearson Correlation	1	.106	.088	-.001	.079	.079	-.112	-.095	-.350**	-.014	.058	-.066	-.002	-.025	.001
	Sig. (1-tailed)		.147	.194	.495	.218	.218	.135	.174	.000	.447	.284	.257	.494	.402	.496
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Correlations

		PR2	PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
PR2	Pearson Correlation	1	.120	-.045	-.062	.191*	-.143	-.143	-.076	-.065	-.010	.160	-.117	.053	-.170*	.132
	Sig. (1-tailed)		.118	.329	.270	.029	.078	.078	.227	.263	.460	.057	.123	.302	.046	.097
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Correlations

		PR3	PT_Informative	PT_Text_heavy	PT_TimeConsuming	PT_EasyToUnder	PT_DiffToApply	PT_Fresh	PT_General	PT_Relevant	PT_Boring	PT_Visual	PT_HardToFindTimeFor	PT_EasyToApply	PT_Repetitive	PT_Specific
PR3	Pearson Correlation	1	.040	-.201*	-.379**	.275**	-.065	.048	-.006	.085	-.116	.207*	-.065	.063	.077	-.027
	Sig. (1-tailed)		.348	.023	.000	.003	.261	.319	.477	.202	.126	.020	.262	.268	.224	.395
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	98

Figure I.3 Correlations Perceived Training Characteristics

J

Regression Analysis PR and PE

Statistics

		PR1	PR2	PR3
N	Valid	99	99	99
	Missing	0	0	0
Mean		3.25	3.41	3.38
Std. Deviation		.930	.926	1.047
Variance		.864	.857	1.096
Sum		322	338	335

Figure J.1 Descriptive Statistics Perceived Productivity

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.060[a]	.004	-.007	.61626	.004	.352	1	97	.555

a. Predictors: (Constant), PR1

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.134	1	.134	.352	.555[b]
	Residual	36.839	97	.380		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PR1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.865	.226		17.069	.000	3.416	4.315
	PR1	.040	.067	.060	.593	.555	-.093	.173

a. Dependent Variable: EB

Figure J.2 Regression Perceived Productivity item 1 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.199[a]	.040	.030	.60497	.040	4.020	1	97	.048

a. Predictors: (Constant), PR2

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.471	1	1.471	4.020	.048[b]
	Residual	35.501	97	.366		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PR2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.543	.233		15.179	.000	3.079	4.006
	PR2	.132	.066	.199	2.005	.048	.001	.263

a. Dependent Variable: EB

Figure J.3 Regression Perceived Productivity item 2 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.293[a]	.086	.076	.59037	.086	9.078	1	97	.003

a. Predictors: (Constant), PR3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.164	1	3.164	9.078	.003[b]
	Residual	33.808	97	.349		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PR3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.414	.202		16.926	.000	3.013	3.814
	PR3	.172	.057	.293	3.013	.003	.059	.285

a. Dependent Variable: EB

Figure J.4 Regression Perceived Productivity item 3 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.432[a]	.187	.178	.843	.187	22.269	1	97	.000

a. Predictors: (Constant), PT

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15.812	1	15.812	22.269	.000[b]
	Residual	68.875	97	.710		
	Total	84.687	98			

a. Dependent Variable: PR1

b. Predictors: (Constant), PT

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.061	.472		2.247	.027	.124	1.998
	PT	.646	.137	.432	4.719	.000	.374	.917

a. Dependent Variable: PR1

Figure J.5 Regression Perceived Training on Perceived Productivity item 1

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.284[a]	.081	.071	.892	.081	8.494	1	97	.004

a. Predictors: (Constant), PT

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.765	1	6.765	8.494	.004[b]
	Residual	77.255	97	.796		
	Total	84.020	98			

a. Dependent Variable: PR2

b. Predictors: (Constant), PT

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.981	.500		3.961	.000	.988	2.973
	PT	.422	.145	.284	2.914	.004	.135	.710

a. Dependent Variable: PR2

Figure J.6 Regression Perceived Training on Perceived Productivity item 2

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.225[a]	.051	.041	1.025	.051	5.176	1	97	.025

a. Predictors: (Constant), PT

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.442	1	5.442	5.176	.025[b]
	Residual	101.973	97	1.051		
	Total	107.414	98			

a. Dependent Variable: PR3

b. Predictors: (Constant), PT

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.098	.574		3.652	.000	.958	3.238
	PT	.379	.167	.225	2.275	.025	.048	.709

a. Dependent Variable: PR3

Figure J.7 Regression Perceived Training on Perceived Productivity item 3

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.022[a]	.001	-.010	.61722	.001	.049	1	97	.825

a. Predictors: (Constant), PE1

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.019	1	.019	.049	.825[b]
	Residual	36.953	97	.381		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PE1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	4.058	.293		13.871	.000	3.477	4.638
	PE1	-.017	.078	-.022	-.222	.825	-.172	.138

a. Dependent Variable: EB

Figure J.8 Regression Perceived Effectiveness item 1 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.132[a]	.017	.007	.61196	.017	1.726	1	97	.192

a. Predictors: (Constant), PE2

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.647	1	.647	1.726	.192[b]
	Residual	36.326	97	.374		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PE2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.747	.198		18.935	.000	3.354	4.140
	PE2	.074	.056	.132	1.314	.192	-.038	.186

a. Dependent Variable: EB

Figure J.9 Regression Perceived Effectiveness item 2 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.155[a]	.024	.014	.60990	.024	2.395	1	97	.125

a. Predictors: (Constant), PE3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.891	1	.891	2.395	.125[b]
	Residual	36.081	97	.372		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PE3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.684	.210		17.550	.000	3.267	4.100
	PE3	.104	.067	.155	1.547	.125	-.029	.238

a. Dependent Variable: EB

Figure J.10 Regression Perceived Effectiveness item 3 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.218[a]	.047	.038	.60259	.047	4.820	1	97	.031

a. Predictors: (Constant), PE4

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.750	1	1.750	4.820	.031[b]
	Residual	35.222	97	.363		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PE4

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.316	.315		10.529	.000	2.691	3.941
	PE4	.179	.082	.218	2.196	.031	.017	.341

a. Dependent Variable: EB

Figure J.11 Regression Perceived Effectiveness item 4 and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.305[a]	.093	.054	.59726	.093	2.411	4	94	.055

a. Predictors: (Constant), PE4, PE2, PE3, PE1

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.440	4	.860	2.411	.055[b]
	Residual	33.532	94	.357		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), PE4, PE2, PE3, PE1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	3.260	.389		8.373	.000	2.487	4.033
	PE1	-.139	.086	-.180	-1.614	.110	-.310	.032
	PE2	.067	.058	.120	1.167	.246	-.047	.182
	PE3	.089	.075	.133	1.200	.233	-.059	.237
	PE4	.198	.087	.241	2.284	.025	.026	.371

a. Dependent Variable: EB

Figure J.12 Regression Perceived Effectiveness and EB

K

Demographic Analysis

Descriptive Statistics

	N	Mean	Std. Deviation
D1	99	1.41	.655
D2	99	31.56	8.751
D3	99	3.30	1.453
D4	99	1.63	.486
D5	99	1.53	.502
D6	99	1.34	.477
D7	99	2.75	1.280
Valid N (listwise)	99		

Correlations

		D1	EB	PT
D1	Pearson Correlation	1	-.096	-.125
	Sig. (2-tailed)		.346	.218
	N	99	99	99
EB	Pearson Correlation	-.096	1	.242*
	Sig. (2-tailed)	.346		.016
	N	99	99	99
PT	Pearson Correlation	-.125	.242*	1
	Sig. (2-tailed)	.218	.016	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D2
EB	Pearson Correlation	1	.242*	.136
	Sig. (2-tailed)		.016	.181
	N	99	99	99
PT	Pearson Correlation	.242*	1	.062
	Sig. (2-tailed)	.016		.541
	N	99	99	99
D2	Pearson Correlation	.136	.062	1
	Sig. (2-tailed)	.181	.541	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D3
EB	Pearson Correlation	1	.242*	-.013
	Sig. (2-tailed)		.016	.896
	N	99	99	99
PT	Pearson Correlation	.242*	1	-.103
	Sig. (2-tailed)	.016		.309
	N	99	99	99
D3	Pearson Correlation	-.013	-.103	1
	Sig. (2-tailed)	.896	.309	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D4
EB	Pearson Correlation	1	.242*	-.011
	Sig. (2-tailed)		.016	.915
	N	99	99	99
PT	Pearson Correlation	.242*	1	-.076
	Sig. (2-tailed)	.016		.454
	N	99	99	99
D4	Pearson Correlation	-.011	-.076	1
	Sig. (2-tailed)	.915	.454	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D5
EB	Pearson Correlation	1	.242*	-.248*
	Sig. (2-tailed)		.016	.013
	N	99	99	99
PT	Pearson Correlation	.242*	1	-.092
	Sig. (2-tailed)	.016		.364
	N	99	99	99
D5	Pearson Correlation	-.248*	-.092	1
	Sig. (2-tailed)	.013	.364	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D6
EB	Pearson Correlation	1	.242*	.134
	Sig. (2-tailed)		.016	.185
	N	99	99	99
PT	Pearson Correlation	.242*	1	.072
	Sig. (2-tailed)	.016		.476
	N	99	99	99
D6	Pearson Correlation	.134	.072	1
	Sig. (2-tailed)	.185	.476	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Correlations

		EB	PT	D7
EB	Pearson Correlation	1	.242*	.060
	Sig. (2-tailed)		.016	.554
	N	99	99	99
PT	Pearson Correlation	.242*	1	-.111
	Sig. (2-tailed)	.016		.275
	N	99	99	99
D7	Pearson Correlation	.060	-.111	1
	Sig. (2-tailed)	.554	.275	
	N	99	99	99

*. Correlation is significant at the 0.05 level (2-tailed).

Figure K.1 Descriptives Demographics and Correlations to PT and EB

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.096[a]	.009	-.001	.61455	.009	.896	1	97	.346

a. Predictors: (Constant), D1

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.338	1	.338	.896	.346[b]
	Residual	36.634	97	.378		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	4.121	.148		27.920	.000	3.828	4.414			
	D1	-.090	.095	-.096	-.946	.346	-.278	.098	-.096	-.096	-.096

a. Dependent Variable: EB

Figure K.2 Regression D1 (Gender) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.136[a]	.018	.008	.61168	.018	1.817	1	97	.181

a. Predictors: (Constant), D2

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.680	1	.680	1.817	.181[b]
	Residual	36.292	97	.374		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	3.694	.231		15.982	.000	3.235	4.153			
	D2	.010	.007	.136	1.348	.181	-.004	.024	.136	.136	.136

a. Dependent Variable: EB

Figure K.3 Regression D2 (Age) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.013[a]	.000	-.010	.61732	.000	.017	1	97	.896

a. Predictors: (Constant), D3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.007	1	.007	.017	.896[b]
	Residual	36.966	97	.381		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	4.013	.155		25.934	.000	3.706	4.320			
	D3	-.006	.043	-.013	-.131	.896	-.091	.080	-.013	-.013	-.013

a. Dependent Variable: EB

Figure K.4 Regression D3 (Department) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.011[a]	.000	-.010	.61734	.000	.012	1	97	.915

a. Predictors: (Constant), D4

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.004	1	.004	.012	.915[b]
	Residual	36.968	97	.381		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D4

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	4.017	.218		18.460	.000	3.585	4.449			
	D4	-.014	.128	-.011	-.107	.915	-.268	.241	-.011	-.011	-.011

a. Dependent Variable: EB

Figure K.5 Regression D4 (TC) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.248[a]	.061	.052	.59813	.061	6.345	1	97	.013

a. Predictors: (Constant), D5

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.270	1	2.270	6.345	.013[b]
	Residual	34.702	97	.358		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D5

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	4.457	.193		23.069	.000	4.073	4.840			
	D5	-.303	.120	-.248	-2.519	.013	-.542	-.064	-.248	-.248	-.248

a. Dependent Variable: EB

Figure K.6 Regression D5 (Security Related Work) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics			
					R Square Change	F Change	df1	df2	Sig. F Change
1	.134[a]	.018	.008	.61179	.018	1.781	1	97	.185

a. Predictors: (Constant), D6

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.667	1	.667	1.781	.185[b]
	Residual	36.306	97	.374		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D6

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	3.762	.185		20.391	.000	3.396	4.128			
	D6	.173	.129	.134	1.335	.185	-.084	.430	.134	.134	.134

a. Dependent Variable: EB

Figure K.7 Regression D6 (Function) and Employee Security Behaviour

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.060[a]	.004	-.007	.61626	.004	.352	1	97	.554

a. Predictors: (Constant), D7

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.134	1	.134	.352	.554[b]
	Residual	36.838	97	.380		
	Total	36.972	98			

a. Dependent Variable: EB

b. Predictors: (Constant), D7

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	3.915	.147		26.592	.000	3.623	4.207			
	D7	.029	.049	.060	.594	.554	-.068	.125	.060	.060	.060

a. Dependent Variable: EB

Figure K.8 Regression D7 (Deployment Length) and Employee Security Behaviour