NTNU
Norwegian University of
Science and Technology

Influencing Factors and Effectiveness of a Security Awareness Campaign

Kristine Larsen Strand

Master of Science in Communication Technology
Submission date: June 2018
Supervisor: Maria Bartnes, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

NTNU – Trondheim
Norwegian University of
Science and Technology

Influencing Factors and Effectiveness of a Security Awareness Campaign

Kristine Larsen Strand

Submission date: June 2018
Responsible professor: Maria Bartnes, NTNU/SINTEF
Supervisor: Erlend A. Gjære, Secure Practice AS

Norwegian University of Science and Technology
Department of Telematics

Abstract

As an organisation, it is important with technical security controls to protect information assets, but without cooperation from the employees, this is nearly useless. Gradually realising the importance of information security awareness, different campaigns and programs have been created to be deployed in organisations that wish to strengthen the awareness and knowledge of their employees. Creating an effective program or campaign is not straightforward, and there are several factors that come into play. Preknowledge, attitude, personality and the company's culture and norms are all examples of such factors. Some studies have been conducted to try to outline what the most optimal way of implementing a program is, or measuring the effect of an awareness campaign, but the topic is still highly relevant to research. This project uses data from an information security awareness campaign that has been deployed in a company existing of around 2000 knowledge workers. The goal is to try to find out to which degree different groups of people have different views on the implemented campaign, and on the general topic of information security. The campaign consisted of three "rounds" running periodically over three years, and continuous communication, reminders and talks were given also outside of the specified rounds. In each round, a set of e-learning sessions were released on the company's intranet, consisting of a video raising a security issue accompanied by PowerPoint slides elaborating on the issue. After each campaign "round" a survey was conducted, asking the employees various questions regarding the campaign and security in general. In addition to data from the campaign (with surveys), interviews were done to substantiate or contradict findings from the surveys. The findings indicate that there are differences in gender, age, and management responsibility level with regard to information security in the workplace. They also imply that the campaign had some effect on the employees' motivation and behaviour. The interviews uncovered four main themes; the campaign, IT-systems in the organisation, information security and policies, and management and organisation. All interviewees were content with the campaign method, although they admitted they learned little new from it. Most agreed that the campaign rounds could be spread more evenly over the year, and some wished for stricter/obligatory completion of the e-learning sessions. Although all candidates expressed that information security was important to them and their coworkers, most of them mentioned the gap between security and practicality. All interviewees agreed that their boss has a positive approach to information

security and that this is important to create a positive engagement around the topic in the company.

Sammendrag

Som organisasjon er det viktig med tekniske sikkerhetstiltak for å beskytte informasjonressurser, men uten samarbeid fra de ansatte i organisasjonen er disse lite verdt alene. I sammenheng med at man har begynt å forstå viktigheten av sikkerhetsbevissthet har mange selskap begynt å implementere kampanjer og programmer som skal hjelpe med å øke sikkerhetsbevisstheten til de ansatte. Det å utvikle et effektivt prorgam eller en kampanje er ikke rett fram og det er mange faktorer som spiller inn. Forkunnskaper, holdninger, personlighet, og selskapets kultur og normer er eksempler på slike faktorer. Noen studier har forsket på hvordan man utvikler sikkerhetsbevissthetskampanjer- og programmer på mest optimalt vis, men emnet er fortsatt høyst relevant for videre forskning. Dette prosjektet bruker data fra en sikkerhetsbevissthetskampanje som har vært implementert i et selskap med omkring 2000 kunnskapsarbeidere, med mål om å finne ut i hvilken grad forskjellige grupper mennesker har forskjellig syn på, eller holdninger til, den implementerte kampanjen og til informasjonssikkerhet generelt. Kampanjen bestod av tre runder som løp periodevis over tre år. Jevnt over de tre årene var det kontinuerlig kommunikasjon rundt temaet informasjonssikkerhet; presentasjoner ble gitt, og påminnelser ble gitt i form av plakater og flyers etc. Etter hver kampanjerunde ble det sendt ut en spørreundersøkelse som de ansatte kunne velge å delta i. Spørreundersøkelsen inneholdt spørsmål om kampanjen og om sikkerhet generelt. I tillegg til data fra kampanjen har det blitt gjort intervjuer med noen ansatte i bedriften. Disse intervjuene er godt tilleggsstoff til resultatene fra kampanjedataene. Resultatene indikerer at det er forskjell mellom hvordan kjønn, aldersgrupper og ansvarsnivå anser informasjonssikkerhet på arbeidsplassen. Resultatene insinuerer også at kampanjen hadde en viss effekt på de ansattes holdninger og oppførsel. Intervjuene avdekket fire hovedtema; kampanjen, IT-system i bedriften, ledelse og organisasjon, og informasjonssikkerhet og bedrifts-policies. Alle intervjukandidatene var fornøyde med kampanjemetoden, men de innrømte samtidig at kampanjen ikke lært dem mye nytt. De fleste var enige i at kampanjerundene kunne ha vært spredt jevnere utover året, og noen gav uttrykk for at de ønsket strengere krav om gjennomføring av e-læringene. Selv om alle gav uttrykk for at informasjonssikkerhet var viktig både for dem selv og for deres medarbeidere, nevnte de fleste at det finnes et gap mellom sikkerhet og anvendbarhet. Alle intervjukandidater var enige om at sjefen deres har en positiv holdning til informasjonssikkerhet, og at dette er viktig for å skape et positivt engasjement rundt temaet i selskapet.

Acknowledgements

I would like to thank my supervisors, Erlend and Maria, for dedicating their time and knowledge to guide me, and for following me closely through this project. I would also like to thank my smart friend Ida for helping me with some of the statistical work in this thesis. Lastly, I want to thank my mother for proofreading my work, and for listening to my complaining in harder times.

Contents

Appendices

List of Figures

List of Tables

Chapter 1
Introduction

This thesis deals with information security awareness, security behaviour, and awareness programs. Information security awareness is the knowledge that end users have about security risks, and the attitude they have towards complying with an organisations' security policies. InfoSec Institute has listed some common security threats to employees that lack cyber-security awareness [Fah]. The threats may seem banal, but are highly relevant and possibly very harmful to a company whose employees do not have enough knowledge about the topic. Phishing is one of the threats to be listed, and is a social-engineering phenomenon where a fraudulent person tricks a person into clicking a bogus link or opening a malicious attachment. This often happens in the form of a legitimate-looking email and can be hard to detect as hackers act more and more sophisticated. Another threat they mention is default or weak passwords, a threat that has always existed and still remains a big problem. Brute forcing, or even guessing, a weak password is fairly simple, and is often an imposter's first try to getting valuable information. A report from 2016 by the Ponemon Institute shows that 25% of security breaches happen due to human errors [LLC16], and people are often referred to as the weakest link in the process of securing networks and systems [MW03]. This is a serious issue which should be addressed accordingly, and many organisations utilise security awareness programs or campaigns to try to mitigate the problem. Such programs are meant to raise employees' awareness regarding the company's security policies and threats, as well as their own responsibilities to address this. According to NIST, a successful IT security program should consist of three main components [MW03]: 1) develop IT security policies that reflect business needs but also their threats; 2) informing users of their IT security responsibilities; 3) establish processes for monitoring and reviewing the program. Despite three, good ground pillars for a program, no explanation is given as to how to best relay information to the users. This is an important question because people are different, they learn differently, and an effective program should optimally motivate and teach all employees in a company.

This project will explore security awareness attitudes, motivations, and behaviour

among employees, information security awareness campaigns, and the relationship between the two. Specifically, following research questions have been developed in coherence with this project:

- RQ1: How do factors like gender, age and management position influence attitudes towards information security and information security training?
- RQ2: How does the implementation of a security awareness campaign affect employees' attitudes towards the topic, and their behaviour?
- RQ3: What is the optimal way of relaying security awareness, and to motivate all employees?

To facilitate the exploring of these research questions, smaller hypotheses have been established. The hypotheses will be explored in Results 4, and will be the basis of discussion and conclusion of the main research questions. The following hypotheses will be explored:

- H1: Women are more positive towards security training than men
- H2: Age plays a role in the positivity towards security training
- H3: Employees with higher management responsibilities feel more responsible with regard to information security than those with lower management responsibilities
- H4: Employees with higher management responsibilities act more securely with regard to information security than those with lower management responsibilities
- H5: Employees are more positive toward information security/training by the last campaign round than they were in the first
- H6: Employees act more securely by the last campaign round than they did in the first

H1-H4 belong to *RQ1*, while *H5* and *H6* apply to *RQ2*.

This thesis is organised as follows: First, some definitions are given, followed by an extensive literature review. The literature review presents studies that have been conducted about security-related behaviour and motivation with employees, and security management at an organisational level. Next, relevant data from the surveys will be presented in conjunction with the hypotheses. The analysis of the interviews

will follow after this, and finally, findings from the results will be discussed, followed by a brief conclusion.

Chapter 2
Related Literature

Firstly in this chapter, some definitions of the most relevant terms are explained. Secondly, a literature review is given, summarising some important studies that have already been done on the topic.

2.1 Information Security Awareness

The term Information Security Awareness (ISA) is understood and used in various ways in the literature. However, there is some degree of agreement, and for the purpose of this project the definition of awareness that seems the most appropriate is taken from Shaw, Chen, Harris, and Huang [RSS09]:

"Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks."

As the definition implies, awareness has different levels depending on the degree of understanding one has of the topic. In their paper, they present three levels of awareness; perception, comprehension, and projection. A person with the lowest level of awareness may know about possible risks but does not have the knowledge to mitigate them. A person at the comprehension level of awareness may know about the risks, and in addition, have obtained the knowledge to act preventively. The projection level of awareness might be that the person has earlier experience with a similar scenario, and, based on that, can draw conclusions and decide on a preventive action.

2.2 Information Security Awareness Programs and Campaigns

The ultimate goal of an organisation with respect to information security would be to decrease the number of security breaches as much as possible. In order to achieve this, the employees have to be aware of security threats and comply with security policies of the company to mitigate the threats. To help raise the awareness about information security to an adequate level, the implementation of awareness and training programs are suggested [Org13]. It is proposed that such campaigns "(...) address the problems that a lack of knowledge could lead to". NIST presents a three-step procedure to implement an awareness program [MW03]. First, a design of the program with the organisation's mission in mind must be done. In this step, the most important substeps include establishing priorities, discover the awareness needs of the organisaton, constructing a plan for the program, and structuring the awareness activity. Second, the program is developed. This step mainly consists of choosing the awareness topics and their sources. The third and last step is the actual implementation of the program. The program has to be communicated to all involved parties and can be done in several ways. Awareness programs are often implemented in the form of campaigns and may be communicated through e-mail messages, posters, lists and other creative means.

As explained above, security awareness efforts in organisations aim to skew focus on, and inform about information security risks and counter measurements, and the employees' responsibilities. The ultimate goal of such efforts is to affect the behaviour of employees, make them comply with company security policies, and eventually create and maintain a security culture. However, research show that awareness does not necessarily result in desired behaviour [JS15], [JMS05]. This is an interesting and important field of research, as optimally all employees should comply in order to create a culture for security. How can awareness programs be designed to be engaging for all, and what may be the reasons for not complying despite having the knowledge and skills to do so?

2.3 Information Security Culture

Every organisation has their own culture constituted by values and behaviours that are specific to that organisation. Having an information security culture refers to having an organisational culture where information security poses an important part, and is of important value to the organisation and, optimally, the people in it. Security should not only be important on paper, it should be reflected in actions and behaviours throughout the company. As stated by Van Niekerk & Von Solms [JVN10] and suggested by Von Solms [vS00], it has become widely accepted that a security culture within the company is the key to tackling the human factors of

information security. Sherif, Furnell, and Clarke [ABC15] argue that a model for cultivating a security culture can be based on information security and information security behaviour, with information security awareness as starting point to influence the security behaviour.

CLTRe [KR17] shortly defines security culture as internalising security issues, and making security an intrinsic part of employees' working day, actively practising security and making decisions that secure organisational assets. In their report [KR17], seven dimensions of security culture are established;

1. Attitudes
2. Responsibilities
3. Communication
4. Compliance
5. Knowledge
6. Norms
7. Behaviours

As the list infers, several factors contribute to the definition of security culture. Some of them are included in the definition of security *awareness*, but security *culture* is defined by even more dimensions. As described in 2.1, the term awareness is defined in various ways, and some of the definitions involve more of these dimensions than others. CLTRe, for instance, defines security awareness as only knowledge, and argues, hence, that security culture is more important than security awareness.

2.4 Literature Review and Earlier Work

There are done several studies on information security awareness (ISA) and information security culture in organisations. Surveys have been conducted in companies to try to map, among other things, security behaviour of end-users, what makes people comply with security policies and what makes them fail to do so, how is personality and intention affecting their motivation, and what is actually an effective security campaign. Each of the following paragraphs are summaries of studies already conducted on the topic.

Previous research has focused on measuring behaviour based on intention, but as has been shown, there are several unknown variables that exist between the intention

and actual behaviour. People may have the best intention, but for different reasons fail to act on them. Hence, the accuracy for predicting compliance behaviour has been relatively low, and as an aid to make this prediction gap smaller, it has been proposed that one understand the "Big Five" personality traits of end-users. Shropshire *et al.* [JS15] discussed especially the two factors conscientiousness and agreeableness. They confirm that these are two personality traits that moderate the gap between intention and behaviour. Specifically, they conclude that people with a higher degree of these traits have a higher probability of behaving according to their intentions.

Stanton *et al.* [JMS05] presented a taxonomy for security-related behaviours, focusing on password-related behaviour, showing that these behaviours mainly can be parted into six groups on a two-dimensional frame of reference. The two dimensions are measured in expertise and intentions respectively, and the six behaviour groups are placed in the frame of reference as a factor of the two; detrimental misuse is a result of little knowledge and malicious intentions, while aware assurance is a result of much knowledge and benevolent intentions. They argue that this confirmation of taxonomy may help an organisation to systematically assess and control behaviour related to security.

The two previously mentioned studies focus mostly on analysing the behaviour and personality traits of end-users, discussing different factors that make people comply to a greater or lesser degree. However, it is also interesting to see how one can change attitudes and behaviour, and Sherif *et al.* [ABC15] do this. They examine what influences cultivating an information security culture within organisations, and they propose a framework for guidance in terms of information security culture management. They base their research on, among other things, the phrase "A culture of security within organisations will not arise by raising their security awareness only", and so they discuss some factors that have been postulated in addition to awareness to develop an information security culture. The three factors are awareness, behaviour, and culture, and within these three constructs, different variables have been defined. The suggested Information Security Culture life cycle uses awareness as a starting point while measuring security behaviour or compliance behaviour serves as the main element. Compliance behaviour, in turn, is constituted by different factors such as security policies within the company, and personal factors. These elements can be used together in order to assess security culture on a regular basis. However, changing or creating a security culture takes time, and the authors stress the fact that additional practical work is required to validate the proposed framework.

The previous paper proposes different variables to measure the culture and cul-

tural change in an organisation, but it does not specifically discuss how to change it. The most commonly suggested approach to promote security policy compliance is training. However, Puhakainen and Siponen [PP10] state that very few of the existing studies about training utilise theory to explain what learning principles affect user compliance, and moreover, that there is a lack of empirical evidence to show the practical effect of the training. With these thoughts in mind they have constructed a training program based on two specific theories, and in retrospect of that, they validate the efficiency of the program through an action research project. The project showed that the theory-based training achieved positive results and that a training program should utilise methods that activate and motivate the learners to systematic, cognitive processing of information. Another requirement for improving compliance was a continuous communication process.

In order to minimise human errors and thereby maximising the efficiency of security techniques, it is important to understand the underlying reasons for the errors. To facilitate this at an organisational level, a program based on a framework could be implemented to assure a systematic approach to the problem, as proposed by Puhakainen and Siponen [PP10]. However, due to the lack of understanding of problems related to awareness, such programs may turn out inefficient. Another paper by Siponen outlines two categories that may help increase this understanding, and the two categories are called *framework* and *content* respectively [Sip00]. The framework category contains issues that can be approached in a structural way, and that can be a part of quantitative research. The content category, on the other hand, should be approached using qualitative research methods. Traditionally, most measures have focused on the framework category, and the measures that have focused on the content category has only been descriptive, not accomplished-oriented. Siponen suggests that instead of simply distributing descriptive security guidelines to employees, one should aim at a prescriptive approach with intrinsic motivation as a goal. To facilitate this, he constructs a conceptual foundation for information systems/organisational security awareness, where he considers the normative and prescriptive nature of end-user guidelines. He also considers a behavioural science framework [Sip00, p. 33] to help understand human behaviour. The framework consists of intrinsic motivation [Dec75][ELD85], the theory of planned behaviour [IA75][Ajz91] and a technology acceptance model [Dav89].

A qualitative study of users' view on information security has been conducted by Albrechtsen [Alb07], discussing *the gap between end-users' motivation and action*, *the conflict between functionality and information security*, and *the usefulness of security campaigns*. Nine informants from two different companies were interviewed, and a pattern following the three aforementioned issues was recognised. One of the main

conclusions from this work states that general awareness campaigns have little or no effect alone on end users' behaviour and awareness. This coincides with the theory of Sherif *et al.* [ABC15] discussed earlier. Out of the nine informants from one of the companies, only one believed that the campaigns completed had an effect on the employees. In addition, only this one person could remember the last completed campaign. This is an interesting finding, and an issue that will be examined also in this thesis. It should be stressed that Albrechtsen's work should not be seen as generalised facts, rather the interpretation of some users' experience with the topic. Another conclusion suggests that risky behaviour has more benefits than cautious behaviour, which, according to Wilde's risk homeostasis theory [Wil82], explains the poor information security behaviour of users. Ergo, the cautious behaviour should be more attractive than the risky behaviour. Based on this last conclusion, it is suggested that security management should consist of more user involvement than is at present. This way, users may get a better understanding of the risks threatening the company, and which simple actions they can contribute with to mitigate them.

Three levels of awareness are explained by Shaw, Chen, Harris, and Huang [RSS09]. Perception is the lowest level of awareness and describes being able to understand the presence of a security threat. Comprehension is the second level of awareness, and is about understanding and assessing possible threats by integrating information obtained from different sources. The last and highest level of awareness is about predicting future situational events. This level is called projection and adopts the precautionary principle. The study refers to a survey conducted by more than 1000 teleworkers in 10 countries. The survey shows that regardless of the country, the teleworkers tend to have a higher degree of awareness than what their behaviour shows. Shaw *et. al* propose that available security awareness programs are not sufficient to cover all the levels of awareness described above. To overcome this deficiency, they suggest online security awareness programs with media richness including e.g. videos, interactive posters, and virtual reality. This is presumed to make the learning more effective for several reasons. One of the reasons is the fact that using the web makes it easier to stage real-world scenarios and learn from that. Another reason concerns the possibility of diversity in the material in digital learning. This fact makes it possible to suit the material to the users' needs and, hence, raise the learning interest. Three media covering three levels of media richness are studied to discover how they influence the effectiveness of online security awareness (SA) programs. Hypertext, multimedia, and hypermedia are the three media from lowest to highest richness, and an SA program was made in each category/level to be tested. Users with a comparable level of awareness were placed randomly in the three programs, and were to study the assigned material for one week. After the one week, the users completed a post-test assessment to evaluate the learning performance.

Analysis of the results showed a positive correlation between the levels of media richness and improvement of the level of awareness, and it was also found that the highest level of media richness is the most effective way of enhancing SA levels.

There is not much literature on the measurement of the effect of security awareness programs [HAK06], but Kruger & Kearney [HAK06] are two that address this issue. They claim that for a security awareness program to be of value to an organisation, it is necessary to measure its effect. In their paper, they report on the development of a prototype model for measuring exactly this. The goal of the model was to monitor change in the security behaviour in a company, and revise or repeat the awareness program/campaign depending upon results from the model. The awareness program that was implemented in conjunction with this study was focused on six critical risk areas. The measuring model was decided to measure knowledge, attitude, and behaviour, and each of these was then subdivided into the six focus areas of the campaign. Additionally, importance weights were allocated to all factors, as not all factors contribute equally to the final measurement. Questionnaires were designed to test the knowledge, attitude, and behaviour of the employees, and they inform that the incorporation of physical tests and other measures form part of an ongoing research process. The rather simple prototype tool was regarded as successful when applied in practice, but at the same time it offers several opportunities for enhancement.

Chapter 3
Methodology

This is a research project concerning, among other things, social science through studying relationships and connections between human beings and trying to disclose the reasons for their actions. This project also concerns compliance management, management influence, and awareness campaign effects. For many years, many researchers in the field of social science saw it necessary to choose between the more scientific-like quantitative research method and the "softer" qualitative method. The belief in having to choose between the two methods is called the 'incompatibility thesis', suggesting that the two different ways of viewing research are so different that they are incompatible with each other. Like [Gub87, p. 31] puts it, "The one [paradigm] precludes the other just as surely as belief in a round world precludes belief in a flat one." In later years, however, mixing the two methods for social research is gradually gaining recognition [Rob11, p. 17-18], commonly labeled mixed method research, or multi-strategy research, as by [Rob11]. Several advantages of mixing the two methods are given by Bryman [Bry06] including e.g. corroboration, complementarity, and development of one method based on results from the other. In this project, a quantitative analysis is good to measure changes in the company in a statistical way and gives a good mathematical background to confirm or deny hypotheses. A qualitative analysis is a good way to find a possible pattern in how people feel, or discover reasons for why people act as they do or feel as they do about a certain topic. In addition to this, it is also important to perform a thorough literature review to get a better understanding of the topic, get familiar with research that has already been done and find material that may substantiate potential theories that may arise along the conduction of this project. In the following subsections, the respective methods are explained further.

3.1 Quantitative Research Analysis through Simple Statistical Analysis

As a part of the awareness program at hand, a survey was conducted after each campaign round, resulting in three surveys in total. The surveys had a various number of predefined response alternatives and were answered by a mean of 808 employees. Some of the questions were changed from year to year, but the questions that remained the same give an advantage in that answers from one year can support the conclusion of a hypothesis drawn from another year. It is also advantageous in that possible changes in e.g. behaviour can be seen with more confidence. Regardless of this, data resulting from these surveys served as a good basis for quantitative analysis, and the numerous answers give statistically well-justified indications of confirmations or contradictions of hypotheses. Survey Monkey was used to conduct the surveys, and the employees were invited through internal platforms. Analysing the answers in Survey Monkey lets you compare answers between different response groups, showing a statistically significant difference using a standard 95% confidence level. This requires at least 30 responses in each compared group. This feature was used to investigate the relevant hypotheses that required comparison of different response groups within the same survey. When investigating the impact of the campaign, however, answers between the different surveys were compared, and the survey platform does not let you compare between different surveys, only within one survey. Harris Research Partners offers an online significance calculator (http://www.harrisresearchpartners.com/SigDiffCalculator.htm), and this was used to find the desired differences between the different years of the surveys. To check that the calculator gave reliable results, some tests were done manually and checked against the online calculator. The formula that was used to check was $P_1 - P_2 \pm 1,96 \left(\frac{P_1(1-P_1)}{Q_1}\right) + \left(\frac{P_2(1-P_2)}{Q_2}\right)$, P_1 and P_2 being the number of e.g. agreeing employees in Year 1 and 2 respectively, and Q_1 and Q_2 being the number of employees participating in the relevant question/statement in Year 1 and 2 respectively. This formula calculates a significance with 95% confidence level, and can be found e.g. in "Statistikk for høgskoler og universiteter" [Lø13].

3.2 Qualitative Research Analysis through Interviews

For this project, semi-structured interviews were implemented as part of the research. Performing interviews in a semi-structured manner allows the interviewer to make a guide and prepare the questions beforehand, but also lets him/her stray from the guide should the interviewee have interesting and relevant things to say. The questions should be open-ended in order to not steer the interviewee, and also to give the opportunity to identify new understandings of the topic [Rob11]. The interviews were subsequently transcribed and analysed using the template approach as guidance [oH]. According to Robson [Rob11], taping and transcribing the interview is of

considerable advantage whenever possible. This allows the interviewer to focus on conducting the interview and creating a good conversation, rather than getting distracted by having to take notes. The interviews were conducted face-to-face, which has several advantages to questionnaires online or over telephone [Rob11]. As this is a social study, social cues of the interviewees are very important and is much more easily noted in a physical presence. Physical presence also creates a closer connection between the interviewer and the interviewee, possibly making the interviewee feel safer and willing to answer more broadly and more personal. With this advantage, the questions asked can be more complex and open-ended as opposed to over e.g. the telephone. In addition, it allows for a longer conversation and more questions, giving the interviewer and the study more material to analyse and utilise.

The interview objects were chosen having in mind to represent the company at hand in a best possible manner. Six candidates were chosen from different organisational units, with different degrees of leadership responsibilities, in different age intervals and of different gender. The aim of such variety was to avoid answers that would lead to finding false patterns and, hence, possibly reaching a biased conclusion. The candidates were invited to take part in the study through e-mail, and they had to sign an information sheet stating that the interview would be recorded.

In advance of the interviews, a pilot interview was implemented. In order to make it as realistic a possible, the interview candidate picked was from the same company as the interviewees from the implemented study. The pilot aided in understanding how the interviewees interpreted the questions, and in revealing which questions worked well and which did not work so well, in order to refine them.

The interviews were transcribed and thematically analysed. As Boyatzis states [Boy98], thematic analysis is a process for encoding qualitative information, and consists of coding the transcribed text into themes. A theme is a pattern in the information that describes and organises observations. According to Boyatzis, a theme may be identified at the manifest level or at the latent level. The latter level includes what can be directly observed in the information, while the former involves the underlying phenomenon. In this project, the information from the interviews was organised and presented in a manner that resembles the manifest level. Though choosing this level may leave a lot of the richness of the raw material out [Boy98], the latent level may get too intricate and may make you lose focus of what you are actually analysing. As a beginner in the field, minimal interpretation has been done in order to prevent misinterpretations. However, as Malterud states [Mal11]: “Interpretation is an integral part of qualitative inquiry”, so some basic interpretations have been performed. Miller & Crabtree [MW99] present three qualitative analysis styles according to the degree of predetermined categories. For this analysis, the

template method was used, sorting the text into preexisting categories.

The transcripts were first studied individually, highlighting relevant and interesting words and phrases. The highlighted words and phrases were then rewritten onto one single page and sorted into four unrefined categories; *Organisation and Management*, *Information Security and Policies*, *The Information Security Campaign*, and *IT systems and tools*. The categories were not predetermined, but emerged with the processing of the material, and fitted well with the main topics of the questions in the interview guide. Further, the words and phrases from the six interviews were grouped together according to category, and words/phrases that were the same in the different interviews, or signified the same, were marked. This provided a good view of the similar, or different, outings within certain categories. Malterud [Mal11] says the following about qualitative research: "The findings from a qualitative study are not thought of as facts that are applicable to the population at large, but rather as descriptions, notions, or theories applicable within a specified setting."

3.3 Systematic Literature Review

A systematic literature review is a means of identifying, evaluating and interpreting research relevant to a specific topic. Performing a literature review following a systematic approach has several advantages as stated by Kitchenham [Kit04]. Some of the advantages include summarising existing evidence, identifying gaps in research on the topic, and providing a background on which to base new research. The following subsections provide a guideline on which the review for this project was based on.

3.3.1 Where did I search?

Google Scholar is a search engine that indexes academic literature across different disciplines. Hence, this is a good starting point when searching for relevant literature. Through this search engine, many good platforms were discovered, and included in this project are mainly articles from social networking sites specifically for scientists and researchers to share their work, and peer-reviewed academic journals that covers research about management information systems. Also, scholarly research databases were searched. The platforms used for this particular project include mainly:

- ResearchGate
- IEEE Xplore
- ScienceDirect
- MIS Quarterly

3.3.2 How did I search?

For this project, mainly articles, papers, reports etc. about information security in organisations has been searched for. Search terms that have been actively used are included in Table 3.1. Work on indirectly related articles were also searched for, like research on gender and age etc.

Information	Security	Organization
information	security	awareness
		campaigns
		culture
		behaviour
		training
		effectiveness
		policy
		management

Table 3.1: Related literature search terms

3.3.3 Article inclusion criteria

The abstracts of articles were examined and studied further if they were interesting and related to the topic. Some additional inclusion criteria for this specific literature review include:

- Articles must be related to the topic; directly or indirectly
- Articles must be peer-reviewed (from an approved networking site as described in subsection 3.3.1)
- Qualitative and quantitative studies can be included

3.4 Case Context

For this project, I will utilise data that has been systematically gathered over three years in conjunction with a campaign for information security awareness that was implemented in a research company. The campaign consisted of three individual "rounds", where each round was carried out during a certain period of time each year. The campaign consisted of different elements including several e-learning sessions, surveys, phishing e-mails, and general information and reminders. One e-learning session contained a short video clip raising a security issue and some PowerPoint slides explaining the issue further. A total of 11 e-learning sessions with

Campaign	Completion of e-learning(%)	Completion of survey (%)
Year 1	24,1	47,2
Year 2	59,3	43,6
Year 3	67,3	38,5

Table 3.2: Campaign and survey participation each year

Total number of employees	2000
Men (%)	67
Women (%)	33

Table 3.3: Gender distribution in the company

different topics were posted on the company's internal web page in three batches. The first four e-learning sessions were made available in October 2014, the next four in November 2015, and the last three were published in November 2016. The goal of the e-learning was to inform the employees about serious, potential security breaches threatening the company, with a humorous twist. The number of users per department completing the e-learning sessions has been accumulated each period, and the percentage of participants per department can be seen in Table 3.2. The material was made available for everyone, i.e. a total of around 2000 people, but was not mandatory. However, the employees were highly encouraged to complete them. In addition to the e-learning, the campaign also consisted of some constructed phishing e-mails that were sent to the employees, and general, continuous reminders during the campaign in the form of posters, roll-ups and informational e-mails. A survey was conducted the following year of each round, so in 2015 a survey was conducted for the campaign of 2014 etc. The campaign of 2014 with the corresponding survey will be referred to as Year 1, the campaign of 2015 with corresponding survey Year 2, and the campaign of 2016 with the survey is called Year 3. The aim of the surveys was, among other things, to find out whether or not the participants found the program useful, to what degree they feel responsible for contributing to a good security culture, and to what extent they feel like they know what secure practice is. A total of 11 e-learning sessions were made available from Year 1 to Year 3, raising security issues like phishing, physical access and ID, locking of the computer when leaving it, USB memory sticks, Cloud and classification, secure while travelling, password etiquette, and scam. In Table 3.2 and 3.3 some key numbers are listed. These numbers will be used, and referred to, in Results (4).

3.5 Ethical Issues

In order to record the interviews for the qualitative analysis, an inquiry had to be issued to, and approved by, the Norwegian Centre of Research Data. Upon approving such an inquiry, this instance requires that the interview candidates are informed about the details regarding recording, anonymisation, and a date of deletion of the acquired material. Hence, a request for a declaration of consent was sent to all the candidates, informing about the relevant rules and details. All interviewees were made anonymous in retrospect of the interviews so that nothing that was said could be traced back to any specific individual. The surveys following the campaign rounds were made available through a shared link on the company's intranet, and are not linked to names or e-mail addresses. Upon the completion of this project, all associated personal data will be deleted, including the recordings and transcripts.

Chapter 4
Results

The results are mainly presented in line with the research questions posed in the Introduction (1). The two first research questions have been explored by the aid of the six hypotheses that are also posed in the Introduction, and the results from the individual hypotheses will be presented here. Most of the results from the different hypotheses originate from survey data, and the results from the interviews are presented separately at the end of this chapter. The reason for this is that the contents of the interviews are rather loosely tied to the very specific hypotheses. Instead, they give a more general view of the information security picture in the company. Although they do not answer any of the specific hypotheses, they give some insight into the employees' perception of information security and things that may be related to this. The analyses of the interviews also give a good basis for answering *RQ3*, together with the results and discussions of *RQ1* and *RQ2*. The last research question [RQ3] is, therefore, presented lastly in the Discussion and can be considered a conclusion of the discussion of the two first research questions [RQ1 and RQ2], and the interviews.

To help the exploration of the different hypotheses, certain statements from the surveys have been chosen to be examined. The answer alternatives to some of the statements explored range from *Highly agree* to *Highly disagree*, and this will sometimes be referred to only as *agreeing* or *disagreeing*, which constitutes *Highly agree* together with *Slightly agree*, and *Highly disagree* together with *Slightly disagree* respectively.

In total, six objects were interviewed in conjunction with this project. The interview candidates covered the four age groups considered in this project (under 35, 35-44, 45-54, 55 and over), four different organisational units, and five different organisational divisions. Out of the six interviewees, five were male, and out of the four listed management responsibility levels, all were covered.

- RG1: Employees whose work does not involve any management responsibility
- RG2: Employees whose work require management responsibility in projects
- RG3: Employees with management responsibility in divisions
- RG4: Employees with management responsibility in an organisational unit

The results from the interviews will be presented lastly in this chapter.

4.1 The influence of age, gender, and management position

The first research question, *How do factors like gender, age and management position influence attitudes towards information security and information security training?*, was explored by analysing the four first hypotheses stated in the Introduction. The four hypotheses are presented in the four following subsections, the first concerning gender, the second concerning age, and the two last regarding management responsibility level.

4.1.1 H1: Women are more positive towards security training than men

The first hypothesis was investigated by comparing the two response groups *Men* and *Women*. The possibility to compare these groups only appears in Year 2 and Year 3. The distribution of participation in Year 2 was 64% men and 36% women, and in Year 3, 62% of the answers were from men and 38% from women. Figure 5.1 shows a visualisation of the mean of the mentioned numbers.

The statements/questions that will be used to investigate this hypothesis are listed in Table 4.1.

	Statement/question	Year
1	Who do you learn the most about information security from?	2 and 3
2	I have completed the campaign's e-learning sessions	2 and 3
3	My knowledge about the topic is sufficient for my work situation	2 and 3
4	I want to learn more about information security	2 and 3
5	What are the biggest motivations to learn more about information security?	2

Table 4.1: Statements examined in conjunction with *H1* and *H2*.

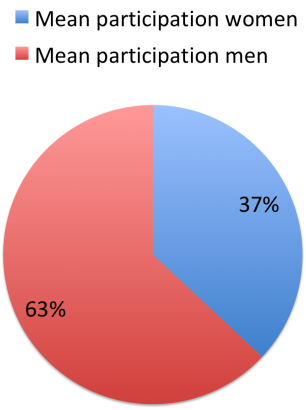


Figure 4.1: This is a visualisation of the mean distribution of male and female participation in the surveys of Year 2 and 3.

Statement 1 A factor that is interesting to review is from whom the two respondent groups learn the most about information security. There were several answer alternatives, but the two most interesting to look at were: "I learn most on my own" and "I learn most from the campaign". The mean of Year 2 and 3 is visualised in Figure 4.2, and as can be seen, a clear majority of men answered that they learn most from themselves, compared to women. The majority of the women stated to learn most from the campaign.

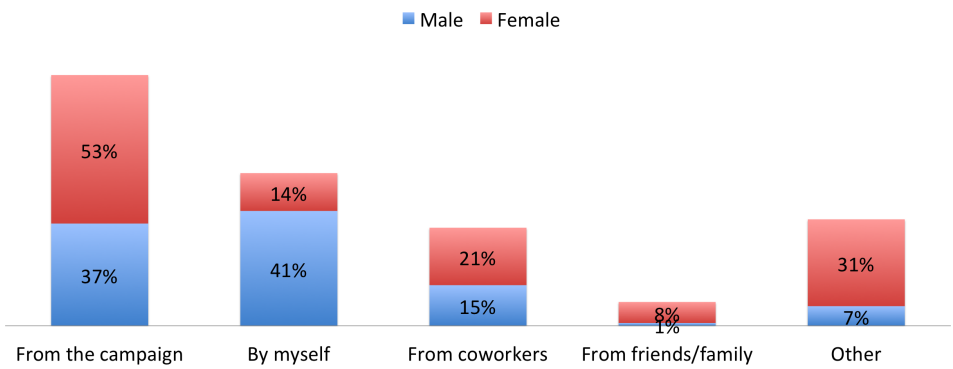


Figure 4.2: A visualisation of the mean of men and women's answers to Statement 1, *Who do you learn the most about information security from?*

Statement 2 In both years, the majority of both response groups affirm that they have completed the e-learning, but there is still a significant difference between them. As illustrated in Figure 4.3 a mean of 94% of the women and 89% of the men agreed that they had completed it. Also, a significantly bigger part of the men answered that they cannot remember, compared to the women (8% to 3%).

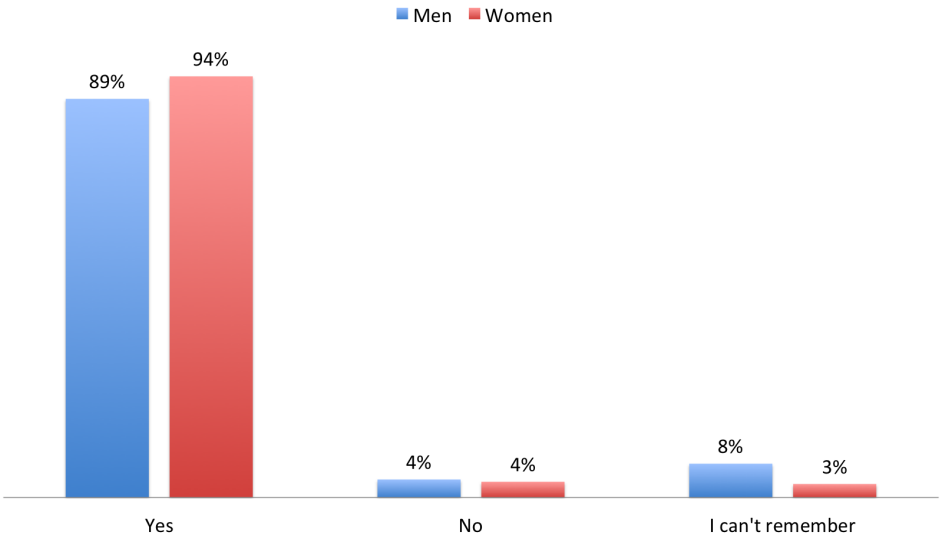


Figure 4.3: A visualisation of the mean of men and women's answers to Statement 2, *I have completed the e-learning sessions.*

The alternatives for Statement 3 and 4 from Table 4.1 are of a sliding scale including the following alternatives: *Highly disagree*, *Slightly disagree*, *No opinion*, *Slightly agree*, and *Highly agree*.

Statement 3 On average, the agreeing side and the disagreeing side are equally big for both genders when asked if they believe that their knowledge about information security is sufficient for their work situation. However, as Figure 4.4 shows, there is some difference in to which degree the genders agree; more of the men tend to highly agree, while more of the women only slightly agree. The average difference between men and women in highly agreeing is significantly big.

Statement 4 In Figure 4.5 the mean of the answers from Year 2 and 3 are shown, and as can be seen, more women than men agree to want to learn more about information security. In fact, significantly more women agree, and as the graph shows, they are also the majority in highly agreeing whereas most of the agreeing men only slightly agree. Both of the response groups are very small on the disagreeing side.

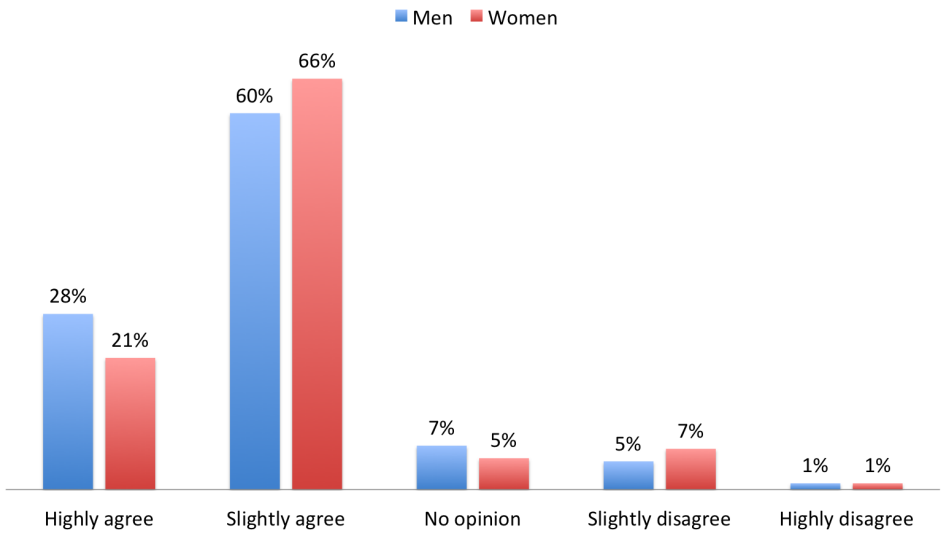


Figure 4.4: A visualisation of the mean of men and women's answers to Statement 3, *My knowledge about the topic is sufficient for my work situation.*

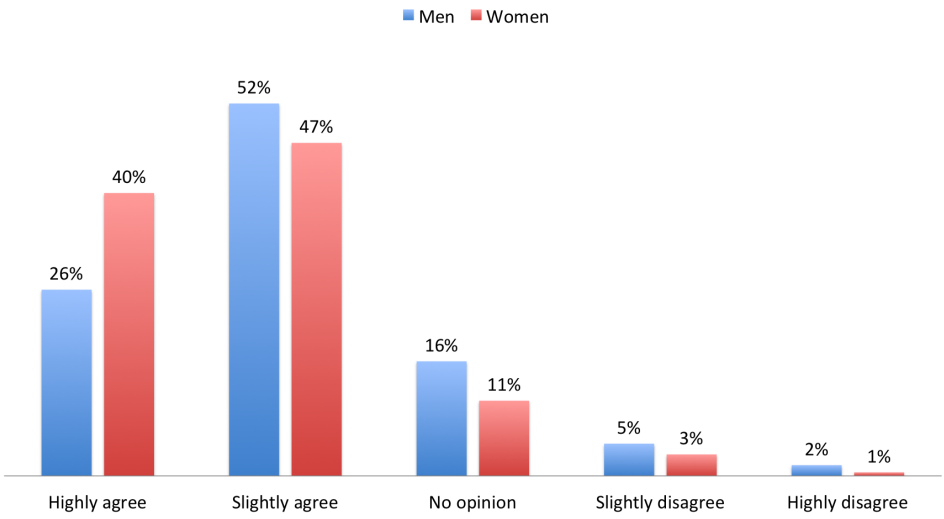


Figure 4.5: A visualisation of the mean of men and women's answers to Statement 4, *I want to learn more about information security.*

Statement 5 One last thing that is curious to examine is if there are any significant differences in what the motivations to learn about information security are. This question was given with twelve answer alternatives, whereof only one of

them show a significant difference; *Because I got a diploma upon completing the e-learning*. This motivation/reason for learning about information security is the least chosen alternative for both response groups. However, the relative number of female employees choosing this was significantly higher than the number of male employees, measuring 3% to 1% respectively. Figure 4.6 shows the two response group's answers to all alternatives. Note that each employee could choose several alternatives.

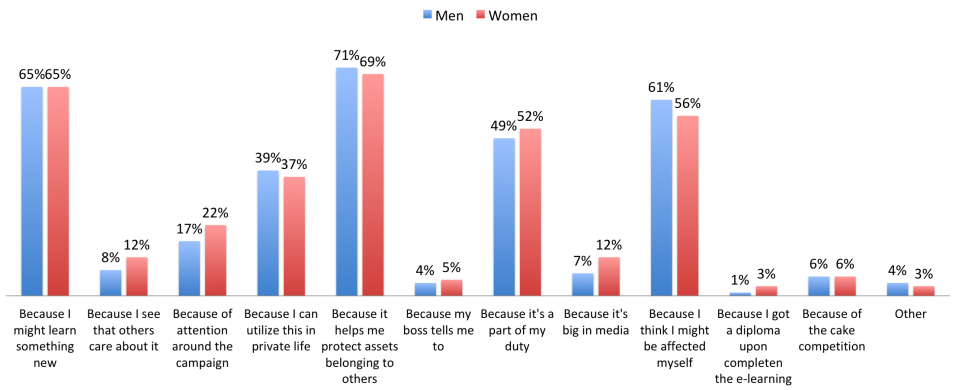


Figure 4.6: A visualisation of men and women's answers to Statement 5, *What are the biggest motivations to learn more about information security?*

4.1.2 H2: Age plays a role in the positivity towards security training

The second hypothesis, *Does age play a role in the positivity towards security training?*, was explored by comparing four response groups, sorted in the following age intervals: Under 35, 35-44, 45-54, 55-. For easier name convention, the response groups (RG) will sometimes be referred to as RG1, RG2, RG3 and RG4, describing the following:

- RG1: Employees under 35
- RG2: Employees between 35-44
- RG3: Employees between 45-54
- RG4: Employees from 55 and up

The statements and questions examined are the same as for the investigation of gender in 4.1.1. However, as the age distribution of the employees in the company

is not public knowledge, it is not possible to calculate the relative amount of the different age groups participating in the survey, as was possible with gender.

Statement 1 Noticeable differences can be seen between the response groups on average in Figure 4.7. The youngest response group (RG1) is the decidedly smallest in admitting that they learn most from the campaign, and a direct positive correlation can be seen between age and *I learn most from the campaign.* RG1 is significantly smaller than the other response groups in choosing this alternative, and RG4 is significantly bigger than all the other groups. At the same time, the youngest group (RG1) is significantly bigger than all other groups to state that they learn most from themselves. Although there is no direct negative correlation between age and *I learn most from myself*, RG4 is significantly smaller than the other groups in stating this. Two other interesting differences can be seen, namely that relatively, significantly more of the oldest employees (RG4) say that they learn the most from co-workers, compared to the youngest age group (RG1). In general, there is a direct positive correlation between age and *I learn most from my co-workers.* RG4 is also significantly lower than the youngest age group (RG1) in stating that they learn the most from friends and family, and also here there is a direct correlation, but negative.

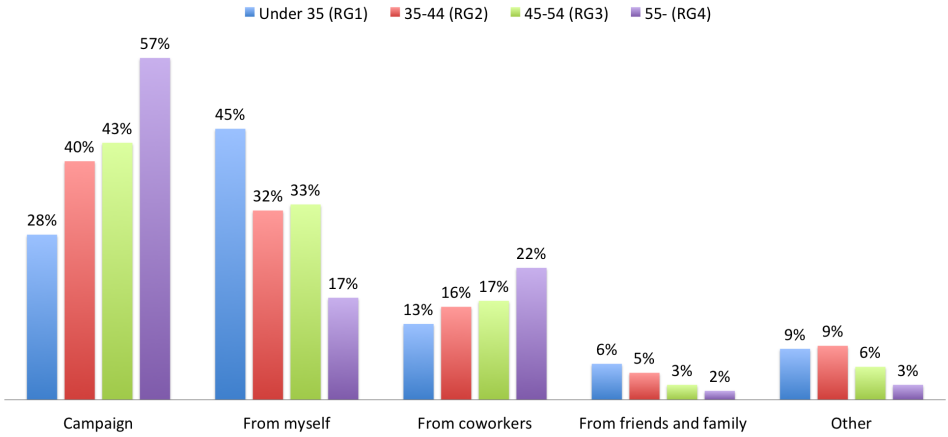


Figure 4.7: A visualisation of the mean of the different age groups' answers to Statement 1, *Who do you learn the most about information security from?*

Statement 2 The second interesting thing to look at is the distribution of who has, and who has not completed the e-learning sessions of the campaign. As seen in Figure 4.8, an average direct positive correlation can be seen between age and completed e-learning. The youngest group (RG1) is significantly smaller than the two oldest (RG3 and RG4) in saying *Yes.* No other significant differences are seen on average, but the direct negative correlation between age and *I cannot remember* may be noted.

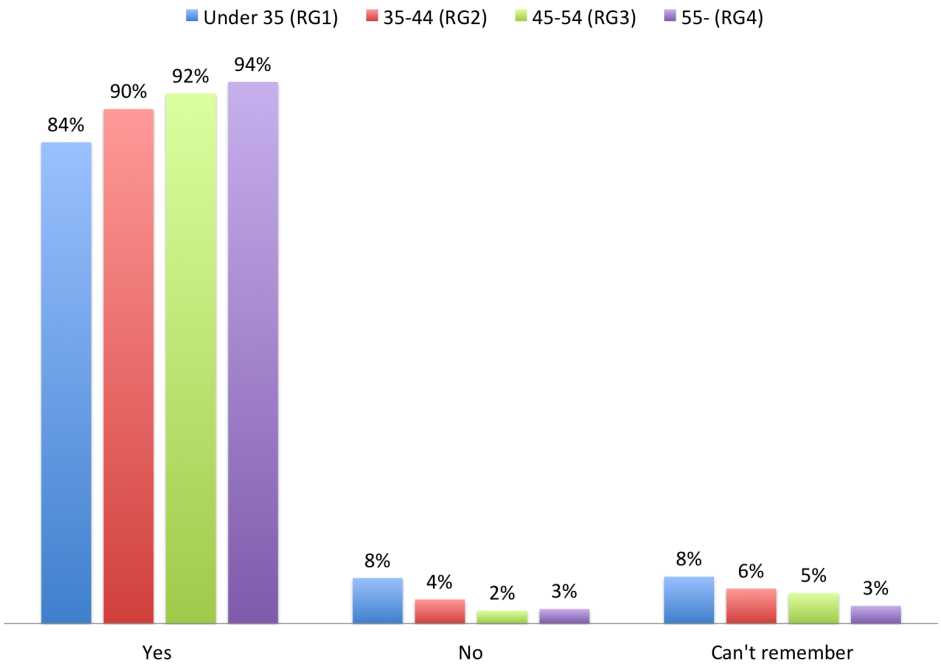


Figure 4.8: A visualisation of the mean of the different age groups' answers to Statement 2, *I have completed the campaign's e-learning sessions.*

Statement 3 On average, the majority of all response groups agreed to have sufficient knowledge about information security for their work tasks, and no direct correlations exist. The youngest groups of employees (RG1 and RG2) are minimally smaller than RG3 and RG4 to agree, having the same group size. However, RG1 is significantly bigger than RG2 in highly agreeing. Other than that, no noteworthy differences or trends exist.

Statement 4 Looking at the statement *I want to learn more about information security*, the agreeing side shows an almost direct positive correlation; the two youngest groups (RG1 and RG2) are the same size, but the size grows with RG3 and RG4. It is also evident that having no opinion directly correlates negatively with age. A small negative correlation can also be seen on the disagreeing side. That said, none of the differences seen is significant. Figure 4.10 shows how the different age groups agree and disagree to Statement 4.

Statement 5 As for gender, it would be interesting to see if there are any significant differences between the four age groups regarding motivations for learning about information security, and it turns out that four out of the twelve alternatives

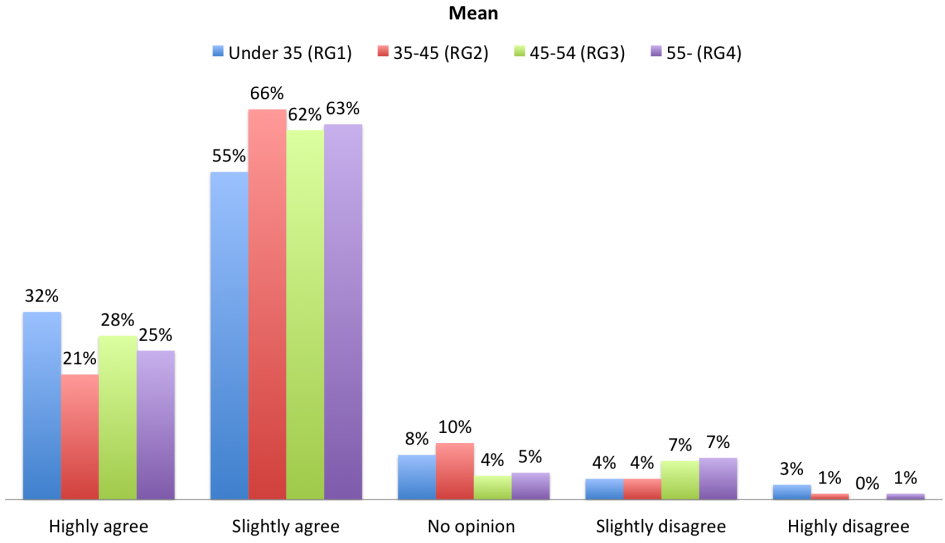


Figure 4.9: A visualisation of the mean of the different age groups' answers to Statement 3, *My knowledge about the topic is sufficient for my work situation.*

show some interesting differences. *Because it is popular in the media* is one of them, and the relative number of employees under 35 is significantly higher than all other response groups in choosing this alternative. Figure 4.11 shows the distribution of votes between the possible motivation alternatives.

The second reason worth mentioning is *Because of attention around the campaign*, where it can clearly be seen that RG4 is significantly higher than RG3 and RG2, and higher than RG1.

Though it is one of the alternatives with the least votes in total, it can be observed that the reason *Because my boss tells me to* appears to the minority of the oldest employees. While 3%, 6%, and 6% of RG1, RG2, and RG3 respectively chose this alternative, only 2% if RG4 did, resulting in RG4 being significantly lower than RG2 and RG3.

By the end of every campaign, the department with the highest degree of completion of the e-learning sessions won a cake, and this results in the last reason/motivation to be examined; *Because of the cake competition.* This alternative shows a very apparent difference in the response groups, where the youngest response group favours the competition to a significantly bigger extent than the two oldest. The oldest response group favours it to a significantly smaller extent than the two youngest.

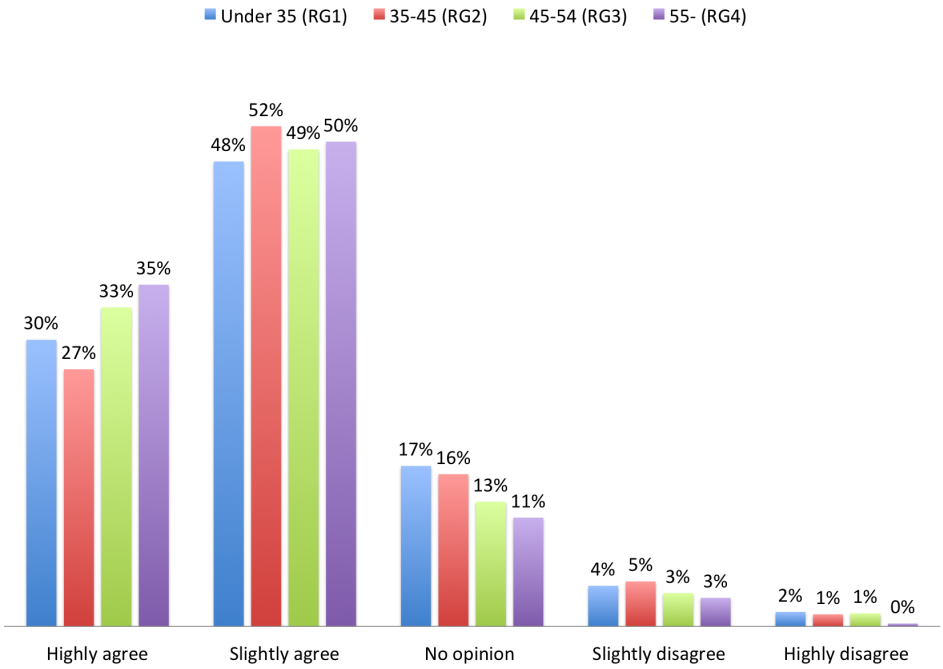


Figure 4.10: A visualisation of the mean of the different age groups' answers to Statement 4, *I want to learn more about information security.*

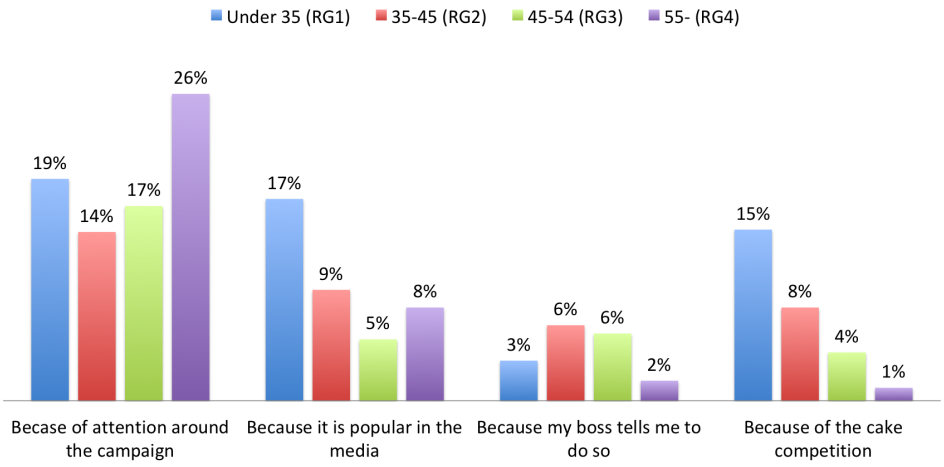


Figure 4.11: A visualisation of the age groups' answers to Statement 5, *What are the biggest motivations to learn more about information security?*

RG1	Employees whose work doesn't involve any management responsibility
RG2	Employees whose work require management responsibility in projects
RG3	Employees with management responsibility in divisions
RG4	Employees with management responsibility in organisational unit

Table 4.2: Four different groups of employees with different management responsibilities are explored. The table contains project-specific abbreviations of the names of the response groups, and an explanation of the responsibilities of the respective response groups.

4.1.3 H3: Employees with higher management responsibilities feel more responsible with regard to information security than those with lower management responsibilities

In order to explore the third hypothesis, four response groups (RG) have been compared. The response groups are listed in Table 4.2. The response groups are numbered from 1-4, where a higher number indicates a higher level of responsibility. The statements that will be used to compare the response groups are listed in Table 4.3.

	Statement/question	Year
6	I feel responsible for maintaining a high level of information security	1, 2, and 3
7	I think I could be a target for actors that try to steel information from the company	1, 2, and 3
8	I am familiar with the information security policies of the company	1, 2 and 3
9	What are the biggest motivations to learn more about information security?	2

Table 4.3: Statements examined in conjunction with *H3*.

Statement 6 The first and most evident statement to examine is to which extent the employees agree to being responsible for contributing to maintain a high level of information security in the company.

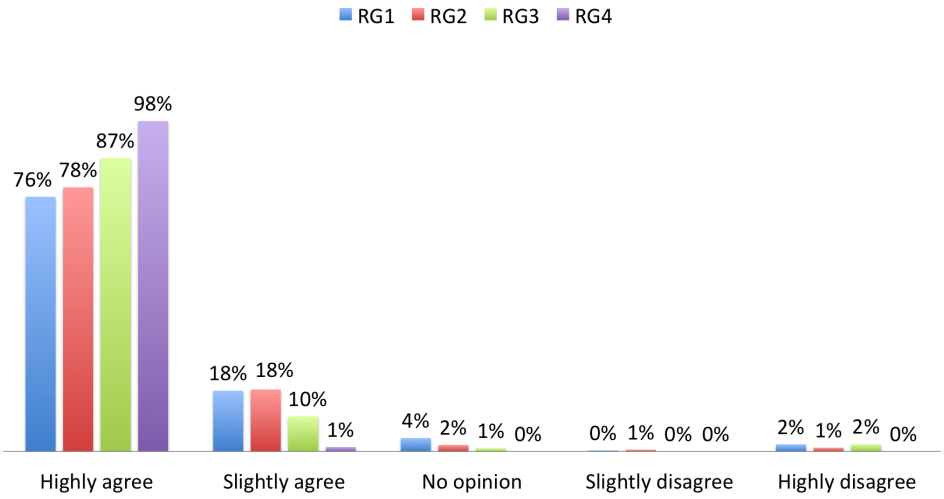


Figure 4.12: A visualisation of the mean of the management levels' answers to Statement 6, *I feel responsible for maintaining a high level of information security.*

The alternatives to the statement scale from *Highly disagree* to *Highly agree*. The majority of all response groups indicated to agree all three years, and the amount of employees on the disagreeing side is minimal. The mean shows a slight direct correlation between *agreeing* and *level of responsibility*, and the difference between the lowest level of management responsibility (RG1) and the highest level (RG4) is significant. Two other interesting things are the correlation between responsibility level and having no opinion, and the difference between the four groups on highly agreeing. A visualisation of the mean of the three years is given in Figure 4.12.

Statement 7 Also for this statement, the answer alternatives range from *Highly disagree* to *Highly agree*, and the mean of the different response groups' answers are illustrated in Figure 4.13. As can be seen, the majority of all groups agree.

The mean shows clear correlations on both the agreeing side and the disagreeing side, as well as on the alternative *I have no opinion*. On the agreeing side, the group size increases consistently with responsibility level, and on the disagreeing side and *I have no opinion*, the group size decreases with management responsibility. The group with least management responsibility (RG1) is significantly smaller than the to groups with most responsibility (RG3 and RG4) in agreeing, and significantly bigger than the two in disagreeing.

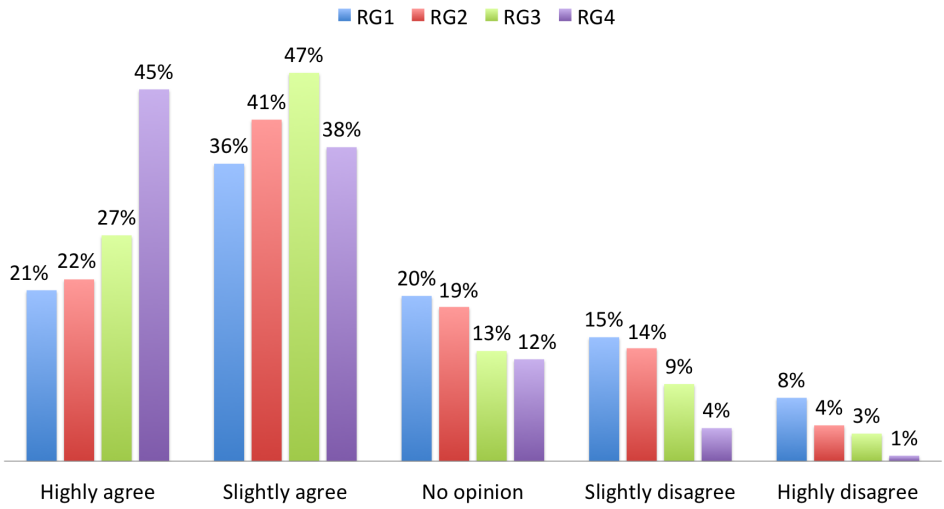


Figure 4.13: A visualisation of the mean of the management levels' answers to Statement 7, *I think I could be a target for actors that try to steal information from the company.*

Statement 8 A factor that could be interesting to investigate when considering the feeling of responsibility is to which extent the different response groups are familiar with the company's information security policies. Figure 4.14 illustrates the mean distribution of answers between the groups.

On average, there is a direct positive correlation between the agreeing side and responsibility level, where the group with the highest level of responsibility (RG4) is significantly bigger than all the other groups. This group is also significantly smaller than all others in disagreeing to Statement 8, and the smallest in having no opinion.

Statement 9 As for the two foregoing comparisons, Gender and Age, the biggest motivations for the different responsibility levels have been examined, and out of the twelve alternatives, three are noteworthy. The answers can be seen in Figure 4.15. The reason with the most indisputable differences is *Because I can utilise it in private life*, where employees with the most responsibility (RG4) are significantly fewer than all other response groups.

The reason *Because I can learn something new* was chosen by a significantly higher number of employees with no management responsibilities (RG1) compared to the group with one level higher responsibilities (RG2). Although RG1 is not significantly higher than RG3 and RG4, it is still noticeably higher. It should be noted that this is the alternative with the second most votes in total.

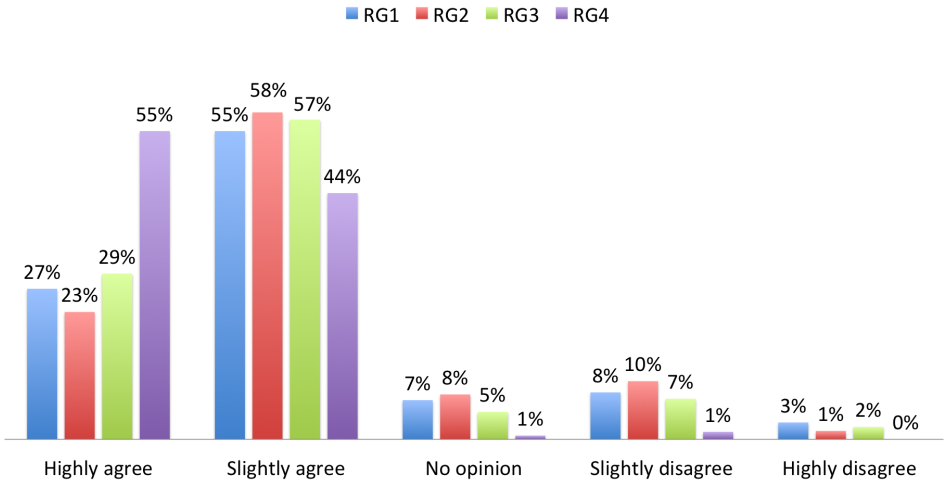


Figure 4.14: A visualisation of the mean of the management levels' answers to Statement 8, *I am familiar with the information security policies of the company.*

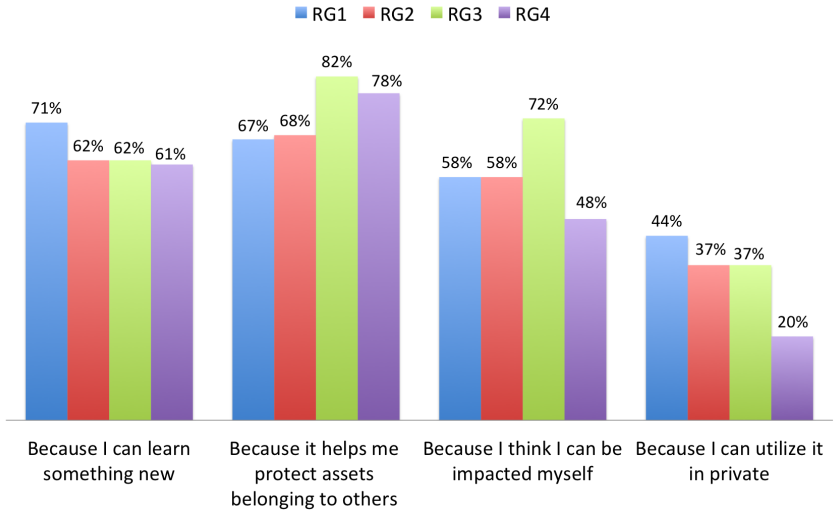


Figure 4.15: A visualisation of the managements levels' answers to Statement 9, *What are the biggest motivations to learn more about information security?*

Because it helps me protect assets that belong to others is the reason that in total has the most votes, and the distribution among the four response groups is 67% (RG1), 68% (RG2), 82% (RG3), and 78% (RG4), where RG3 is significantly higher than RG1 and RG2.

4.1.4 H4: Employees with higher management responsibilities act more securely with regard to information security than those with lower management responsibilities

For the exploration of *H4*, four appropriate statements will be examined, all of them based on some of the official information security policies of the company. The statements are given in Table 4.4.

	Statement/question	Year
9	I always lock my computer screen when I leave it	1 and 2
10	I utilise several methods to verify the content of an e-mail	1 and 2
11	I let other people borrow my work computer	2 and 3
12	I always connect to VPN when connecting to public WiFi	2 and 3

Table 4.4: Statements examined in conjunction with *H4*.

Statement 9

On average, all response groups are on the agreeing side, and the majority of all groups say that they highly agree. The group with the highest level of management responsibilities (RG4) is significantly bigger than all other groups to agree, and the decidedly smallest group to disagree. Only 1% admitted to slightly disagree, which is significantly smaller than the other groups. As can be seen in Figure 4.16, there is no direct positive correlation between responsibility level and locking the computer, RG1 is actually bigger than both RG2 and RG3 in agreeing in general, but also to highly agreeing.

The mean of the two years the statement was posed can be seen in Figure 4.17. On average, RG2 is the smallest group to agree, followed by RG1 and RG4 which have the same relative size, and RG3 is the biggest. This order (just opposite) can also be seen on the disagreeing side. There are no significant differences on average.

Statement 11 The third action-related statement concerns lending of work computer. The employees are given the five alternatives *Never*, *Only spouse/partner*, *Children/family*, *Not relevant*, and *Other*. The mean of the answers to all alternatives can be seen in Figure 4.18, and as the figure shows, there are only very small

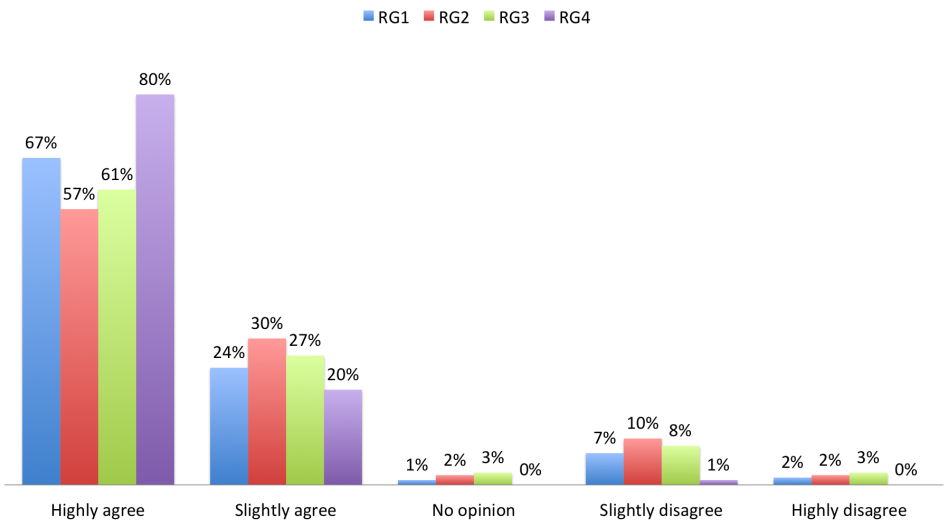


Figure 4.16: A visualisation of the mean of the management levels' answers to Statement 9, *I always lock my computer screen when I leave it.*

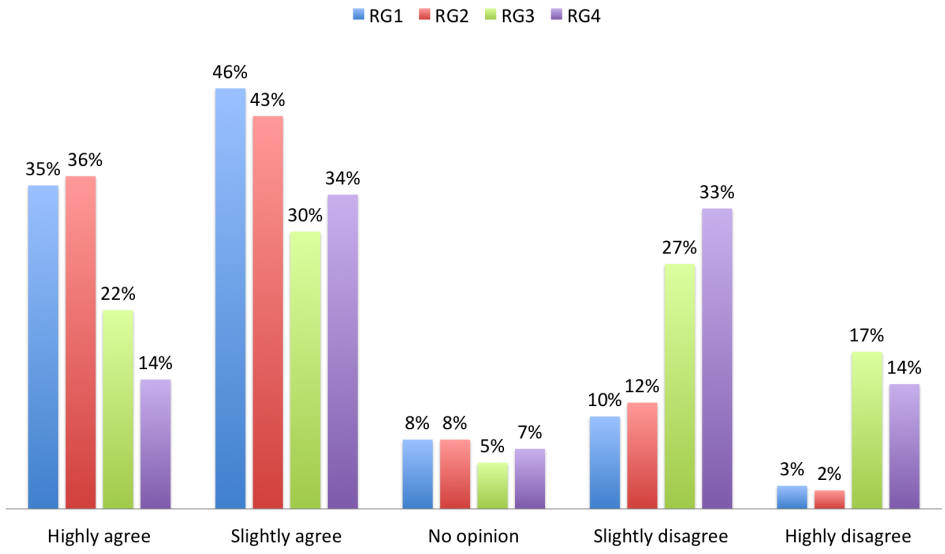


Figure 4.17: A visualisation of the mean of the management levels' answers to Statement 10, *I utilise several methods to verify the content of an e-mail.*

differences. RG4 is barely the biggest to answer *Never*, and barely the smallest to answer *Spouse/partner* or *Children/family*, closely followed by RG1 in all three cases.

RG2 and RG3 are the two smallest groups to answer *Never* and the two biggest to answer *Spouse/partner* or *Children/family*.

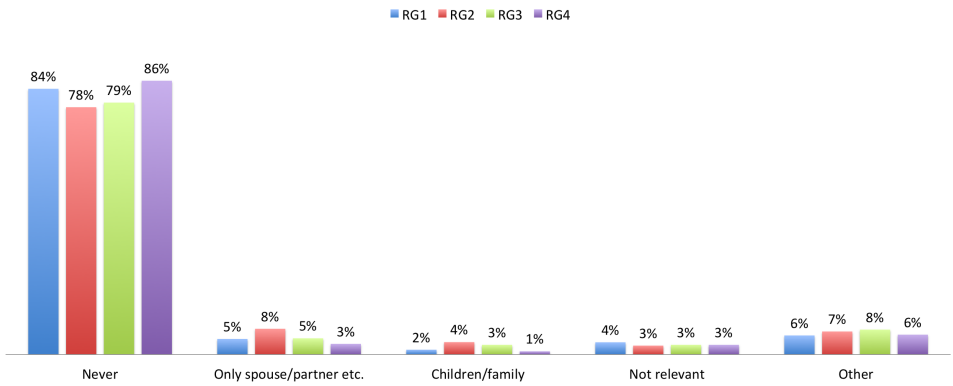


Figure 4.18: A visualisation of the mean of the management levels' answers to Statement 11, *I let other people borrow my work computer*.

Statement 12 The use of VPN when connecting to public WiFi's is the last action-related statement to be examined. As Figure 4.19 shows, the group of employees with the highest management responsibility level (RG4) is the biggest to agree, and the group size decreases with responsibility level, showing a direct positive correlation between responsibility level and the use of VPN.

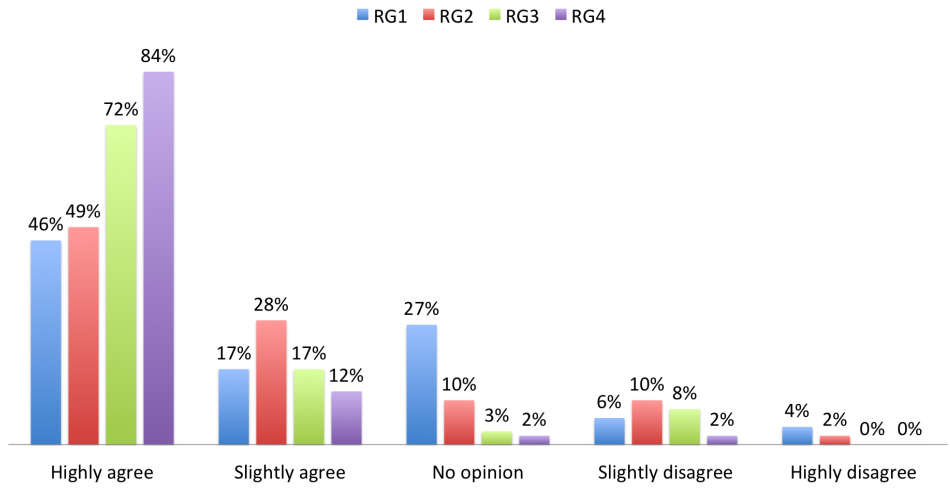


Figure 4.19: A visualisation of the mean of the management levels' answers to Statement 12, *I always connect to VPN when connecting to public WiFi*.

Nb.	Statement	Year
13	I have visited the e-learning videos	1
14	I have completed the e-learning videos	2 and 3
15	The campaign has motivated me to strive for good information security practice	1 and 3
16	Who do you learn the most about information security from?	2 and 3
17	I want to learn more about information security	2 and 3

Table 4.5: Statements examined in conjunction with *H5*.

4.2 The security awareness campaign's effect on employees

The second research question, *How does the implementation of a security awareness campaign affect employees knowledge of the topic, and their behaviour?*, was explored by analysing hypothesis 4 and 5 stated in the Introduction. The two hypotheses are presented in the two following subsections. The hypotheses are analysed by comparing answers from identical statements/questions over the three years from the surveys. As there is some variety in which statements are the same in the three surveys, all three will be considered, where either Year 1 and 2 will be compared, Year 2 and 3, or Year 1 and 3. Evidently, comparing Year 1 to Year 3 would give results with more certainty, as the employees should learn more over two years than one, so this should be taken into account when analysing the results. Table 4.5 and 4.6 give an overview of the statements explored for the fifth and sixth hypothesis respectively, and from which years they are compared.

4.2.1 H5: Employees are more positive toward information security/training by the last campaign round than they were in the first

The fifth hypothesis is hard to evaluate, as numbers do not directly reveal feelings or attitudes. Still, some statements from the surveys are chosen that may facilitate in indicating some kind of change in attitude towards information security training, or more specifically, the campaign. The statements are given in Table 4.5

Statement 13 and 14 The two first statements are formulated somewhat different in Year 1 compared to in Year 2 and 3, and are therefore listed as two

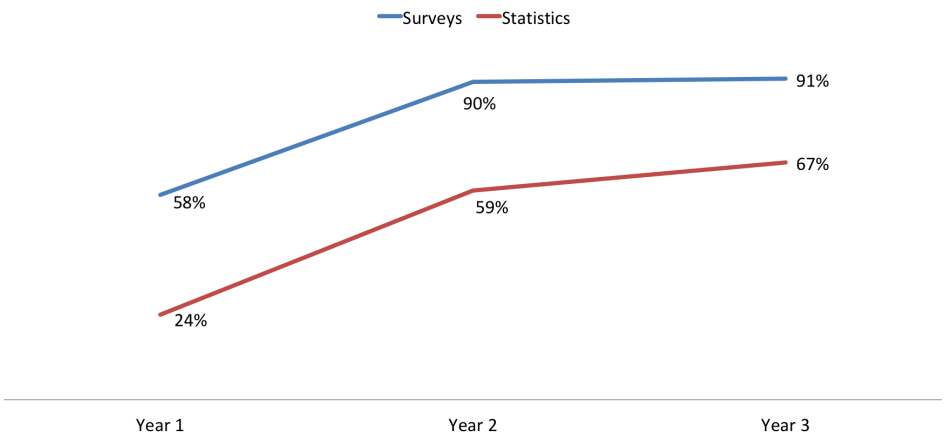


Figure 4.20: Completed e-learning sessions from Year 1 to Year 3.

different statements, but essentially they say the same thing, and they are therefore compared as if they were the same statement. In Year 1, 58% stated that they had visited the videos, in Year 2, 90% said they had completed the e-learning, and 91% said they had completed it in Year 3. The increase from Year 1 to Year 2 is significant, while the increase from Year 2 to Year 3 is not. In addition to looking at the surveys, it is interesting to look at the statistics to see how many actually completed the videos each year in total, independently of who answered the associated surveys. From Year 1 to 2 it can be observed that the number of employees completing the e-learning sessions increased quite a lot compared to from Year 2 to 3. Also here, the difference between Year 1 and 2 is significant, while from Year 2 to 3 is not. When looking at the statistics individually for each department, it is seen that all departments increased their completion rate from Year 1 to Year 2, while from Year 2 to Year 3 some departments actually decreased the completion rate. Thereof the steep slope Year 1-Year 2 and the evener slope Year 2-Year 3. The completion rates from Year 1 to Year 3 for both the surveys and the statistics can be seen in Figure 4.20.

Statement 15 As can be seen in Figure 4.21, more people feel motivated to strive for good information security practice at the end of the campaigns compared to in the beginning. Not only did the total agreeing side increase significantly, but the number of employees to highly agree also increased fairly. Also, the disagreeing side decreased significantly from Year 1 to Year 3.

Statement 16 Figure 4.22 clearly shows a positive shift in favour of the campaign in that the number of employees answering that they learn the most from the campaign increased significantly, and at the same time significantly fewer employees answered

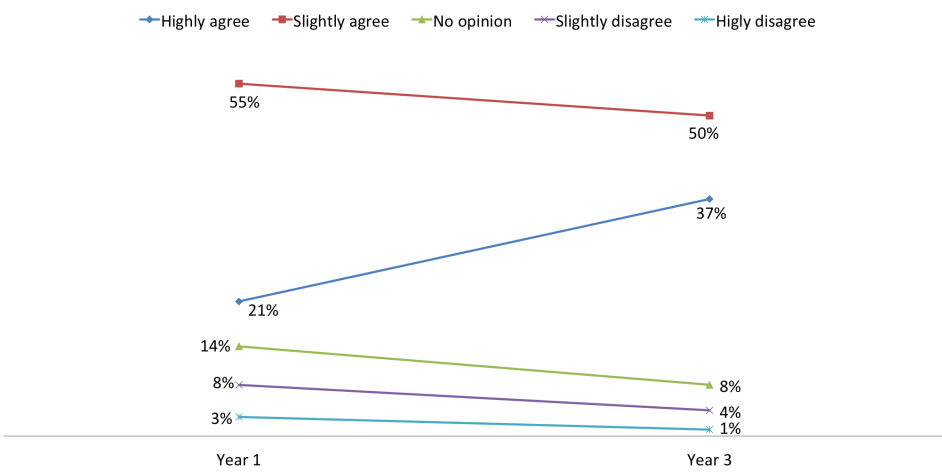


Figure 4.21: Comparing Statement 15, *The campaign has motivated me to strive for good information security.*

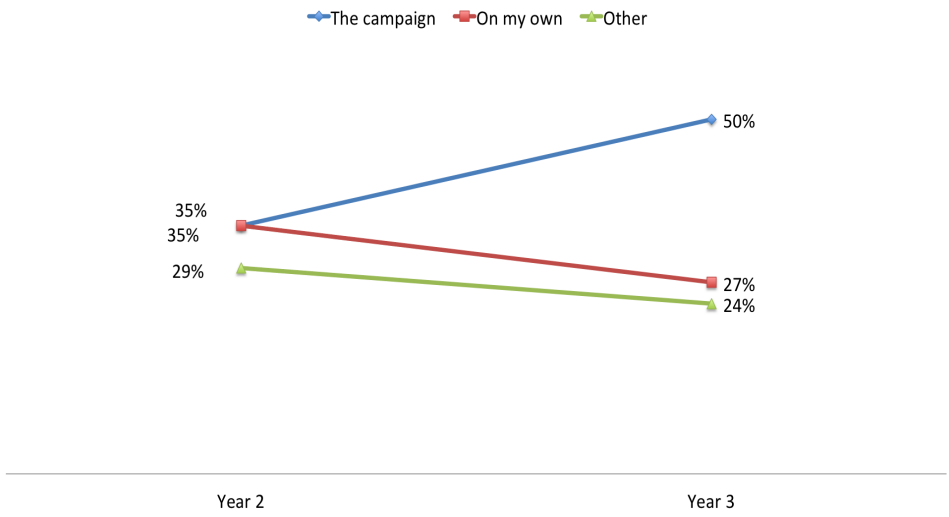


Figure 4.22: Comparing Statement 16, *Who do you learn the most about information security from?.*

that they learned the most by themselves. The other answer alternatives stay fairly stable.

Statement 17 The answers to the statement *I want to learn more about information security* are visualised in Figure 4.23. In total, the agreeing side increased

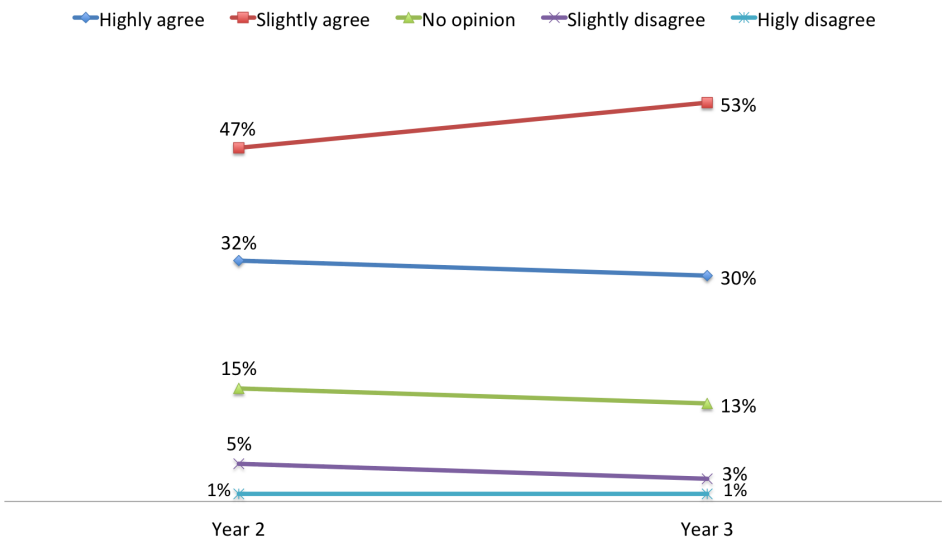


Figure 4.23: Comparing Statement 17, *I want to learn more about information security.*

somewhat and the disagreeing side decreased, but none of the changes is significant, so they might only be natural variations.

4.2.2 H6: Employees act more securely by the last campaign round than they did in the first

The sixth hypothesis is easier to examine, as results from the surveys show the actions of the employees directly, there is no need to interpret the numbers in the same way as for *H5*. The statements explored, and from which years they are compared, are given in Table 4.6.

Statement 18 As can be seen in figure 4.24, there is a slightly positive development every year in the percentage of employees who lock their computer screens when leaving it. The increase from Year 1 to Year 2 is significant, while the increase from Year 2 to Year 3 is not. One can also see that the percentage of employees highly disagreeing or slightly disagreeing has decreased, albeit minimally.

Statement 19 The results from this statement show a significantly positive development in the percentage of employees utilising several methods to verify the

	Statement	Year
18	I always lock my computer when I leave it	1 and 3
19	I use several methods to check the contents of an e-mail before I open any attachments or click any links	1 and 2
20	I always use a USB memory stick to exchange files, also when dealing with computers that don't belong to my company	1 and 3
21	I feel uncomfortable asking people I don't recognise for ID if they are not wearing any	1 and 3
22	I prefer Google Docs, Dropbox or other cloud-based solutions to work on documents simultaneously	1 and 2
23	I sometimes intentionally break rules for information security	2 and 3

Table 4.6: Statements examined in conjunction with *H6*.

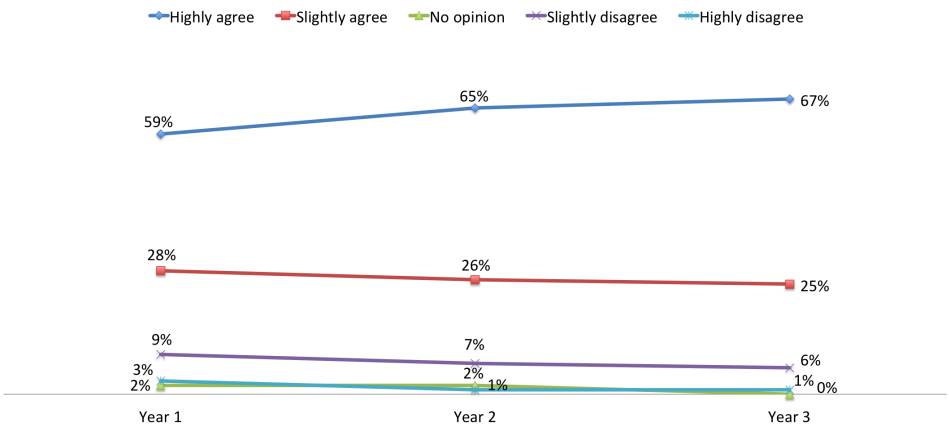


Figure 4.24: Comparing statement 18, *I always lock my computer when I leave it.*

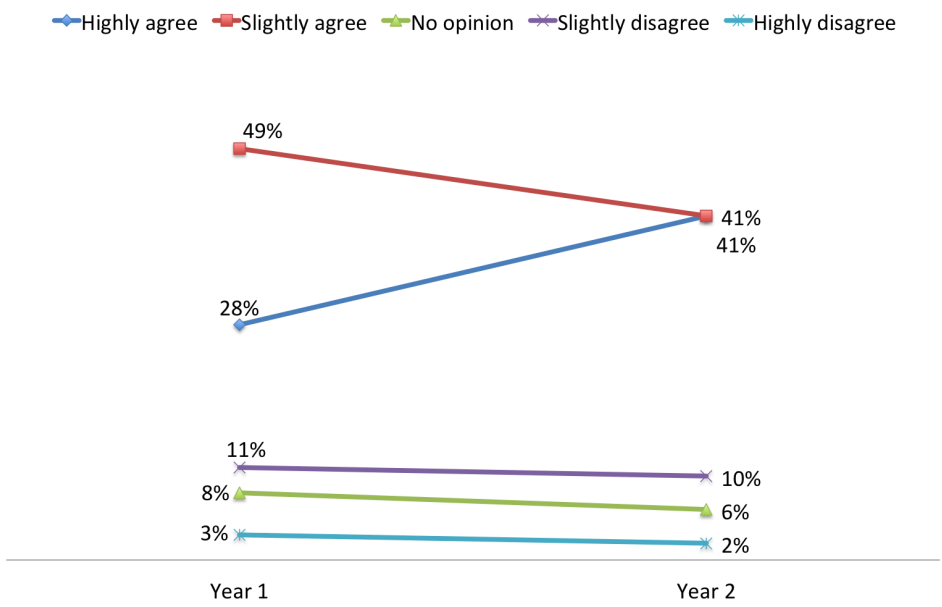


Figure 4.25: Comparing statement 19, *I utilise several methods to verify the contents of an e-mail before opening attachments.*

contents of their e-mails. However, as Figure 4.25 shows, there is barely any change in employees disagreeing.

Statement 20 For this statement, a positive development would be an increase in disagreement, and a decrease in agreement, as memory sticks are something the company is trying to highly avoid. And indeed, there are both significantly fewer employees agreeing, and significantly more disagreeing over the years of the campaign. Actually, the change between all years is significant, both for the agreeing and the disagreeing side. Figure 4.26 visualises the development from Year 1 to 3.

Statement 21 Looking at Figure 4.27, it can be observed that there is only a slight development in the number of employees agreeing and disagreeing with feeling uncomfortable when asking for ID. There is only a slightly higher percentage disagreeing, and a slightly lower percentage agreeing to the statement.

Statement 22 The fifth action related statement to be considered, concerns the use of cloud-based solutions for simultaneous cooperation. Neither for this statement are there any big changes, but in total there is a bigger increase on the disagreeing side than there is a decrease on the agreeing side, see Figure 4.28.

Statement 23 As Figure 4.29 shows, a slight increase in the number of employees

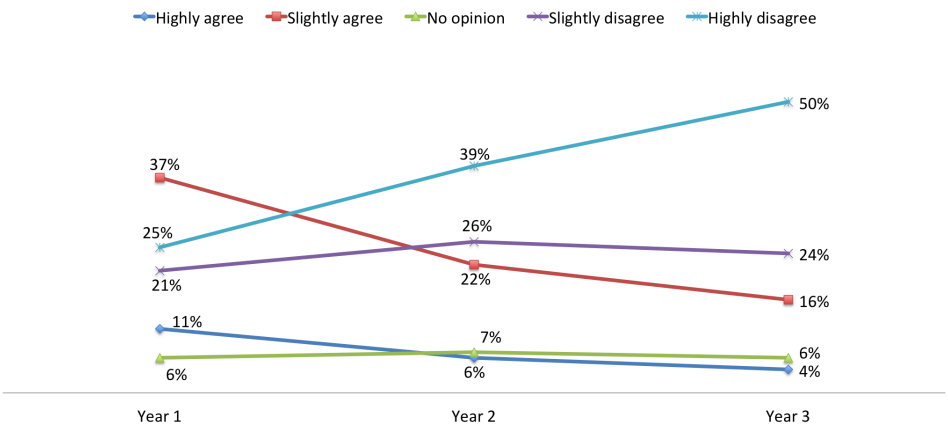


Figure 4.26: Comparing statement 20, *I always use a USB memory stick to exchange files, also when dealing with computers that don't belong to my company.*

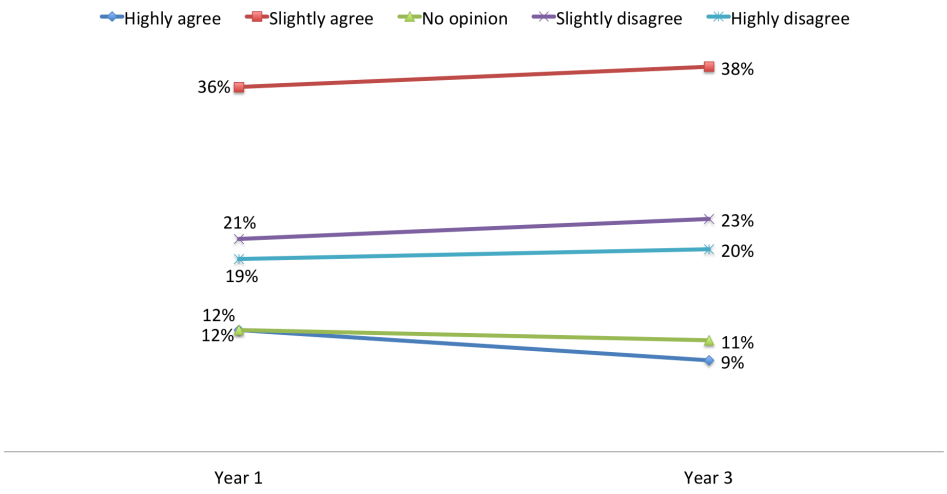


Figure 4.27: Comparing statement 21, *I feel uncomfortable asking people I don't recognise for ID, if they are not wearing any.*

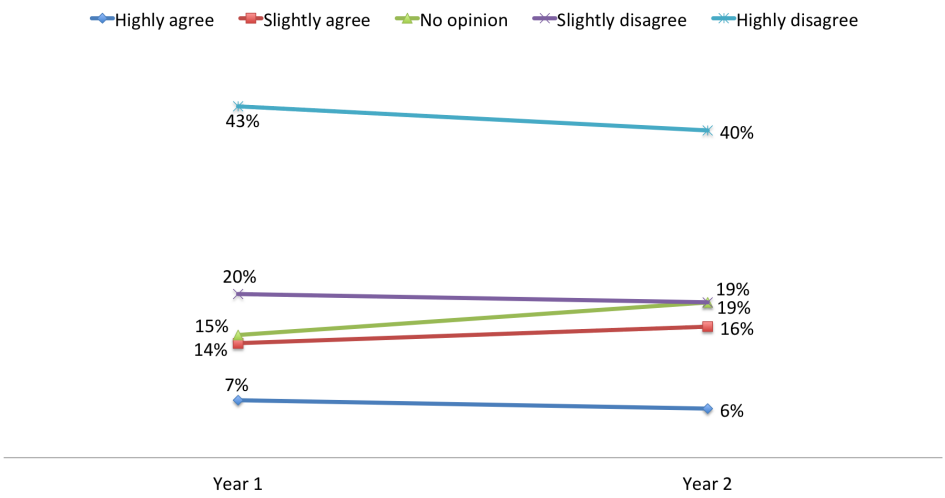


Figure 4.28: Comparing Statement 22, *I prefer Google Docs, Dropbox or other cloud based solutions to work on documents simultaneously.*

answering *No* to sometimes breaking the rules intentionally can be observed, but also a minimal increase in *Yes*. In addition to this, there are also fewer people in Year 3 answering *Not after the campaign*.

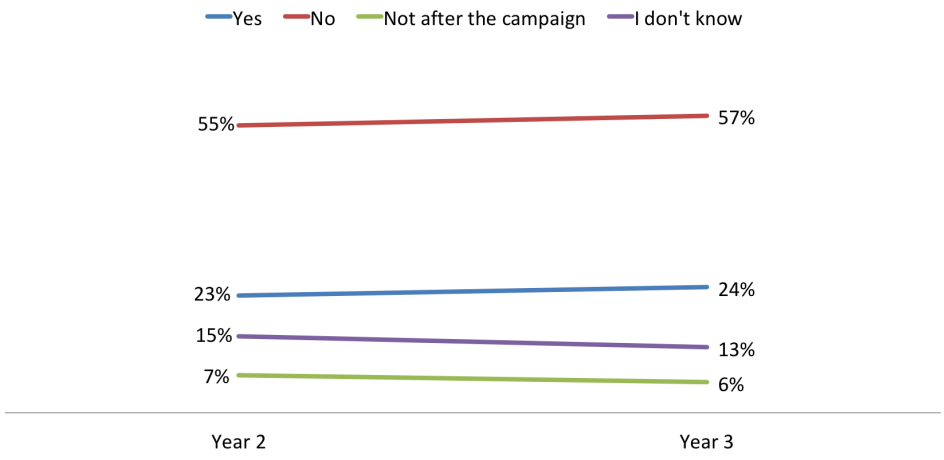


Figure 4.29: Comparing Statement 23, *I sometimes intentionally break rules for information security.*

4.3 The Interviews

From the analysis of the interviews, four main themes were drawn out; *Information Security and Organisation Policies*, *Organisation and Management*, *IT Systems in the Organisation*, and lastly *The Campaign*. These themes are presented in the following subsections.

4.3.1 Information Security and Organisation Policies

The importance of information security The first notable fact is how all the employees expressed information security in the organisation as highly important. Though a couple of them explained that their specific work is not directly interesting to outsiders and is mostly open to the web, the general impression is still that they believe that everyone in the company should consider information security as important. For example, one explained that it is important that there is a consistent level of knowledge about information security throughout the company in order to facilitate cooperation and flexibility within the company.

The gap between security and practicality All interview candidates except one mentioned the difference in theory and practice in some way, and explained the gap with impracticality. All of the five agreed that practical regards almost always surpass security regards, and that a user-friendly balance should be established. Four of them also mentioned some reasons to be the lack of understanding of the subject, not understanding the necessity of certain rules, or naïvety. In relation to this and the latter outing, one employee explained that it is a problem for him/her that people have different ways of acting.

Familiarity with organisation policies When asked about their knowledge of the organisation's information security policies, the response was, evidently, consistently of a hesitant character. Three of them initially claimed that they know them very well, but after some follow-up questions they admitted their uncertainty. The same three explained that they follow the campaign and that they believe that the campaign is based on the policies. Though hesitant when asked specifically about the information security policies, all the interview objects mentioned several security-related actions that they include in their working day. They were not given a list of suggestions, they only mentioned actions that came to mind at the time of the question, most likely leading to fewer answers than had they been provided with a list. Anyhow, one action was common between all, and that was the procedure of checking e-mail; sender address, links, and attachments. As mentioned, more actions would probably overlap if the interviewees had more time and help, but the fact that all mentioned e-mail on top of their head might indicate that this has been most advertised in/by the company.

In addition to some of the information security-related procedures the interviewees do during their day, all of them talked about the use of common sense, or expressed that they perceive their co-workers to be generally precarious, and to have a good sense of what to do and what not to do.

4.3.2 Organisation and Management

The importance of management and routines All of the interviewees somehow expressed the importance of management with regards to information security in the company without being directly asked for it. As mentioned in the foregoing subchapter, some of the employees mentioned lack of understanding of the topic, and naïvety as reasons for the gap between practice and theory, and it is evident that the interviewed employees believe that it is important that counter measurements for this come from management. Everyone considered, to different degrees, their boss to regard information security as important, and to speak positively about information security and its importance. However, there were divided opinions about what kind of pressure or expectations they feel from their boss. One half explained that information security is not a topic that is much discussed, and they do not feel a pressure, but they do think their boss has certain expectations regarding secure practice. The other half expressed that they feel specific, clear expectations from their boss. Especially with regards to information security, all of the interview objects, in some way, expressed that they would like stricter routines.

Four out of six believed that the reason why information security is not as strict as they wished, is that employees, management or not, are not fully aware of the possible consequences, they have not themselves been subject to any critical situations.

Lack of communication and reorganisation All six interview candidates expressed that information security is not something that is often talked about. A couple of them explained that it is talked about to some extent during the specific campaign rounds, but not other than that. Four of them agreed that information security is an issue that should be talked about more, and mentioned that it should be on the agenda for department meetings or similar, and that more info from management leads to a more similar practice throughout the company. The last two did not express any strong opinions on the matter, but one of them admitted that management's focus on the topic has dispersed, and indicated that the reason might be a reorganisation that has been done within the company. Though not directly linked to this specific matter, one other employee also mentioned the word *reorganisation*, as well as "frequent pace of change", as reasons for reluctance with regards to information security.

4.3.3 IT Systems in the Organisation

Frequent change of technology When talking about the IT systems in the organisation, all interviewees mainly talked about the company's web-based collaborative platform. They all agreed that there is/has been a lot of changes over the years, and that transitions to new tools have been, and are, troublesome. Similar as for reorganisation with people and departments, frequent changes in systems and tools was also suggested to be a reason for restraint employees. Two suggested that employees that have gone through several changes might have bad experiences with new tools and that they, therefore, are reluctant. They also mentioned that learning new tools is time-consuming and difficult, and that people choose the easy way in order to finish their work on schedule. One interviewee answered the following when asked about the transition from an old to the new platform:

"And I'm... well, I'm still relatively young, and I don't find these things so scary, and I don't have as many bad experiences as it seems like many others do. A lot of other employees have tried to learn new systems, found that it didn't work out too well, and now they don't bother learning any more new systems."

In relation to the desire of stricter routines mentioned earlier, the same employee that outed the latter quote said this when asked about why he/she thinks that some employees linger on the old systems:

"(...) you have a job that has to be done, and it takes time to familiarise oneself with a new tool. If you are using something that already works, it's time-consuming to transition to something new. If the company wants us to completely transition to a new system, maybe there should be a bigger degree of coercion involved. People are used to controlling their own time and do what works best for them."

Nevertheless, three out of six said that the current system works well and that it offers good security facilities, e.g. to regulate and control access to files and folders. One of the remaining three admitted that the platform is rather good but that there exist many holes, and that it currently does not work optimally because employees do not yet know how to use them "correctly". Another expressed clearly that he/she does not believe that the new platform works well, and favoured the older version. The last of the remaining three not in apparent praise did not express any definite opinion.

The gap between security and practicality Many of the matters and problems that were discussed during the conversations with the employees overlap, hence, issues/reasons/words within the four outlined themes also overlap at times. Also when elaborating on the organisation's IT systems, or the platform, the gap between theory and practice emerged. Five of six communicated this in some way, and four

said that people prefer the easy way rather than the secure way. They said that for things to work optimally, it

"(...) should be more practically accommodated for", and that

"(...) a balancing act between security and user-friendliness should be established".

4.3.4 The Campaign

Method of the Awareness Campaign Every interview candidate was very familiar with the campaign implemented in the company over the last years, and everyone had completed or partly completed the e-learning sessions on the organisation's intranet. They were unanimous in their opinion about the implementation of security awareness campaigns in general, but their views on the specific campaign differed somewhat. Nonetheless, the attitude towards it was positive everything considered. Perhaps the most noticeable positive factor that all of them mentioned, was the use of humour in the e-learning videos. This seems to appeal to all except one, who despite not being too fascinated him-/herself, admitted that it may appeal to others. Another factor that seems to raise interest in the videos, and the campaign as a whole, is the creation of something that the employees feel ownership to. Four of the candidates mentioned the use of internal personnel in the videos, the name of the campaign itself, and the fact that the campaign has its own logo. Moreover, four of them expressed that the fact that the videos use familiar situations to teach about information security, is appealing. One of the interviewees said the following about the implemented campaign and the e-learning:

"I think my co-workers liked it. It's done with a little bit of humour, with the company's own personnel, and they show situations you recognise. So, I actually think it's genius. I really do."

Regarding the competition aspect and cake reward of the campaign, this only seemed to appeal to three of six interviewees. Some found this fun and motivating, while others did not see the point in "(...) having to be tempted with cake".

Incentives for completing the e-learning, and its perceived influence When asked whether they felt the e-learning was obligatory, all of them answered yes. However, it seems like the pressure that the interviewees experienced from their boss has been somewhat different. One half expressed that they were constantly reminded through e-mail to complete the e-learning, and the other half emphasised that they felt obliged to complete them on a more personal level. Following are two quotations, one from the first half, and one from the second half respectively:

"Why I completed the e-learning? Well, there are expectations for you to complete it. And in our department, not completing it wasn't an option."

"Because there might be some useful information to pick up. And also because it is a little silly to not do it. I would feel like I was cheating if I started the video and let it play while I left the room, even though the opportunity is there."

Nevertheless, none of them communicated the obligatoriness as something negative. Rather, four of the six conveyed that they want stricter requirements, whereof two wondered why the completion rate of the e-learning is not 100%.

Only one interview candidate said that the campaign had taught him several new things, the rest were rather unified in that most of the material was already known, but that the campaign still served as a good reminder. One expressed that things you originally know tend to be forgotten in a busy everyday-life, and that the videos are good as a repetition of those things. Also, five of six agreed that the campaigns make them more aware.

How they would have done the campaign differently One of the questions in the interview guide asked the candidates how they would have done the campaign differently, or what they liked less about the campaign. It should be mentioned that the employees seemingly referred to the e-learning, specifically, when talking about the campaign. Five of six expressed that it should be implemented more evenly throughout the year, or that small tests or checkpoints should be implemented in conjunction with the videos. This way, one check what one has learned. One said that as of now, too little work is being done regarding information security training between campaign rounds, and wished for methods to work with the material between and after video releases. Three also mentioned that practical assignments and personal appearance or personal follow-ups would be optimal.

Chapter 5
Discussion

The following section is a discussion of the results obtained in the previous part. The Discussion will be presented in the same fashion as Results, covering the research questions and associated hypotheses one by one. Although the interviews, also here, are presented separately, material from these may be used in the other subsections to substantiate indications made. *RQ3* is presented lastly in this chapter, after the interviews.

5.1 The influence of age, gender, and management position

The answer alternatives to some of the statements explored range from *Highly agree* to *Highly disagree*, but as in Results, this will sometimes be referred to only as *agreeing* or *disagreeing*, which constitutes *Highly agree* together with *Slightly agree*, and *Highly disagree* together with *Slightly disagree* respectively.

5.1.1 H1: Women are more positive towards security training than men

The first interesting thing to regard, before looking at any of the statements, is the relative amount of women versus men that participated in the surveys. Remembering that the majority of the employees in the company are men, it is not strange that the majority of participants in the surveys are men. What is interesting, however, is how many men and women of the total men and women in the company that participated. In Year 2, 64% of the participants were men, resulting in 39% of all the men in the company this year. The women posed 36% of the participants, 40% of all female employees employed that year. In Year 3, the partition of men and women was 62% to 38%, which constitutes 34% of all the men, and 39% of all women, respectively. The mean total participation is visualised in Figure 5.1

The differences in total participation between the genders are not significant, but both years slightly more women (of the total) than men (of the total) participated

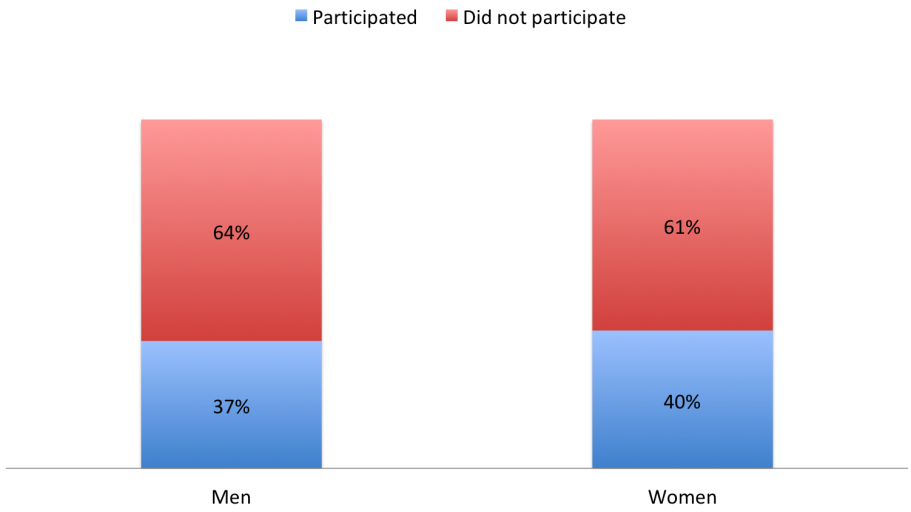


Figure 5.1: This is a visualisation of the mean total distribution of male and female participation in the surveys of Year 2 and 3.

in the surveys. Although that fact does not teach us anything directly about the respondents' information security attitudes, the simple fact that relatively more women than men answered the survey may be a first indicator that women are more engaged in the campaign than men, which again may imply that they are more positive towards security training. On the other hand, social research on genders shows that women score higher on the personality trait *Agreeableness* [YJW11], which is a trait that is described by, among other concepts, cooperation and conformity [WGG97]. When considering this, the fact that a bigger part of the women participated compared to the men, might be substantiated in that women to a higher degree feel conformed to participate, and want to maintain harmony in the organisation by cooperating.

In order to further explore the sub research question at hand, results from five statements/questions given in the surveys were gathered. The first statement asks the employees who they learn the most about information security from. It can be argued that people who claim to learn more on their own are less positive to training than the ones who learn most from the campaign. It may imply that they do not feel the need for awareness campaigns and training, and therefore are not that positive towards it. Looking at the average numbers from Statement 1, one can see that a majority of the men claimed to learn more from themselves than from the campaign, and that the majority of women claimed to learn more from the campaign than by themselves. In addition to this, there are significant differences between the genders within both alternatives, even when calculating the mean; significantly more

women than men claimed to learn more from the campaign, and significantly more men than women claimed to learn more by themselves. As mentioned, saying that one learns most from the campaign may be an indication of positivity towards the campaign and, hence, positivity towards security training in general. However, it may also be the result of men, in general, having more self-efficacy than women [Jr.97]. Then again, self-efficacy for learning and development is shown to be closely tied with attitudes, intentions, and voluntary participation in training and development activities [J.M01]. This is curious, as in this case relatively more women than men participated in these voluntary surveys.

The results show that, on average, a significantly bigger group of women had completed the e-learning sessions compared to men. It can also be seen that significantly more men than women claim to not remember. The fact that the percentage of men answering that they cannot remember is so much higher than that of women may indicate that more men than women adopt an uninterested attitude towards the campaign. Combined, the numbers seem to indicate that more women than men are positive to the campaign and, hence, possibly security training. Again, it may also be due to women, in general, feeling more obliged to complete the campaign than men.

Statement 3 and 4 were interesting to look at as sufficient knowledge may indicate not wanting to learn more and vice versa. Also, employees wanting to learn more could imply employees that are more positive towards the campaign and security training. On average, more men than women agreed to have sufficient knowledge for their work situation. The difference on agreeing, in general, is not significant, but the difference on highly agreeing is, and the biggest response group highly agreeing is the men. The other alternatives to this statement do not show any other big differences. As assumed, Statement 3 and 4 seem to be closely related, as the average also shows that the group of men is significantly smaller than the group of women in agreeing to want to learn more about information security. In other words, more men than women agreed to have sufficient knowledge, and more men than women disagreed with wanting to learn more. No other significant differences in Statement 4 are seen on average. Although not significant, it is interesting to see that the group of men was the biggest to have no opinion on both statements. Not having an opinion may indicate an uninterested attitude towards the topic, as discussed earlier. All this combined could indicate that more women than men are positive towards information security, at least to this specific campaign. When thinking of reasons for why more men than women feel like their knowledge about the topic is sufficient, it is interesting to look at the two gender's interest in it. One statement from the survey states *I'm interested in technology/IT* and will have to suffice as a topic that is closely enough related to information security. As Figure 5.2 shows, the group of men agreeing to be interested in IT/technology is significantly bigger than the group

of women, and the group of women disagreeing is significantly smaller than that of men. As it looks, interest may be the reason, or part of the reason, why more men than women feel like they already know enough about the topic. According to NorSIS [Nor17], interest induces awareness and knowledge, and they assume that interest is one of the keys to information security culture. However, it is interesting that, in this case, consistently more men do not want to learn more about information security, but at the same time more men state to be interested in technology/IT. It would be reasonable to believe that being interested in something results in a desire to learn more about this. In addition to the supposed interest, self-efficacy may also play a role in the results of these two statements, perhaps especially Statement 3; *My knowledge about information security is sufficient for my working situation.*

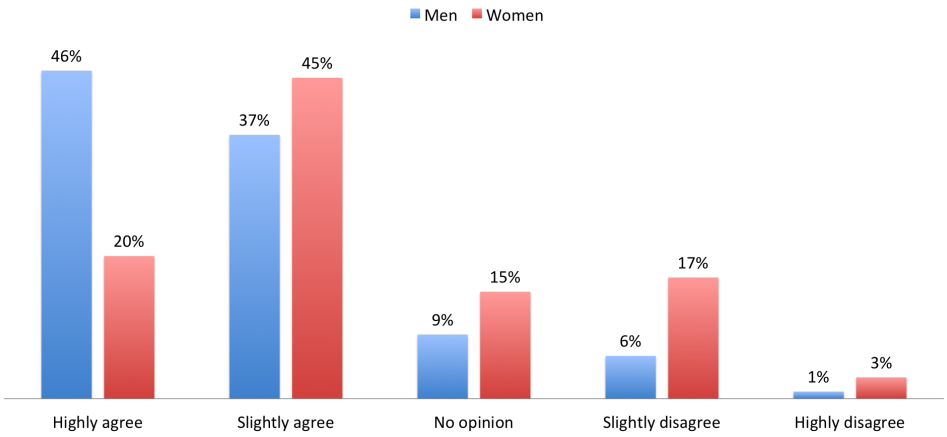


Figure 5.2: This is a visualisation of to which degree men and women agree to be interested in technology/IT, explored in conjunction with Statement 3, *My knowledge about the topic is sufficient for my work situation.*

When investigating the two response groups' biggest motivations to learn more about information security, no major differences are seen. The one alternative that does show a significant difference is the alternative with the least answers in total, so few answers that one may wonder what the practical difference actually is. Significant differences aside, there are no striking differences between the two response groups indicating that one response group is more motivated by some factors than the other group.

Combining the results from the five statements analysed and the total amount of women versus men participating in the surveys, it can look like the campaign appealed to more women than men. Whether this implies that the women are more positive towards information security training than men, or if it shows that women to a bigger extent want to comply and cooperate, and that men to a bigger extent

have more self-efficacy, is hard to say. Nevertheless, the differences that can be seen are interesting, and is substantiated by research represented by CULTRe [KR17]. They found that gender indeed plays a role in information security, and suggest that gender balance in the workplace reduces risk and improves security culture. To support findings from the surveys further, CULTRe also found that women are more prone to comply with norms, which was insinuated in this research through the fact that more women than men claimed to have completed the e-learning, and more women than men participated in the surveys. According to CULTRe, men report a higher knowledge of security requirements and practices, which is also true for the findings of this research. In the report from CULTRe, men also reported a lower compliance with the security policies than women. However, this is not necessarily true for this case. A brief check of some relevant statements showed that, in fact, more men than women, in general, report a higher degree of compliance. The policies that the employees were asked in the surveys are mostly technical, however, so one reason for the contradictory finding could be that men have more knowledge about information security combined with the fact that they are more interested in the topic.

5.1.2 H2: Age plays a role in the positivism towards security training

As when analysing differences between genders, it is interesting to see who the different age groups learn the most about information security from, because this might be an indicator of positivity towards the campaign and information security training. As could be seen in Results and Figure 4.7, the mean numbers give a direct positive correlation between *age* and *I learn most from the campaign*, and almost a direct negative correlation between *age* and *I learn most by myself*. This may indicate that the ability/wish to learn from yourself decreases with age, while the wish to learn from the campaign increases. Also interesting, is the fact that older employees seem to learn more from their co-workers compared to the younger. Morris and Venkatesh [MGM06] suggest that younger people are more independent in their judgment of different aspects of technology than the older are. This may e.g. be due to the fact that younger people have been exposed to different kinds of technology at an earlier stage in life compared to older people. Another reason for this can be that older people perceive less comfort, efficacy and control over computers than younger do [J.M01]. Anyhow, if information security is considered as an aspect of technology, this fits well with the insinuation made above, and one can say that the young employees to a bigger extent trust upon themselves to learn about the topic at hand. The mentioned article also suggests that older people rely more on the opinions of co-workers and friends which, transferred to this setting, may imply that older employees trust more upon co-workers, friends, and maybe the organisation (the campaign) than themselves to learn about the topic. This suggestion goes well with

the findings from the surveys when considering the alternatives *I learn most from myself* and *I learn most from the campaign*. It only fits somewhat with the other alternatives, because *co-workers* and *family and friends* are given as two different alternatives in the surveys, and their numbers are very different (see Figure 4.7 for reference). While the oldest age group is the biggest in saying that they learn most from their co-workers, it is the smallest in saying that they learn most from friends and family. Also, there is no direct positive correlation between *age* and *I learn most from co-workers*, the only thing that can be clearly stated is that significantly more of the oldest employees chose this alternative compared to the other age groups. Though there is not a direct correlation between the age-co-workers and age-family/friends relationships, it is interesting to see the fairly consequent differences. If the age intervals are split into two (under 35-44, and 45-) rather than four, one can say that there are direct correlations; a positive in the age-co-workers relationship, and a negative in the age-family/friends relationship. This is interesting, because it partly contradicts the suggestion made by Morris & Venkatesh [MGM06], where co-workers and friends are referred to as the same thing. However, based on research by Porter [Por63], it makes more sense to keep friends and co-workers separate, as he found that employees' need for security and affiliation in the workplace increased with age, and friends are not necessarily included in the workplace. A combination of research from [MGM06] and [Por63] could be one reason for the numbers seen. Older employees learn most from the campaign and from their co-workers due to a lower degree of independent judgment of technology and low perceived efficacy. They learn more from their co-workers and less from friends/family than the younger employees as affiliation gets more important by age, and one therefore talks and learns more among one another at work about important and relevant issues.

According to the surveys, the youngest age group is the smallest on average in stating that they had completed the e-learning, and the biggest in admitting that they had not. This is not very surprising having just discussed that they say that they learn most from themselves. The mean distribution shows a direct positive correlation between the relationship *age* and *I have completed the e-learning*, a direct negative correlation between *age* and *I can't remember*, and almost a direct negative correlation in the relationship *age* and *I have not completed the e-learning*. Of these mean differences, there is only one significant difference, as stated in Result: the youngest response group (RG1) is significantly smaller than the two oldest (RG3 and RG4) to say that they had completed the e-learning. The other differences may be random variations in the answers, but when numbers over two years show such clear differences, they are still interesting to consider. Anyhow, the general, statistical trend over the two years shows that fewer younger employees have completed the e-learning videos compared to their older co-workers. As mentioned, it is not surprising when comparing it to whom the different age groups learn the most from. It is surprising, however, looking at research by Cleveland and Shore [JNC92], who note

that older employees, due to lack of self-confidence in development, tend to not participate as much as younger employees in training and development activities. As the age distribution in the company is unknown, it cannot be shown how many employees in the different age groups participated in the survey of the total number of employees in the age groups. However, considering only the ones participating in the surveys, there are almost as many old employees participating as young, if one again split the age intervals into two (under 35-44, and 45-). This as well contradicts the statement from [JNC92].

When asked if the employees believe that they have sufficient knowledge about information security for their working situation, all age groups are on the agreeing side both years. However, the mean shows no direct correlation in any of the alternatives. Had there been a direct negative correlation between e.g. age and agreeing to have sufficient knowledge, the theory of age-efficacy in [J.M01] could be utilised as a reason, but there is not. The fact that no patterns exist makes it difficult to conclude if some age groups, in general, believe that they have more sufficient knowledge than other groups. This, again, makes it hard to conclude whether some age groups are more positive towards information security and information security training than others.

In conjunction with the statement discussed in the latter paragraph, the statement *I want to learn more about information security* was also investigated. The mean of the results is shown in Figure 4.10 in Results, and as stated there, the youngest response groups (RG1 and RG2) are the smallest in agreeing and the biggest in disagreeing. This is somewhat surprising having in mind that the groups of the youngest employees were the smallest in agreeing to have sufficient knowledge about information security. The mean differences are marginal, but one would believe that the desire to learn more would be bigger if one did not feel like one's knowledge was sufficient for one's work tasks. What is also interesting, is that the oldest response group (RG4) is the biggest in agreeing to want to learn more. It is known that as one age, speed and amplitude of perception reduces, which makes it harder to process new, and perhaps especially, complex information. Rhodes suggests that this ageing effect may be a factor that can affect work attitudes and behaviour [Rho83]. This is an interesting contradiction to the results from the statement examined. Mentioned results also differ from the theory that older people have less confidence in their ability to learn and develop [JNC92]. The company in this specific case is a highly regarded and modern research organisation, employed with researchers and other people whose work is to discover new things, and many of them work with (new) technology every day. This might be the reason why the findings from the surveys contradict with research from both Rhodes [Rho83], and Cleveland & Shore [JNC92]. However, the studies do not inform about the type of company utilised for the research. Other than this, there are no patterns that stand out either of the

years of the surveys, making it difficult to conclude if age, in this specific case, is directly related to the wish for learning more about information security.

What is interesting to regard when considering the element of age, is whether the differences seen are due to physical age, or due to the difference in generations. Prensky [Pre01] describes people born roughly between 1980 and 1994 ([SB08]) as Digital Natives, suggesting that people within the two youngest age groups examined (RG1 and RG2) fall into this description. Digital Natives are people who grew up with the new, digital technology, and Prensky indicates that this makes them "(...) think and process information fundamentally differently from their predecessors." It would not be surprising if at least some of the differences discussed in this subchapter can be explained by the generation shift, and it would, therefore, be important to take both age and generation into consideration when constructing an awareness program or campaign. If indeed the differences are caused by generation characteristics, one would also expect the statistics to look different as the older generations in the company are replaced by younger ones.

Biggest motivations

Some interesting findings are revealed from looking at what the biggest motivations are for the different age groups. As can be seen in Figure 4.11, only one age-reason relationship correlates directly, but there are other noteworthy differences.

In choosing *Because my boss tells me to* as a reason for learning about information security, the oldest response group (RG4) is the smallest. In one way this is curious because of what is discussed earlier about affiliation [Por63]. Also, Morris and Venkatesh [MGM06] argue that older workers tend to emphasise subjective norms more than younger workers. Younger workers, however, were more influenced by the attitude toward using the technology. The research concluded, though, that the influence of subjective norms diminished over time. Hence, the numbers seen can be explained by new, young employees wanting to comply and show interest, while the older workers have other motivations than their boss after some time. For example, in choosing the alternative *Because of attention around the campaign* the oldest response group (RG4) is the biggest. This can be linked to the theory that older people trust more in the organisation to learn about information security.

Another interesting difference is that the youngest employees are in a clear majority in having media as motivation. This can be linked to the attitude towards using the technology as discussed earlier [MGM06]. It is not the subjective norms that make younger people learn about information security, rather it is their own interest. This is reflected in the alternative *Because I might utilise it in private life*, where the youngest response group (RG1) is the biggest.

The last, and perhaps the most interesting difference is the direct negative correlation in the relationship *Age* and *Because of the cake competition.* These results are well substantiated by research from [MGM06] suggesting that younger workers are more focused on extrinsic rewards than older workers.

5.1.3 H3: Employees with higher management responsibilities feel more responsible with regard to information security than those with lower management responsibilities

As indicated by CULTRe [KR17] and described in 2.3, security culture is one of the most important aspects of organisational security, and as stated by Chang and Lin [Hre74], organisation culture is the media between management and organisational behaviour. Hence, management is the starting point for developing and maintaining good security culture in an organisation, and top positions should show a positive attitude towards information security in order for this attitude to spread to lower positions. Although this project does not concern the top management of the organisation at hand per se, it is still interesting to explore whether there are differences in attitude, knowledge, and behaviour between different groups of people with different management responsibilities. See Table 4.2 in 4.1.3 for explanation of the different management responsibilities. The three first statements from Table 4.3 will be discussed first, then the statements from 4.4, and lastly the last statement from Table 4.3 will be presented.

The first statement considered in Results assesses to which degree the different response groups feel responsible for contributing to maintain a high level of information security in the company. The results show that the majority of all four response groups agreed all three years, even highly agreed. However, it is evident that relatively more employees with a higher degree of management responsibility highly agree to feel responsible, compared to employees with lower or no degree of management responsibility. There is actually a direct positive correlation between responsibility level and a strong feeling of information security responsibility all three years. Although not many, there are some employees in the groups RG1-RG3 that even disagree with the statement every year, or have no opinion on the matter. The group with the highest level of responsibilities (RG4) have a continuous 0% on the disagreeing side as well as in having no opinion. Optimally, all employees should feel just as responsible, regardless of their positions, but taking into consideration that higher positions are the starting point, the numbers might not be so surprising. Unless the company has a well established and incorporated security culture, it is not evident that e.g. attitudes towards the topic yet have moved down to all levels of responsibility in the hierarchy of the organisation. Even with a well integrated security culture, perhaps the employees with higher levels of management respon-

sibilities always will feel the responsibility more than those with less management responsibility.

It is interesting to see to which extent the different groups feel targeted from actors outside of the company, because it can be argued that this feeling is closely related to the general feeling of responsibility for information security. If one does not think of oneself as a possible target, this may indicate that you do not feel responsible for maintaining information security, and vice versa. As for the previous statement, the majority of all response groups is on the agreeing side, but also here there is a noticeable difference between the response groups. Taking into consideration the argument that this and the former statement are closely related, the direct positive correlation, when calculating the mean (see Figure 4.13), in the relationship *Level of responsibility* and *I highly agree to the possibility that I might be a target*, is not so surprising. Also, there is a direct negative correlation of the mean between *Level of responsibility* and disagreeing with the statement, and *Level of responsibility* and *I have no opinion*. As discussed earlier, having no opinion may indicate an uninterested and, hence, irresponsible attitude towards the topic. Not only is there a positive direct correlation between *Level of responsibility* and *Highly agreeing*, but the majority of RG4 highly agreed on average, while the majority of the other groups only slightly agreed on average.

How familiar the employees claim to be with the information security policies of the company might give some indications of how responsible they feel. If one feel highly responsible for maintaining a high level of information security, one should be familiar with the company policies. The mean (see Figure 4.13) does not show a direct positive correlation between *Responsibility level* and *Highly agreeing to be familiar with the policies*. Actually, the group of employees with no management responsibilities (RG1) is bigger than RG2. However, if the agreeing side is counted as one (adding *Highly* and *Slightly agree*), there is a direct positive correlation. Nonetheless, it is evident that the group of employees with the highest degree of management responsibility (RG4) is significantly bigger than the rest to highly agree. Actually, the majority of this group highly agreed on average, while the majority of the other groups only slightly agreed. This group [RG4] is also on average the smallest group to have no opinion, or to disagree. All these observations fit well with earlier ones.

The exploration of the three latter statements strongly indicates that a higher level of management responsibility indeed induces a stronger feeling of responsibility towards information security in the company. Not all statements show direct correlations between *Level of responsibility* and *Agreeing* or *Disagreeing*, but what is indisputable is that the group of employees with the highest level of responsibility (RG4) on average is the biggest to agree, even highly agree, to the statements, the

smallest to disagree, and also the smallest to have no opinion.

5.1.4 H4: Employees with higher management responsibilities act more securely with regard to information security than those with lower management responsibilities

Until now, the explored statements consider only theory, meaning that they reveal only what employees think or know, nothing about how they actually behave. According to Kajava, Varonen, Anttila, Savola & Röning [JK06], top managers only have a superficial understanding of information security, which might lead one to believe that they do not necessarily act as securely as they feel responsible for the security. Although Kajava *et al.* say top managers in their article, this project transfers this to mean higher management responsibilities in general.

The first action related statement asked the employees to which degree they agreed to lock their computer when leaving it. As figure 4.16 shows, RG4 is on average the biggest group to highly agree, and the smallest to disagree or have no opinion. So far, behaviour corresponds well with feeling of responsibility as far as the level of management responsibility is concerned, but this action is straightforward, and no deep understanding or technical requirements are involved. This may also be noted in the fact that the difference between RG4 and the other response groups is not as big on the agreeing side as in the statements explored earlier. Also, RG1 is noticeably bigger than both RG2 and RG3 in agreeing, so there is no longer a direct positive correlation to be seen. Lastly, the majority of all response groups highly agreed to the statement on average. In other words, the differences are not as clear and big as observed earlier.

A more technical requirement involves to which degree the employees agree to utilise several methods to verify the contents of an e-mail, and now a fairly drastic change is observed. On average, the group with the highest level of responsibilities (RG4) is no longer the largest to agree. It is the second largest, counting the same as RG1, and it is actually the smallest to highly agree. Also, RG4 is no longer the smallest group, on average, to disagree. On average, the majority of all groups are on the agreeing side, slightly agreeing. However, the difference in proportions between *Highly* and *Slightly agree* between the response groups tend to get bigger as the responsibility level increases, see Figure 5.3 This change between the groups may be irregular, but it is interesting to see that the change appears at the first technical statement examined, having in mind what Kajava *et al.* suggested about top management and superficial understanding.

Looking at the mean numbers of the statement *I let other people borrow my work computer*, there are barely any differences in any of the alternatives. One

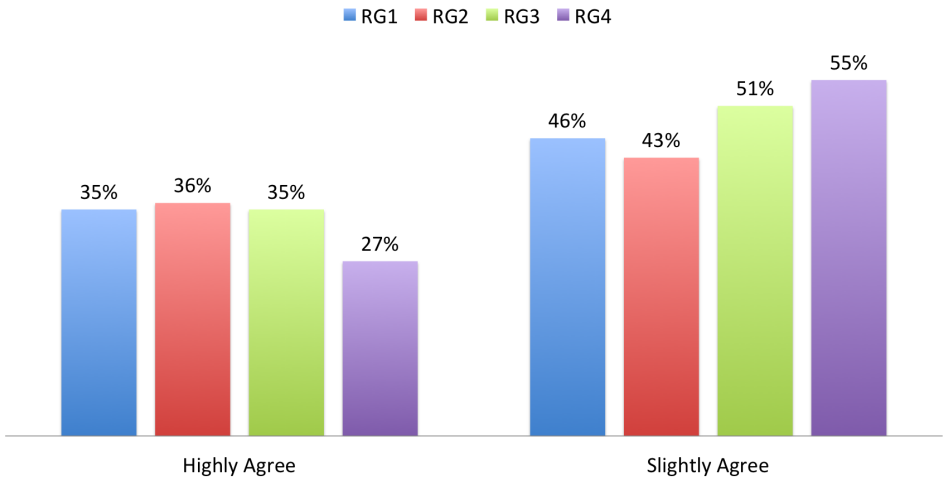


Figure 5.3: This is a visualisation of the difference between how the different responsibility levels answered *Slightly agreeing* and *Highly agreeing* to the statement *I utilise several methods to validate the contents of an e-mail.*

interesting, small difference is that a bigger group of employees with no management responsibilities (RG1) is following the security policies, compared to the two groups with higher responsibility levels (RG2 and RG3). This combined may be an indication that responsibility level is not related to the action/behaviour of letting other people borrow the work computer.

In contrast to the three action-related statements recently explored, the pattern for Statement 12 (use of VPN) looks similar to the patterns observed when exploring *H3* in 4.1.3; a direct positive correlation exists between *Level of responsibility* and agreeing to use VPN when connecting to public WiFi's. This contradicts the theory indicated earlier; that employees with a higher level of management responsibility do not necessarily act as securely as they like to give the impression of. The direct negative correlation between *Level of responsibility* and *I have no opinion* is also interesting, and follows the patterns seen in subchapter 4.1.3.

The four behaviour-related statements recently explored do not really give any strong indications about anything specific, other than that a higher level of management responsibility does not necessarily directly indicate a higher level of secure working habits. Some statements did to some degree agree with tendencies observed when exploring H3 (e.g. the use of VPN), but they were few, and the differences between the response groups were in general smaller. Also, fewer direct correlations were seen.

The last part of this subsection will discuss the last statement from Table 4.3; the four groups' biggest motivations for learning about information security.

Because I can utilise it in private life was chosen by a significantly smaller group of employees with the highest responsibility level compared to the other groups. As indicated in the discussion over, the knowledge about information security may be somewhat superficial for some of the employees with higher responsibility levels, and this is in a way emphasized with this choice of motivation. It may mean that employees within RG4 are not genuinely interested in the topic, they are only interested and motivated on a level adequate for their work situation.

The fact that *Because I can learn something new* is the second biggest motivation in total, gives a general impression of the company that its employees are eager and thirsty for new knowledge. But, as the numbers show, the group with no management responsibilities (RG1) choosing this reason is fairly bigger than the three other groups. Looking at the age distribution in the different response groups, this is somewhat surprising, as the majority of employees in RG1 are 55 years or older. This is surprising because, as mentioned in subsection 5.1.2, Cleveland & Shore [JNC92] suggested that older people have less confidence in their ability to learn and develop. Then again, this suggestion was partly contradicted also in the discussion of the age factor. Another reason worth to discuss with regard to this motivation, is newly employed people. It would be reasonable to assume that newly employed people start at the bottom of the hierarchy (RG1), and have to work their way up to the other levels (RG2, RG3, RG4). With this in mind, one might say that newly employed people are more eager to learn and show engagement, and newly employed people have no management responsibility (RG1), and that is one reason why RG1 choosing this reason is bigger than the other groups.

Because it helps me protect assets that belong to others is the reason that in total has the most votes, which gives the general impression that the company is trustworthy, and takes their clients seriously. One would perhaps wonder why the biggest motivation for learning about information security is protecting other people's assets, and why it is not the fear of being targeted oneself. It is not uncommon to not answer completely truthfully in anonymous surveys, so could it be that the employees answered what they wished was true, or in a way that they imagined would be satisfying to management. An experiment conducted by Grant & Hogmann [AMG11] aimed at motivating health care professionals to maintain a good hand hygiene. The effectiveness of two different signs were evaluated; "Hand hygiene prevents you from catching diseases", and "Hand hygiene prevents patients from catching diseases". The results showed that the sign victimising the patient was the most motivating to the health care professionals. As Grant & Hofmann also state, most people tend to be overconfident about their own immunity. If one transfers the experiment to include

people (working with other people) in general, it is not so surprising that *Because it helps me protect assets that belong to others* is the most chosen reason. Despite the fact that RG3 is bigger than RG4 in this choice of motivation, it looks like this motivation, in general, increases with the level of responsibility, as both RG3 and RG4 are fairly bigger than both RG1 and RG2.

In general, the difference in motivation for learning about information security seems to mostly lay in the difference between genuine interest and motivation, and work-related interest and motivation.

In total, it seems like employees with a higher level of responsibilities do feel more responsible for the information security in the company, but they do not necessarily seem to practice it more than the groups with lower levels of responsibility. The reason for this may be, as proposed earlier, that higher levels on the hierarchy might not have a deep understanding of the topic. A deep understanding does not necessarily have to involve technical understanding, it can also be that one does not really understand the reason for e.g. not lending your work computer to your children. What is curious, is that the group of employees with the highest level of management responsibility (RG4) actually was the biggest in agreeing to use VPN when connecting to a free WiFi, which was one of the two more technical behaviour-related statements. The statement was only given the last year, and considering all other behaviour-related statements examined, it might be that the numbers would look somewhat different if a mean of two years was calculated.

It is important that management emphasises information security and relays it as important, because management is an essential part in resolving security problems ([Par81]; [Bra68]). Dutta & McCrohan also say that "Only senior management can initiate the plans and policies that address the different aspects of security in a balanced and integrated manner". However, it seems like, to a certain extent, the importance of the topic is not relayed properly from management to lower levels of the hierarchy. Indeed, communication between senior management and the workers can be a challenge in big companies [RvS04], and perhaps especially if there are many levels. Especially regarding the feeling of responsibility for information security, this could be a reason for the difference seen between the different management levels in this specific case.

5.2 The security awareness campaign's effect on employees

The following section debates the campaign's effect on both employees' motivations and actions, as described by hypothesis 5 and 6. The two hypotheses are presented in order in the following subsections.

5.2.1 H5: Employees are more positive toward information security/training by the last campaign round than they were in the first

H5 mainly considers the employees' attitudes. Attitude, according to Thomson & von Solms [MET98], constitutes a system of several aspects which determines how a person will behave in a certain scenario. The aspects are behavioural intentions, behaviour, cognition, and affective responses, and combined they have an impact on the attitude of a person. The four aspects and how they are connected to a person's attitude, simplified, is visualised in Figure 5.4. For the first part of this discussion, the part considering *H5*, mainly changes in employees' cognition and behavioural intentions are considered. Changes in behaviour are examined in the second part of this discussion (*H6*).

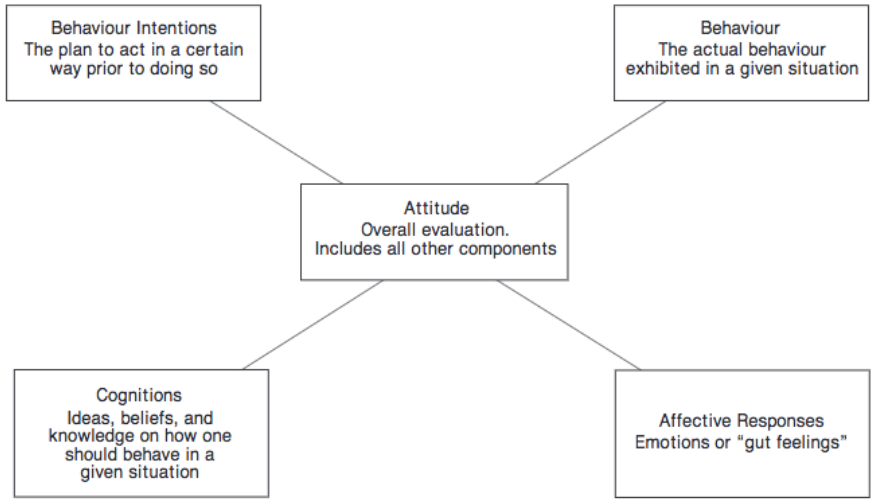


Figure 5.4: An attitude system [MET98].

According to the surveys, there was a significant increase in the completion rate of the e-learning from the first to the last year, and the same is true for the "real" statistics. The completion rate looks higher when looking at the numbers from the surveys, and this is due to the fact that out of the employees that participated in the surveys, the majority had taken the e-learning, it does not represent the total number of completion in the company. The statistics show the real numbers of completion, and they are somewhat lower. As the results show, the increase in completion rate is higher from Year 1 to Year 2, than from Year 2 to Year 3. One reason for the difference in increase between the different years could be that the videos in Year 1 were very much more appealing than in Year 2, or that the employees realised

the importance of information security and got motivated to participate and learn. Another, perhaps more realistic, reason could be that relatively few employees had heard about the campaign the first year, and during that year the campaign gained a lot of recognition so that substantially more people participated the next year. From Year 2 to Year 3, the campaign was already known for most employees, which could be one reason for the smaller increase this year. It can also be seen in the statistics that some departments did not increase their completion rate at all from Year 2 to Year 3. In combination with the growing of the campaign, the employees were highly encouraged from higher levels of the hierarchy to complete the e-learning sessions. All things considered, this statement, most likely, does not say anything about the employees' change in positivity towards the campaign. Neither can the increase in completion rate give any guarantees to changes in employees' cognition, whether they have learned anything from the e-learning. This is because one can, in theory, let the videos run in the background while one does other work-related tasks, and there is no test involved in the e-learning to check the learning effect.

I feel motivated to strive for good information security is a statement that can be related to behavioural intention, as motivation is the desire to do something. Motivation does not necessarily result in the desired action, there are many paths from intention to actual behaviour, and some of them are explained in Section 2. Albrechtsen's qualitative study of employees' experience with information security [Alb07] showed that employees tend to state that they are motivated to work in a secure manner, but that they do not perform many individual security actions. Anyhow, increasing employees' motivation is a good step on the way to change their behaviour, so it is interesting to see if the campaign had any effect on motivation. The results do show a total increase in employees agreeing, and slightly fewer employees disagreed in Year 3 compared to in Year 2. The increase in agreement was significant from both Year 1-Year 2 and Year 2-Year 3, and the decrease in disagreement was significant from Year 1-Year 2. It may be argued that this increase in motivation with the employees may insinuate an increase in positivity towards the campaign or information security in general. In contrast to looking at the e-learning completion rate that might give an incorrect picture of reality, there are no obvious reasons as for why the employees would state that they are motivated if they, in reality, are not, and it may look like the campaign indeed has motivated the employees to a certain extent.

When investigating the fourth statement in Table 4.5 (*Who do you learn the most about information security from?*), it is especially interesting to see what kind of change can be spotted with regards to the alternative *I learn most from the campaign.* If the change is positive, i.e. increase in employees who learn most from the campaign, it could mean that people are more positive towards the campaign, and, hence, information security training in general. The numbers show an increase

of 15% from Year 2 to Year 3 in employees who state that they learn most from the campaign, which makes a significant difference. The percentage of employees stating to learn most by themselves also decreased significantly, with 6%, which may indicate, as mentioned, that people indeed are more positive to the campaign by the last campaign round than they were in the beginning. Recall that more people had completed the e-learning in Year 3 than in Year 2, so more people may have learned something, which may also be a reason for the numbers seen. A third reason could be that the e-learning was better or more interesting the last year compared to the previous.

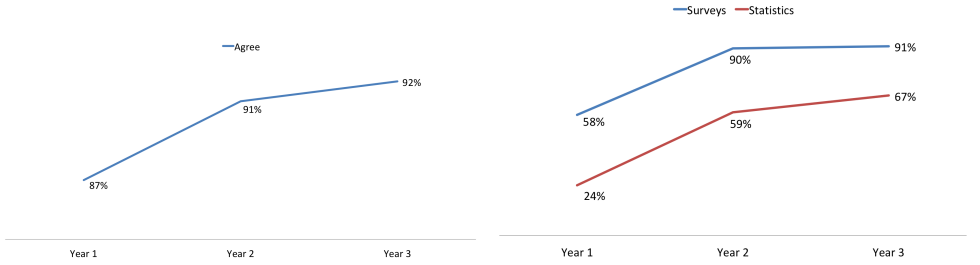
To look for a change in the statement *I want to learn more about information security* is perhaps the most direct manner to spot a change in positivity towards the campaign and information security training in general. The agreeing side increased, in total, from Year 2 to Year 3, but only barely. There was also a minimal decrease on the disagreeing side. However, as argued before, so small changes are most likely only irregularities, and might not reflect a practical change in the motivation to learn more. Should it not be irregularities, but an actual development, the changes are still so small that the effect of the campaign on employees' positivity and motivation has been minimal with regards to wanting to learn more about the topic. However, not wanting to learn more does not necessarily mean that the employees are not positive towards information security. As was revealed in the interviews, many found the security policies hard to follow due to impracticality. Although the surveys give the impression that the employees do not want to learn more, it could be that they are still positive towards acting securely, they just need what they already know to be practically feasible.

As mentioned, changing/developing the behavioural intentions and cognition of employees is one step closer to changing their attitude. With respect to those two factors, the campaign seems to have had some significant impact, the way it has been measured in this project. It has to be taken into consideration that measuring these kinds of factors is hard, and the methods utilised in this project are somewhat coarse.

However, as stated by earlier works (e.g.:[MET98], [JS15], [ABC15]) there are several factors that affect a person's attitude, one of them being changing their behaviour. *H6* relates to this factor, and with respect to that hypothesis, the six behaviour-related statements listed in Table 4.6 were compared over the years to examine if the employees actually changed their behaviour after the campaign. The statements were compared from year to year to see if any significant change could be observed regarding employees' security behaviour. Statements explored include, e.g., the utilisation of several methods to verify the contents of an e-mail, and the use of commercial cloud-based solutions for file sharing and simultaneous cooperation.

5.2.2 H6: Employees act more securely by the last campaign round than they did in the first

The first, and maybe simplest, behaviour explored was the action of locking the computer screen whenever leaving it. As the results show, the agreeing side increased from Year 1-Year 2 and from Year 2-Year 3, but only significantly from Year 1-Year 2. This is an action that requires no technical understanding or skills, and as long as one remembers to do it, it is not a very impractical security action that substantially hinders an employee's normal work tasks. Remembering the pattern of increase in completed e-learning sessions, it seems natural that the increase in employees locking their computer screen is as it is. See Figure 5.5 for comparison of the increase patterns. Also, 90% agreed to lock their computer when leaving it already in Year 2, not leaving room for much more improvement. Optimally, there should be a 100% agreement, especially since this is such an easy security action to comply with, but there will always be some employees that will not comply, and it can, therefore, be argued that 91% (which was the maximum agreement the last year) is a decently high percentage of compliance.



(a) Increase in agreement to the statement *I always lock my computer screen when leaving it*

(b) Increase in completion of e-learning videos

Figure 5.5: Comparison of the increase in agreement to the statement *I always lock my computer screen when leaving it* (5.5a) and increase in completion of e-learning videos (5.5b).

The action of utilizing several methods to verify the contents of an e-mail requires somewhat more technicalities than locking one's computer screen, but it has been part of the campaign, so the employees should know how to do it, or can at least search for the relevant e-learning session to learn it. However, it is a somewhat more cumbersome action than locking the computer screen, judging by the slight smaller agreeing percentage. Nevertheless, the increase on the agreeing side was significant from Year 1 to Year 2, indicating that the campaign had some impact on the employees' behaviour whether it was that they learned something new, or got reminded of something they already knew.

The use of USB memory sticks is something that has been highly prioritised in the company the last years, as they are trying to get completely rid of them. With this in mind, the increase in disagreement is perhaps not a surprise. The increase was significant between all three years, and so was the decrease in agreement to the use of memory sticks. If this is because of the campaign alone, or because of the added attention to this matter specifically, is hard to say. Looking at the remaining behaviour-related comparisons may give a better indication of this.

To ask strangers for ID if they are not wearing any on the work premises is a security action that seems to be socially hard, and many find this uncomfortable. Both years, the agreeing side is higher than the disagreeing side, and the small changes that can be seen in Figure 4.27 are most likely only natural variations. One reason why this is found uncomfortable was mentioned by one of the interview objects to be that one is afraid that one does not recognise people one feels like one should have recognised, and therefore refrains from intervening. Another reason could be that people do not want to seem too sceptical, and in fright of seeming too extreme, they do not say anything. This is not something that can easily be changed overnight, it requires cultural change, and that can take time. The employees should carefully be taught the risks and possible losses of a stranger with bad intentions on the work premises, focus on waryness should be prioritised, and acceptance of alertness should be communicated.

Instead of using commercial cloud-based solutions for collaborating, the employees should use a common company-specific platform for this. Still, around 1/5 claim that they prefer solutions like Google Docs or Dropbox both years. In addition to this, the numbers for having no opinion are also fairly high in both years, which may indicate an uninterested attitude, which again may indicate an uninterested attitude towards information security. From Year 1 to Year 2 there was actually a decrease in employees disagreeing, insinuating that more people preferred Google Docs etc. in Year 2 compared to in Year 1, which is the opposite of the desired change. The change is not significant, however, so it might just be irregularities. One reason for not complying with this rule could be that the employees lack the knowledge for utilising the company platform, and therefore use what they know and are familiar with. Another reason could be that using the commercial solutions is more practical. Although never specifically referring to cloud-based solutions, several of the interviewees mentioned the gap between practicality and security on more than one occasion. Or, rather, the information security aspects of using these services are not clear to them. The vagueness of policies is something that was expressed in the interviews as well, and is discussed further in subsection 5.3.

The last statement examined said *I sometimes intentionally break rules for information security.* This is a statement that helps to give a bigger picture of the

impact of the campaign as it does not concern one policy, rather it concerns all of them. As the results show, none of the alternatives changed significantly. The changes seen are extremely small (1%-2%), which questions the practical difference of the change, and the difference in answers between the years may just be natural variations. Employees might have improved some security actions, but if one knowingly breaks rules for information security to the same extent before and after a campaign, this questions the total impact of the campaign. Reasons for generally breaking rules for information security could be, as mentioned, due to impracticality or lack of knowledge about how to complete the work task in a secure way. Although intentionally breaking the policies is not a good thing, the fact that so many employees answered *Yes* to this, indicates that they, at least, know about the policies they are breaking.

According to Robinson [Rob13], people base their decisions, among other things, on whether the effort will be worth it. This was also the impression after having talked to the interview candidates, where it was mentioned that a task has a deadline, and risking the deadline to learn and find out how to do things another way than how they are usually done, is not worth it. Combining all the statements examined and discussed in subsections 4.2.1 and 5.2.1, it seems like the campaign had some impact on the employees' behaviour; three out of six statements explored showed a significant change for the positive. However, out of these three, one concerns the very simple action of locking the computer screen, and one concerns the much talked about utilisation of memory sticks. Indeed they changed positively, but taking into consideration that they are very elementary and/or especially much focused on, it is difficult to say if it was because of the campaign alone. Also, employees respond that they sometimes intentionally break rules for information security to the same extent in Year 3 as in Year 2.

For the cognition-related statements (the motivation and knowledge related statements), three out of four changed significantly for the positive. Also here one of the statements has to be taken carefully into consideration, because *I have completed the e-learning sessions* does not necessarily mean that one has learned something. Additionally, the employees were highly encouraged to complete the videos, and in some departments it was even made obligatory according to some of the interview candidates, so not all who watched them did it because of personal motivation. Another thing to note, is that the survey participation decreased somewhat every year, in total it decreased by around 18%. This could insinuate a drop in enthusiasm and motivation towards the campaign or information security in general, or it could be because the employees did not have time to prioritise it even if they wanted to. Management's advertisement of the surveys decreased the last year as well, which results in a very possible reason for the drop in participation. The decrease in participation is considered when calculating significant differences between the years, but it is important to have in mind when interpreting the results. There is a

possibility that the fewer employees that did participate were more positive to the campaign originally, and therefore answered in favour of the campaign.

The implemented campaign seemed to have some effect on both the employees' cognition and behaviour, but it is difficult to say exactly how much. In this project, certain statements were chosen to try to measure the change by looking at significant changes. For the measurement of change in cognition and behavioural intention, a quantitative method is perhaps limiting. For the measuring of change in behaviour, one cannot blindly look at the number of statements that showed a significant change, and from that conclude how good the improvement was, or how good the effect of the campaign was. As most of the figures in Results show, the numbers show consistently high agreement and disagreement in the right contexts, indicating a relatively good initial secure practice. Although "only" 3/6 behaviour-related statements showed a significant change for the positive, there *was* an improvement, and seeing as the initial numbers were rather good, perhaps one can say that the behaviour improved from good to better, instead of saying that it did not improve so much. It is interesting that almost all interviewees stated that their behaviour had not changed after the campaign, when the surveys indeed show a change.

Bada & Sasse [DMB14], and Kruger & Kearney [HAK06] state that information security awareness and training programs can be effective if the material is interesting and current. Other factors that can make training effective is, according to Puhakainen & Siponen [PP10], a continuous communication process. The implementation of this specific campaign did involve some continuous attention around the topic (see subsection 3.4 for a description of the case context), and the campaign seems to have gained interest from the employees through the use of relatable scenarios in the e-learning sessions, and through the use of familiar faces in the videos. As explained in subsection 4.3, five of six interviewees expressed that the campaign/e-learning did not teach them anything new. Evidently, six employees are not representative for the whole company, but it is perhaps not so surprising if this were the answer from more employees as well. They have been through the company policies once (in the beginning of their employment), so, in fact, nothing should be completely new to them. The change in motivation and behaviour may be due to the campaign material functioning as a reminder of what they already know rather than a channel for new information, and the interviewees also confirmed this in the interviews. Perhaps an even better improvement in behaviour and motivations could be achieved through a more even distribution of the campaign rounds over the year, which was mentioned by some interviewees as one of the ways they would have changed the campaign if given the opportunity. Like the interview candidates in Albrechtsen's study [Alb07], some of the candidates from this study also expressed the wish for more user involvement or practical engagements.

5.3 Discussion of the Interviews

As described in Results (4), the interviews are meant to give a general view of the information security picture in the company. Although they do not answer any of the specific hypotheses directly, they give some insight into the employees' perception of information security in the company and things that may be related to this. The analyses of the interviews also give a good basis for answering *RQ3*, together with the results and discussion of *RQ1* and *RQ2*. The discussion of the interviews are presented in the same order as in Results.

5.3.1 Information Security and Organisation Policies

The company has information security-related policies and rules that everyone should comply with, which is common for many companies. However, having defined policies does not automatically make the employees follow them [RvS04], and this is true also in this case. When the interview candidates were asked about the company policies almost all of them got somewhat hesitant. Some first gave the impression that they were very familiar with them but admitted, after a while, that they were unsure. After some thinking they did mention some security-related actions that they did during their day, and they also said they believed that the campaign considered some of the policies. Perhaps the interviewees would have remembered more if they had been given more time, but there was generally consistent hesitation and insecureness when talking about the policies. Two actions that were frequently mentioned were *Locking the computer screen when leaving it* and *Be careful with e-mails*. The employees said that they were exposed to the policies at the beginning of their employment in the way that they had to sign a document proofing that they had read them. Besides from that, the employees admit that they have not been exposed to them, and they cannot remember to have been tested or trained in the policies. According to von Solms & von Solms [RvS04], policies must manifest in some company culture, and that this can only be achieved through a proper education process. In the comment section in the surveys, it is also mentioned that the policies should be made more available for the employees. Additionally, it is mentioned that the policies should be more applicable, and the rules are characterised as being hard to practice.

Some of the interview candidates even admitted to not follow some of the policies though they were aware of them. Two main reasons were given for this; 1. They did not see how the policy was relevant to information security and therefore did not see the point in following the policy, 2. Practicality often comes before security, and all the others do it so it is more convenient if I do it as well. Particularly, if one does not understand the relevance of the policies, they might only seem like bothersome warnings and almost threats, and in the extreme case one might abandon all efforts

to act securely [EBFJ86]. One of the interviewees mentioned about the information security policies:

"(...) I guess they are mostly like 'Don't do this, don't do that'(...)",

and although the employee does not seem to find them directly threatening, he/she gives the impression that they are more bothersome than informing. Another employee expressed something similar in the comment section of the surveys:

"Inspire instead of using fear as a measure. Also, let us use common sense instead of having to be constantly scared of doing something wrong."

This is not an unreasonable opinion, as scaring and tricking people into complying with security measures do not gain the employees' attention and respect, as stated by Sasse [Sas15].

It also seemed like some of the employees were missing some good reasoning and explanations of the policies. Through the interviews, it seemed like many in the company tended to do what is practical above what is secure, and this is not uncommon. Kajava *et al.* also state that ease-of-use often is valued more than security in business life. One of the interviewees in this project articulated:

"A manager will do anything in his/her power to produce (...) and the risk of e.g. having information astray is not always highest on the agenda."

This is also something that was frequently seen in the comment section of the surveys; employees want reasons for the rules, and clear, simple alternative methods. Perhaps the most commented specific rule is the USB memory stick rule, which seems to frustrate many employees. One states:

"It has to be informed about why things are dangerous. For example the memory-stick, why is a memory-stick dangerous? What can one do to protect oneself if one has to use a memory stick? When people understand why, they get more motivated."

The interviewees explained that practicality too often comes before security, and this is reflected also in the comments of the surveys. Many explain that some of the policies are practically impossible to follow in their everyday work, as they hinder their work tasks.

Other things were mentioned during the interviews that may be interpreted to be reasons for not complying strictly with the policies. One reason could be that no serious situation has occurred yet, and so one is not fully aware of the consequences. This can again be seen in conjunction with the gap between theory and practice mentioned earlier. One may say that the reason for the gap is a regime

that is not strict enough, and that this, again, is because employees do not know the consequences, or do not believe it will happen to them. Bada & Sasse also mention that only after a hazard do things [norms/attitudes] change [DMB14]. Though the question was somewhat leading, one of the interview candidates answered the following to the question *Do you think a serious happening would motivate people even more to learn more [about information security]?*:

"Yes, absolutely. Then you get reminded of a vulnerable situation, and you want to do something about it. You don't want to do it again."

Another candidate expressed that the interest for information security was fairly big among his closest co-workers, and reasoned it with:

"I don't know if it's because we've had a couple of episodes (...), so that's pretty serious. We have seen the consequence of not being secure."

Another reason for flexible compliance with the policies could be that security-related expectations are not clear enough, making it easy not to prioritise security. A candidate expressed this about failing to do security-related actions:

"I think that everybody, in general, wants to do the best that they can. But one has different prioritisations, and if the expectations are not there, it's not even wrong to abstain from doing things. Because if there are no expectations, it's legitimate to have another prioritisation. So to make sure that things are done, one has to help people to prioritise, and that's done through accuracy and expectations."

This relates well to the concept of information security culture (defined in Definitions 2.1), which the relevant candidate also mentioned at some point in the interview. As is described by von Solms & von Solms [RvS04], a culture needs to be cultivated in order to make the employees satisfy the intentions of management. According to Schein [Sch92], cultivating a security culture involves, among other things, defining and developing shared assumptions for the management and employees. This can be almost directly linked to the uttering above if one regards the assumptions as some kind of expectations. Hence, the lack of clear expectations could be a reason for non-compliance.

5.3.2 Organisation and Management

As hinted in the last paragraph and pointed out by Ajzen [Ajz11], organisational culture and norms are some of the things that influence the behaviour of employees. The last citation indicated that directness from management is important in order to produce desired behaviour in the company, but it is also important, as discussed in 5.1.3, that management is positive towards information security, and that they relay

it as an important topic. All of the interview candidates expressed that they believed their manager/boss to take information security seriously, and considered this to be an important and positive thing. The surveys also show that on average 70% of the participants felt the same. From the interviews, it also seemed like everyone, to some degree, felt expectations from their boss and had the feeling that information security is regarded as important to their co-workers. This is substantiated by results from the surveys that show that, in the statements explored, the majority of employees comply with the policies. The surveys also showed that the majority of the employees regarded information security as important. All this combined serves as a good basis for good information security culture in the company, but there is still some way to go remembering the frequently mentioned gap between practicality and security. Even though all levels of the hierarchy in a company consider information security important, people will keep failing to comply until a drastic change happens, and this has to come from management ([Par81]; [Bra68]).

5.3.3 IT Systems in the Organisation

Due to the relatively small amount of interview candidates, and therefore a fairly small variation span, it is difficult to insinuate affirmations or contradictions of already discussed hypotheses based on the interviews alone. Nevertheless, one interesting difference could be noticed between the different age groups of the candidates. Again, not many from different age groups were interviewed so opinions uttered might be arbitrary and independent of the age of the interviewee, but it is still alluring. When talking about the IT systems in the company, and especially the new platform, it is evident that it is the youngest employees that find it the most practical and easy to use. Not all of the older candidates expressed discontent with the new system, they said that it is originally a good system with high potential, but they stressed that it presents many challenges, and that it does not work optimally. They did not say directly whether this concerns themselves as well, however, the younger candidates uttered none of these concerns. Two admitted that some of the employees find the system more difficult to use, and insinuated that age could be a reason for "lagging behind". Morris & Venkatesh [MGM06] suggest that younger people adopt new technology faster, and this could be a reason for what the employees are experiencing in this case. However, the discussion of age differences in subchapter 5.1.2 did not give strong indications that age was a big hinder for learning new things in this specific company. Another reason mentioned by one of the young candidates was the fact of being newly employed. As newly employed, one is directly introduced to the new system, unknowing of the old one. By several occasions, the candidates mentioned that earlier, bad experiences with transitions and new tools seem like barriers for many employees. This corroborates well with research claiming that people have a hard time changing their habits and what they are used to [Hre74]. Danowski's research [JAD80] found that good experience with

computers leads to positive attitudes towards computers. Although this applied for computers specifically, it can be argued that a more general view on this is valid; good experiences (with whatever it might be) lead to positive attitudes (towards whatever it might be). A system difficult to use will eventually lead users to make mistakes and avoid it [DMB14], and so if the new system is perceived as more difficult to use than the old, that is a valid reason for trouble regarding migration. If it is true, what some of the employees sense, that it indeed is the older people that have the hardest time changing to new tools, this is not necessarily because they find it less important. On the contrary, security culture often comes with age ([KR17], [MGM06]), not with understanding of the topic. In other words, why the younger employees utilise the new system is not automatically because of security-related reasons, but because they find less trouble changing their habits, or they have only been taught the new system. Also, the conversations revealed no implications that either of the age groups found information security more important than another, rather everyone expressed that information security is highly important.

5.3.4 The campaign

All the interview candidates seemed generally positive to the campaign and the e-learning. However, only one said that he/she learned something new from the e-learning. The rest said that it served as a good reminder of things they already knew, and this seemed sufficient for them. They expressed that they still found the e-learning useful, but that there was no need for more. The fact that five out of six stated that the campaign did not teach them anything new is interesting, looking at the numbers from the surveys and the statement *Who do you learn the most about information security from?*. The last year the statement was posed, the majority answered that they learned most from the campaign. Either, the interviewees' opinions are not representative, or people interpret the statement/question to mean that it is mostly the campaign that serves as a good reminder, rather than themselves. Based on what the interviewees said, it seems like they do not feel the need to learn more about information security, and this is curious when 85% if the survey participants declared that they do want to learn more about the topic. Either, people have stated that they are more motivated than they really are, or the conversations were, unintentionally, interpreted in disdain of the candidates.

The general impression is that the interview candidates did not feel the need for more material, but several mentioned that the material could have been distributed more evenly over the year, and like stated by Puhakainen & Siponen [PP10], a *continuous* communication process is important for an effective program. Although time was mentioned by one of the interviewees as a possible reason for not completing the e-learning, it seems like they would not mind spending time regularly on the campaign. They also explicitly said that time was not a hinder for them, personally,

to finish the e-learning. Also, the surveys show that only 7% say that they cannot prioritise a four-minute video about information security, so, in general, the campaign (the e-learning especially) does not seem to take too much of people's time, or the employees seem to want to prioritise it. As can be seen in Figure 5.6, the majority actually say that they could prioritise this on a monthly basis.

There are also split opinions about the competition element to the campaign. The partition here is evident, and substantiated by the results seen from exploring the statement *What are the biggest motivations to learn about information security?*, and discussed in the Age subsection 5.1.2. In the interviews, it is clear that the older candidates are little impressed by receiving cake as a reward for being the department with the highest e-learning completion rate. They seem sceptical about the competition part in general, and expressed that it should not be necessary. The younger candidates, on the other hand, seem excited about the competitions and suggest that there be more of it.

What also seemed to be positive to all interview candidates was the use of local and familiar faces, and that the campaign had an own name and logo, exclusively for use in the company. It may seem like the employees were motivated by some kind of feeling of ownership, and this is also seen in the study of Kruger & Kearney [HAK06]; when implementing a program, they found it important to get the local buy-in and identification with the program.

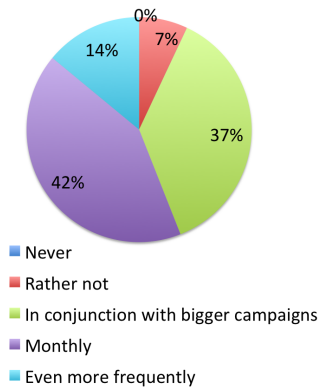


Figure 5.6: Employees' answers to the statement *I can prioritise four minutes to a e-learning video about information security.*

In total, the interview candidates seem to regard information security as important themselves, and they have the impression that people around them do so as well. This was also the general impression from the survey comments; though some of them were directly negative, a lot were very positive. The company seems to have a good foundation for a good security culture, but ease-of-use seems to still come before security in many cases. The company policies for information security seem to be vague for most, but the interview candidates do mention some security actions that they do in their daily work. The

new platform that the company has decided to use seems to be adopted faster by younger employees compared to older, and it is suggested that older employees in general lag somewhat behind. The campaign, in general, seemed to appeal to all interviewees, though most of them stated that it did not teach them anything new. Nevertheless, they expressed that they found it useful, and that they had no problem prioritising time for it.

5.4 RQ3: What is the optimal way of relaying security awareness, and to motivate all employees?

This section debates which is the optimal way of relaying information security awareness, and the indications and/or suggestions formulated are based on the discussions of *RQ1* and *RQ2*, and the interviews.

As mentioned in earlier sections, there are certain "official" criteria for a campaign to be effective, or to be good. For example, the material of the campaign should be current and interesting [HAK06], it should be well planned, and regularly assessed and adapted [MW03]. Planning a campaign is something that can be fairly straightforward, and assessing a campaign is also something that there has been done research on (e.g. [HAK06] and [MW03]), albeit little. Finding current material is fairly simple, but how can one determine what is interesting, and is it possible to create interest? Results in this project have indicated that there are differences in how gender, age groups, and responsibility levels view information security and the implemented campaign, hence implying differences in their interests. Obviously, not all of the same gender or age group think the same and have the same interests, but considering some of the apparent differences that do exist, perhaps they should be accounted for in the work of information security awareness. This project has mostly considered establishing the differences, not so much what they are and how this can be used in the work of security awareness, but it can be a good basis for further research on the topic.

Some clear differences were found in motivation for learning about information security, however. This is, arguably, one of the most important factors in the work of information security awareness, and should definitely be studied further. For instance, it was evident that more older people were more motivated by attention around the campaign than younger. Also, the competition element seemed to appeal to more younger people than older, which is something that was also seen in the interviews. Only one significant difference was seen in the motivation between genders; that of receiving a diploma upon completion of the e-learning. A difference in motivation between responsibility levels was the usefulness of the material in private life, where the people with highest responsibility levels were the fewest to answer. All of these differences (and possibly many more), should somehow be considered when planning

and implementing an information security awareness campaign. Perhaps even several versions of the campaign could be made, targeting different groups. Evidently, good planning and needs assessments should be conducted in this case, as suggested by NIST [MW03], in order to avoid misuse of resources, time, and money. Perhaps utilising the differences between people may help to create interest for information security, and as interest is assumed to be the cornerstone for all learning [Nor17], this would be optimal.

Some of the interview candidates did not believe there are any creative ways to motivate the employees, and that making them, dutifully, follow rules is the only way to ensure desired security behaviour. However, some things were mentioned by other candidates who did believe in methods to produce motivation. As commented in the Interview sections 4.3 and 5.3, many of the interviewees expressed that the campaign rounds could have been distributed more evenly over the year. A couple of them said that, given the chance to change the campaign, they would have done more of relevance in between the rounds, of relevance referring to attention in general around the campaign and about information security. It was commented that information security is a topic that could be on the weekly/monthly meeting agenda. Having tests in retrospect of the e-learning was also suggested, that way the employees would be reminded of the issue, and be tested to see if they actually learned something from the e-learning. One candidate also said that he/she would prefer more practical work on the topic, and that working in groups could be motivating.

5.5 Validity and Reliability

As the surveys in retrospect of the campaign rounds were not obligatory, and not encouraged to complete to the same extent as the e-learning, not all of the employees participated, and it may be argued that the employees that did participate may have contributed to partial results. In other words, the employees who decided to complete the surveys may originally have been more interested, motivated, or positive, which may mean that indications made from the results are not entirely correct. There is also a chance that the answers in a survey are not completely honest, and the fact that there are predetermined answer alternatives can make the answers less accurate. Nevertheless, the number of employees that participated in the surveys does fulfil the sample size required to yield a confidence level of 95% and a confidence interval of 3, considering around 2000 employees. This means that with a certainty of 95% and an error margin of 3%, the same answers will be obtained if the surveys are conducted again. Also, the fact that there are three surveys over three years gives a good basis for making indications in the cases where the results corroborate, e.g. where the mean numbers show a direct correlation there is bigger ground for implying that there is something of importance.

The sample size of the qualitative part of this project, the number of interview candidates, could surely have been bigger, but because of time restrictions, this was not feasible. Optimally, the number of interview candidates should not be predetermined, rather one should interview candidates until saturation is achieved, i.e. nothing new is found.

In general, it is a huge challenge to measure security. In this case, the surveys were used as a means to measure, but the employees were not explicitly tested in their knowledge/behaviour before and after the campaign, so it is difficult to determine the actual learning outcome. The interviewees said that they did not feel like their behaviour had changed due to the campaign, but the numbers from the surveys showed a general change in behaviour. It might be that the employees have been subconsciously affected by the campaign throughout the years, but that they are not really aware of it, and how do one measure this kind of influence?

5.6 Further work

As mentioned in subsection 5.4, this project has mainly focused on establishing differences, not necessarily what the differences are and how they can be used in the work of information security awareness. Evidently, further research on findings in this project is relevant, but also more specifically what the differences are, and how they may be used in awareness work. It may have to be considered that the employees participating in the surveys are employees that in general are more positive to the campaign and/or information security training, and it would, therefore, be interesting for additional investigation to somehow involve the total number of employees in the company to see if the results would be different. Additionally, it would be curious to learn the underlying reasons as for why people are not motivated or participating, by asking employees directly about this. This could be done through a survey, or through interviews. Perhaps face-to-face conversations with employees are more effective for revealing root causes, and in that case, it is advised to press the interview candidates by using e.g. the root cause analysis technique of asking "why" 5 times [Wil01]. It would also be interesting to see if the analysis of the interviews are substantially different if more candidates are interviewed, perhaps the conclusions implied based on the interviews in this project are somewhat unilateral due to the small sample size of interviewees.

Not only would it be interesting to expand the research to consider the entire company, but to broaden it to involve more, and different, kinds of organisations. Perhaps differences found in this company do not exist in other kinds of companies, or perhaps there are differences not revealed in this company that exist in others.

Chapter 6
Conclusion

The importance of information security awareness within companies is widely acknowledged, and it is important that employees understand the security risks of the company, understand their individual role in the security picture, and that they comply with company policies. One way to raise the awareness level of employees is to implement information security awareness campaigns/programs. People have different opinions on the effectiveness of such campaigns, but not many studies have been done with regard to measuring the effect. Also, many different kinds of people work in an organisation, perhaps having very different attitudes and approaches to information security and information security campaigns.

This project considered a specific case where an information security awareness campaign had been implemented in a research company over three years. The surveys that followed each round of the campaign were used in order to answer the three research questions stated in the Introduction.

RQ1 From the surveys, it seems like the specific campaign appealed to relatively more women than men, but it is hard to say whether this is because of personality differences between genders, or if it is because women to a bigger extent are positive towards the campaign and information security training than men. Nevertheless, there are differences in their views of information security which could be interesting to study further. Relatively more of the older than younger employees seemed to take interest in the campaign. As with gender, it is difficult to conclude if this is because of a positive attitude towards the camaign or information security training in general, or if it is because of norms and a growing feeling of company culture that comes with age. A clear pattern could be seen when investigating management responsibility levels and information security. Overall, a higher level of responsibility seemed to lead to a higher feeling of responsibility towards information security. However, it did not necessarily lead to a more secure behaviour.

RQ2 The campaign seemed to have some impact on the employees' motivation

and behaviour, to the extent that this can be inferred from the available data. The interviewees expressed that they learned little or nothing new from the campaign, and that they had not experienced any change in behaviour because of the campaign, neither with themselves nor with their co-workers. This is interesting, as the measurements from this project indeed show a change. The fact that they stated that the campaign had taught them nothing new, however, does not mean that their behaviour could not have changed; the campaign may have served as a good reminder of what they already knew, as confirmed by the interviewees as well, and in that way changed their behaviour. It is interesting though, that they cannot perceive any change in behaviour due to the campaign, when the numbers show a change. As explained in section 5.5, the campaign may have influenced the employees without them explicitly noticing it, and this kind of effect is hard to measure.

RQ3 Based on the findings of the two first research questions, the optimal way of relaying security awareness in a company would be to reach out to all the different kinds of people working in that company. As the answers to *RQ1* showed, there are differences between male and female, old and young, and between different responsibility levels, regarding information security, and there are surely many more differences than explored in this study. Not only should the content of a campaign be current and relevant in general, it should be relevant to different kinds of people; the same message could be conveyed differently to reach and motivate more people. One general thing that seemed to motivate the employees in this specific case, was not only to be given the rules but also be told the reason for them. It was also mentioned that a test in retrospect of the campaign could be a good contribution to all the information given to the employees.

Awareness is just one of many factors contributing to secure behaviour [KR17], but it should be taken seriously. Awareness campaigns should be well planned and structured. In addition to this, as communicated throughout the study, it is important that management has a big and deciding role in the work of information security, as only they can get things done efficiently.

References

[ABC15] *Proc. 10th International Conference for INternet Technology and Secured Transactions (ICITST, London, UK, December 2015)*. IEEE, 2015.

[Ajz91] Icek Ajzen. Theory of planned behaviour. *Organizational Behaviour And Human Decision Processes*, 50:179–211, 1991.

[Ajz11] Icek Ajzen. The theory of plannned behaviour: Reactions and reflections. *Psychology & Health*, 26:1113–1127, 2011.

[Alb07] Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26:276–289, 2007.

[AMG11] David A. Hofmann Adam M. Grant. It's not all about me - motivating hand hygiene among health care professionals by focusing on patients. *Psychological Science*, 22:1494–1499, 2011.

[Boy98] Richard E. Boyatzis. *Transforming Qualitative Information: Thematic Analysis and Code Development*. SAGE, 1998.

[Bra68] Allen Brandt. Danger ahead - safeguard your computer. *Harvard Business Review*, pages 97–101, 1968.

[Bry06] Alan Bryman. Integrating quantitative and qualitative research: how is it done? *Qualitative Research*, 6:97–113, 2006.

[Dav89] Fred D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13:319–340, 1989.

[Dec75] Edward L. Deci. *Intrinsic Motivation*. Springer, Boston, 1975.

[DMB14] Professor Angela Sasse Dr. Maria Bada. Global cyber security capacity centre: Draft working paper. cyber security awareness campaigns - why do they fail to change behaviour? 2014.

[EBFJ86] K. Rost E. B. Fisher Jr. Smoking cessation: a practical guide for the physician. *Clinics in Chest Medicine*, 7:551–565, 1986.

[ELD85] Richard M. Ryan Edward L. Deci. *Intrinsic Motivation and Self-Determination in Human Behaviour*. Springer, Boston, 1985.

[Fah] Ryan Fahey. Top 7 security threats for employees.

[Gub87] Egon G. Guba. What have we learned about naturalistic evaluation? *American Journal of Evaluation*, 8:23–43, 1987.

[HAK06] W. D. Kearney H. A. Kruger. A prototype for assessing information security awareness. *Computers & Security*, 25:289–296, 2006.

[Hre74] Lawrence G. Hrebiniak. Exploring organizational culture for information information security management. *Academy of Management Journal*, 17, 1974.

[IA75] Martin E. Fishbein Icek Ajzen. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley, 1975.

[JAD80] William Sacks James A. Danowski. Age differences in attitudes toward computers. *An International Journal Devoted to the Scientific Study of the Aging Process*, 6:125–135, 1980.

[JK06] Rauno Varonen Reijo Savola Juha Roning Jorma Kajava, Juhani Anttila. Senior executives commitment to information security - from motivation to responsibility. In *International Conference on Computational Intelligence and Security*, pages 1519–1522, Guangzhou, 2006.

[J.M01] Todd J.Maurera. Career-relevant learning and development, worker age, and beliefs about self-efficacy for development. *Journal of Management*, 27:123–140, 2001.

[JMS05] Paul Mastrangelo Jeffrey Jolton Jeffrey M. Stanton, Kathryn R.Stam. Analysis of end user security behaviors. *Computers & Security*, 24:124–133, 2005.

[JNC92] Lynn McFarlane Shore Jeanette N. Cleveland. Self- and supervisory perspectives on age and work attitudes and performance. *Journal of Applied Psychology*, 77:469–484, 1992.

[Jr.97] Bernard E. Whitley Jr. Gender differences in computer-related attitudes and behavior: A meta-analysiss. *Computers in Human Behaviour*, 13:1–22, 1997.

[JS15] Shwadhin Sharma Jordan Shropshire, Merrill Warkentin. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[JVN10] R. Von Solms J.F. Van Niekerk. Information security culture: A management perspective. *Computers & Security*, 29:476–486, 2010.

[Kit04] Barbara Kitchenham. Procedures for performing systematic reviews. Technical report tr/se-0401, Department of Computer Science, Keele University and National ICT, Australia Ltd, July 2004.

[KR17] Dr. Gregor Petric Kai Roer. Indepth insights into the human factor: The 2017 security culture report. Technical report, CLTRe, 2017.

[LLC16] Ponemon Institute LLC. 2016 cost of data breach study: Global analysis, 2016.

[Løl3] Gunnar G. Løvås. *Statistikk - for universiteter og høgskoler*. Universitetsforlaget, 3 edition, 2013.

[Mal11] Kirsti Malterud. Qualitative research: standards, challenges, and guidelines. *The Lancet*, 358, 2011.

[MET98] Rossouw von Solms M. E. Thomson. Information security awareness: Educating your users effectively. 6:167–173, 10 1998.

[MGM06] Viswanath Venkatesh Michael G. Morris. Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Phsycology*, 53:375–403, 2006.

[MW99] Crabtree BF Miller WL. *Doing qualitative research*. Thousand Oaks, CA: Sage Publications, 2 edition, 1999.

[MW03] Joan Hash Mark Wilson. Building an information technology security awareness and training program, 2003.

[Nor17] NorSIS. Nordmenn og digital sikkerhetskultur. Technical report, Norsk senter for informasjonssikering, 2017.

[oH] University of Huddersfield. What is template analysis?

[Org13] International Standards Organization. Iso/iec 27002: code of practice for information security management, 2013.

[Par81] D. B. Parker. *Computer Security Management*. Prentice Hall, 1981.

[Por63] Lyman W. Porter. Job attitudes in management: Ii. perceived importance of needs as a function of job level. *Journal of Applied Psychology*, 47:141–148, 1963.

[PP10] Mikko Siponen Petri Puhakainen. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34:757–778, 2010.

[Pre01] Marc Prensky. Digital natives digital immigrants. *On the Horizon (MCB University Press)*, 9, 2001.

[Rho83] Susan R. Rhodes. Age-related differences in work attitudes and behavior: A review and conceptual analysis. *Phsycological Bulletin*, 93:328–367, 1983.

[Rob11] Colin Robson. *Real World Research*. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom, 2011.

[Rob13] Alyssa Robinson. Using influence strategies to improve security awareness programs. https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385, 04 2013. Accessed 18-04-2018.

[RSS09] Albert L.Harris Hui-Jou Huang R. S. Shaw, Charlie C. Chen. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52:92–100, 2009.

[RvS04] Basie von Solms Rossouw von Solms. From policies to culture. *Computers & Security*, 23:275–279, 2004.

[Sas15] Angela Sasse. Scaring and bullying people into security won't work. *IEEE Security & Privacy*, 13:80–83, 2015.

[SB08] Lisa Kervin Sue Bennett, Karl Maton. The 'digital natives' debate: A critical review of the evidence. *BJET*, 39:775–786, 2008.

[Sch92] Edgar H. Schein. *Organizational Culture and Leadership*. Jossey-Bass, 2nd edition, 1992.

[Sip00] Mikko T. Siponen. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8:31–34, 2000.

[vS00] Basie von Solms. Information security — the third wave? *Computers & Security*, 19:615–620, 2000.

[WGG97] Nancy Eisenberg William G. Graziano. Agreeableness; a dimension of personality. In J. Johnson R. Hogan, S. Briggs, editor, *A Handbook of Personality Psychology*, chapter 30, pages 795–870. San Diego, CA, San Diego, CA, 1997.

[Wil82] Gerald J. S. Wilde. The theory of risk homeostasis: Implications for safety and health. *Risk Analysis*, 2:209–225, 1982.

[Wil01] Patricia M. Williams. Techniques for root cause analysis. *Baylor University Medical Center Proceedings*, 14:154–157, 2001.

[YJW11] Jacob B. Hirsh Yanna J. Weisberg, Colin G. DeYoung. Gender differences in personality across the ten aspects of the big five. *Frontiers, article 178*, 2, 2011.

Interview Guide

.1 Interview Guide

.1.1 Form

1. Introduction of interviewer and introductory warm-up question to the interviewee
2. Prior knowledge, and associations to the topic
3. Key questions
4. Round up

.1.2 Introduction

1. (Introduction of interviewer, reason for interview, and how the interview will be used)
2. Can you first tell me a little about yourself?
3. Briefly, what does your every day work involve?
4. Have you every been worried that your work might be of interest to somebody outside of the company?

.1.3 Prior knowledge, and associations to the topic

1. What do you associate with IT in the company?
   - How are your experiences with this?
2. What do you associate with information security?
   - How are your experiences with this?
3. To which degree would you say that you think about, or don't think about, information security during your work day?
   - Do you deliberately do any information security counter measurements?
   - Which, and why?
4. Would you say that you act securely enough for your working situation?

   - Do you deliberately do any information security counter measurements?
   - Which, and why?

5. To what extent would you say that your coworkers act securely?
   - What is your impression of your coworkers attitude to information security in general?

.1.4 Key questions

1. How familiar are you with the company's information security policies?
   - What are your thoughts around these, and to which degree do you follow them?
2. Many companies implement some sort of information security awareness program to make employees aware about the company's information security policies, about information security in general etc. What are your thought around such programs?
3. Are there some roles/positions that you perceive as more responsible for maintaining/thinking about information security than others?
   - Who and why?
4. How do you perceive your boss to consider the topic of information security?
   - Do you feel that he/she has expectations to you or your department?
5. About the specific campaign that was/is implemented:
   - What are your thoughts around it?
   - Do you have any thoughts about the visibility of the campaign?
   - What do you think about the method(s) that was(were) utilised to inform about information security?
6. Have you completed the e-learning?
   - Why/why not?
   - do you have a feeling of whether the e-learning was obligatory or optional?
7. What has the campaign taught you?
8. How has the campaign influenced your work day, with regards to information security?

9. Do you have any impression of whether the campaign has influenced your coworker's work day with regards to information security?
10. Do you have any opinions about how the campaign and awareness work could have been done differently?
    - What do you think could engage the majority of people?
    - What engages you?

.1.5 Round-up

a) (Interviewer tries to summarize most important points made during the conversation)

b) Do you have anything more you want to add?