Universiteit Leiden

ICT in Business and the Public Sector

Quantifying the Effectiveness of Cyber Security Awareness on Human Behavior

Name: Mounaim Ben Touhami
Student-no: 2636263

Date: 17/07/2021

1st supervisor: Dr. O. Gadyatskaya
2nd supervisor: Dr. T. van Steen

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Universiteit Leiden

ICT in Business and the Public Sector

Title page

Quantifying the Effectiveness of Cyber Security Awareness on Human Behavior

Author:	Mounaim Ben Touhami
Student number:	2636263
Date:	17 July 2021
Version:	1.0
Institute:	University Leiden
Study:	ICT in Business
University supervisor:	Dr. O. Gadyatskaya
Second reader:	Dr. T. van Steen
Period:	January 2021 – July 2021
Organization:	PwC
Internship supervisor:	Damaris Sweet

Abstract

Even though more and more organizations adopt a cyber security awareness program, cyber security incidents are increasing. The aim of this research is to quantify the effectiveness of cyber security awareness activities on human behavior. This is done by indicating which cyber security awareness activity or which mix of cyber security awareness activities is most effective, so that these activities can be applied in a proper manner and frequency. This mix of activities can prevent or limit the risk of a security breach.

In addition to prior literature, interviews with various professionals were used to provide insights to better understand human behavior. This resulted in four predictive factors that influence the success of implemented cyber security awareness activities. These four factors are:

- *Embedded culture* – The culture of cyber security awareness should be in line with the existing culture of the organization. An effective relationship between the cyber security department and employees is important.
- *Technical aspect* – Technology can be used at the front-end, e.g. where spam email is already filtered out. Technological interventions could have a positive influence.
- *Repetitive* – Repetition of the message is important to keep it alive. The same message must be presented in a different form.
- *Target specific audience* – The message has to fit the role of the professional and focus on what is relevant to the employee.

Furthermore, a survey is used to determine which cyber security awareness activity is observed as the most effective by employees. The answers of the respondents were ultimately used as input for the model. Based on the survey results, each cyber security awareness activity is weighted in points, to make their contribution relative to each other. We also determine that a minimum of awareness-raising activities is required in order to be sufficiently familiar with the risks of cyber security.

Lastly, the distinguishing characteristic of this study is that a model has been developed which consists of the quantification of cyber security awareness activities (such as an e-learning, gamification, etc.). This model establishes a baseline that defines the minimum awareness-raising activities needed to increase awareness of cyber security risks.

Acknowledgments

This is my thesis entitled “Quantifying the Effectiveness of Cyber Security Awareness on Human Behavior”. This thesis was written as part of the completion of my ICT in Business study at Leiden University. The graduation internship took place at PwC.

With this thesis my study have come to an end. In 2019, I enjoyed my first lectures to graduate within two years. It was a period that I look back on with great pleasure. The study has developed me into a skilled professional who is at the start of his career. The best way to predict your future is to create it yourself. I feel like I have done that too and I am far from finished. I would like to thank all teachers for their contribution to my development.

'The best way to predict the future is to create it.'

Abraham Lincoln

I would like to express my special thanks and gratitude to those who supported me in various ways during my research. First and foremost, special gratitude goes out to my research supervisor Olga Gadyatskaya for providing continuous support, energy and feedback. I would also like to thank Tommy van Steen and Damaris Sweet for their assistance and feedback.

Furthermore, I would like to thank all research participants for their time and provided insights. Without these valuable individuals, parties, and enterprises, this research would not have been possible. Finally, yet importantly, I would like to thank my family and friends for their unconditional and continuous encouragement and support throughout the entirety of this dynamic and exciting research trajectory.

I hope you enjoy reading it.

Mounaim Ben Touhami

Schiedam, July 17, 2021

Table of content

1. Introduction

1.1 Background

Cyber security awareness is no longer a neglected child on the agendas of business leaders. To better understand why one should be aware of cyber security, we need to step back to understand cyber security in its entirety and the associated threats. The widespread and continually changing nature of technology means that more people than ever before are affected by cyber security incidents (Jones et al., 2019).

Companies see people as the weakest link when it comes to security incidents. The weakest link as a human is also true given the stated facts. However, it is not useful to create a guilt culture. The result of such a culture is that people are not likely to report incidents. This behavior usually happens out of fear for their own reputation within the organization (Swinhoe, 2019).

Professionals that are at the forefront of cyber attacks or threats could do more damage than others. The negligence of employees can cost organizations not only money, but also valuable information. The danger from the employee might not always be deliberate; it may be due to the lack of adequate awareness of cyber risk and consequences. So, the level of awareness IT employees have about cyber risks in the corporate network must be understood. Cyber security awareness programs that can help both employees and organizations recognize the vulnerability of the network should also be pursued by organizations (Al-Mohannadi et al., 2018, p. 191).

A successful training program for cyber security should help employees understand why they need to take cyber security seriously and what they can gain from its proper implement-tation. Ideally, by promoting a shift in the attitude of employees towards cyber security, a cyber security awareness program should prepare employees for cyber security training (Thomson & von Solms, 2006, p. 13).

This master's thesis examines which cyber security awareness activities there are in the field of cyber security. The effectiveness will be examined for each activity. In addition, the quantification of the effectiveness of cybersecurity awareness activities on human behavior will be addressed. The result will be a model that organizations can use in any setting to be more effective in creating awareness about the subject of cyber security.

1.2 Problem description

Cybercrime costs are expected to increase by 15% each year over the next five years, hitting $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015 (Morgan, 2021). In addition to having an impact on companies, cyber security incidents can have a negative effect on individuals (phishing attacks, identity theft), national and state level (state-sponsored attacks, coordinating crime groups, leveraging vulnerabilities on 'smart' devices to access data, control systems, or vital national infrastructure), due to the interconnectivity of digital technologies (Spremić & Šimunic, 2018, p. 4).

Even though COVID-19 (in relation to cyber security) is not a main research focus for this study, it is important to note that due to the Covid-19 pandemic this year, the cyber risks have increased manifold (Nabe, 2020). One of the key reasons why users do not act optimally in the context of cyber security is that security systems and policies are poorly designed (Bada et al., 2015). Cyber security incidents are often caused by human actions. People fall prey to strategies of social engineering, phishing or other techniques of cyber criminals. Cyber security knowledge and training has been shown to improve the possibility of detecting a scam or assault before it has a full impact (Furlow & Disparte, 2019).

With the home working policy, it is estimated that the losses from cyber attacks will only increase (Auld & Smart, 2020). The importance of this research can be found in the study by Buil-Gil et al. (2021). Research by Buil-Gil et al. (2021) suggests that the most promising ways to reduce cyber attacks and their consequences are through internal knowledge of cyber security and improving employees' online self-protection. This is better than simple software protection and strong password guidance.

This research will illustrate which cyber security awareness activity or which mix of cyber security awareness activities is most effective, so that these activities can be applied in a proper manner and frequency. This can prevent or limit the risk of a security breach.

We will offer important insights into the effectiveness of cyber security awareness activities on human behavior. The findings will make an important contribution to the field of cyber security risk and cyber security awareness. CISOs will be better equipped to make cost-efficient decisions about which awareness activities to implement in their awareness program.

1.3 Purpose and research questions

The aim of this research is to gain insight into quantifying the effectiveness of cyber security awareness activities on human behavior. This is done to indicate which cyber security awareness activity or which mix of cyber security awareness activities is most effective, so that these activities can be applied in a proper manner and the organizational risk can be limited.

The respondents and interviewees are professionals dealing with cyber security-related risks. The following research question is central:

"How can the effectiveness of cyber security awareness activities on human behavior be quantified?"

In order to answer this research question, the following sub-questions have been formulated:

1. What is cyber security awareness?

2. What cyber security awareness activities exist within organizations?

3. How much do these activities contribute to the cyber security awareness of a person?

4. What level of cyber security awareness is deemed "sufficient"?

5. What combinations are possible to achieve a solid result for sufficient cyber security awareness?

6. Which factors influence the success of implemented cyber security awareness activities?

1.4 Research scope

This dissertation is written as part of a graduation internship at PwC Netherlands within the Risk Assurance discipline. The focus is on large organizations where employees are expected to have a higher education degree and at least some degree of digital skills. Therefore, this research project focuses primarily on the Netherlands. This means that the majority of the participators and the context of the research are located in the Netherlands.

The most frequently used cyber security awareness activities during the writing of this thesis were included in this research. The following cyber security awareness activities were involved: interactive workshop, classroom training by a teacher, phishing simulation, e-learning, keynote by an expert speaker, cyber security awareness month, gamification, central information source. These were established through informal conversations with employees within PwC and literature research. The thesis will be limited to these activities.

In terms of time frame, this thesis has examined a threat that is constantly developing and ongoing. At the time of writing, the incident of the largest online store in the Netherlands Bol.com was only a few days ago and freshly engraved in the public memory. During this incident, Bol.com transferred 750,000 euros to scammers after the company fell for a phishing email (NOS, 2021). This study therefore provides insight into current affairs and has a future focus in terms of recommendations that can have a positive influence on the policies necessary to create more awareness against cyber security risks.

1.5 Outline of the thesis

This section presents the outline of the thesis, with the aim to demonstrate the process of answering the research questions. Chapter 2 describes the research design and methodology which have been chosen for the purpose of the study. Moreover, the qualitative and quantitative research method are described thoroughly from the perspective of theory. In chapter 3 a literature review will be conducted so that firstly, cyber security awareness and human behavior can be defined. In chapter 4 the results of the data collection methods are presented and linked to the relevant literature. The model constructed upon the results and the important factors for the model is described and discussed in chapter 5. In chapter 6 the results will be discussed and the limitations of the research. At the end of the thesis, the conclusion and questions for further research are discussed.

2. Methodology

In the introduction, a research question was formulated with the associated sub-questions. Varying methods will be used to answer the sub-questions and research question. These methodologies and their use are discussed in this chapter.

2.1 Introduction

The three primary research methods chosen for this research are a literature study of cyber security awareness, human behavior and the relationship with each other. Subsequently, interviews with various professionals were also used to provide insights to better understand human behavior and a survey was distributed among Risk Assurance professionals. The literature study aims to provide a conceptual framework with regard to cyber security awareness and human.

There have been several studies in the field of cyber security awareness. These studies are about the impact of cyber security awareness policy (Li et al., 2019), why people fail to change behavior (Bada et al., 2015) and best practices on how to improve awareness (Nachin, 2019). The distinctive character of this study is that a model is developed quantifying what cyber security activity (activities such as a seminar, a monthly email, etc.) contributes to awareness and a goal to be achieved (number of points that must be security aware). Additionally, interviews were held with various professionals to see which factors influence the success of implemented cyber security awareness activities.

The model essentially contains a scorecard, in which each cyber security awareness activity has a weight and is therefore awarded a number of points. The company can use the scorecard to determine how to create sufficient awareness among employees by combining the activities until the intended number of points has been reached.

This chapter aims to describe the scope of this research project and to illustrate how the different methods chosen for this research helped to find a satisfactory answer to the presented research question. It also describes the considerations that played a role in the use of the research methods selected for these projects.

2.2 Research approach

For the research approach, which data collection and data analysis techniques and procedures best suit the problem definition was examined. A research philosophy is used for this. The research philosophy contains important assumptions about the way in which one view the world. The different ones have been looked at. The "research onion" was chosen for this research.

The research onion was chosen because the shells of the research onion provide insight into the underlying issues underlying these methodical choices. The figure below shows the research onion (Saunders et al., 2009).

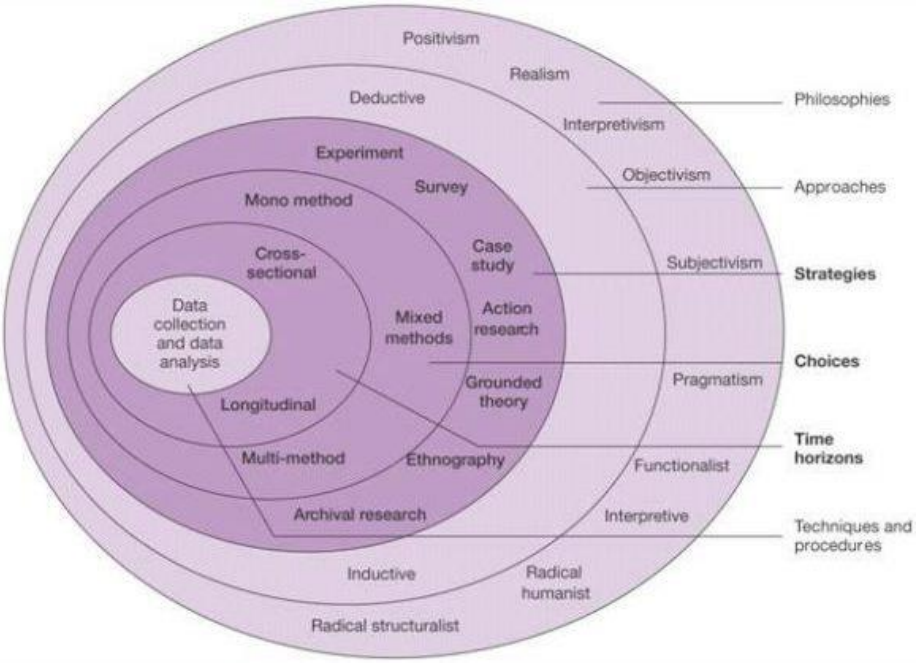


Figure 1 Research Onion (Saunders et al., 2009)

Interpretivism is defined by the research theory that will be used as the background for this research. Interpretivism uses the vision of the people involved to explain why groups of people behave in a certain way**.** Within this research it is important, because we put the individual at the center to research the effectiveness of cyber security awareness.

The method chosen to construct a theory will be inductive. By collecting data to analyze the phenomenon in question and to define possible trends and patterns, the construction of theory is realized. To support this approach methodologically, as Figure 2 illustrates, the emphasis will be on mixed methods research.

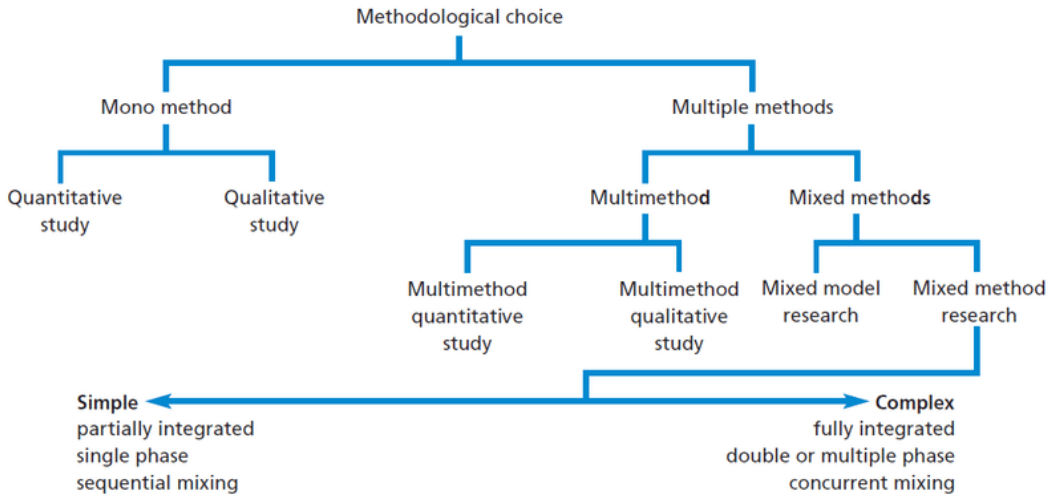


Figure 2 Methodological choice (Saunders et al., 2009)

Survey strategy and thematic analysis will be used for this research. The following subsection explains in detail the approach to data collection.

2.3 Research strategy

A strategy has been determined for this research. This is shown in the figure on the next page.

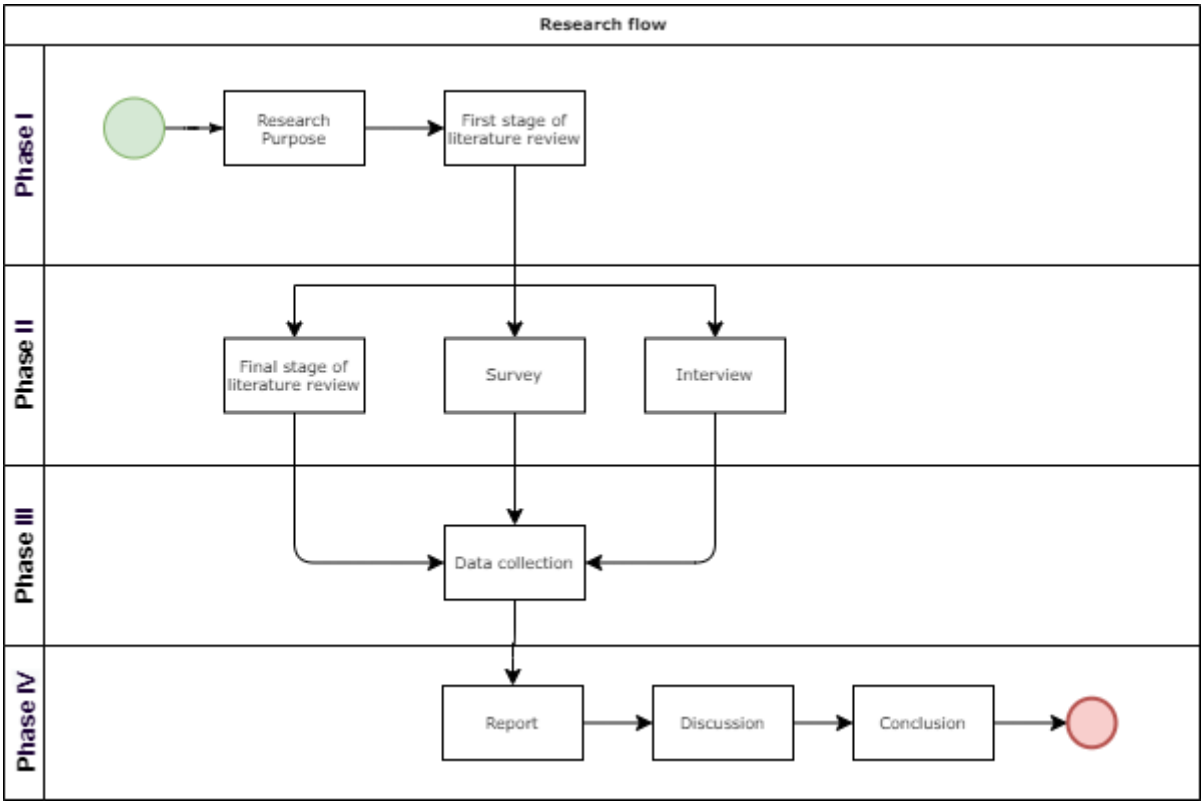


Figure 3 Research flow

Phase

I. The basis of a research is to formulate a goal for the research. The problem becomes clearer and the research questions are formulated. Subsequently, literature will be collected and read to get an idea of the topic.

II. The second phase shows that methodical triangulation is used. This is done to look at the problem from multiple angles. This phase is therefore the core content of this paper and represents the primary research stage.

III. In this phase, the results of the research methods will be interpreted. The interviews will be transcribed and coded to see what connections there are between them. The survey will be analyzed with the integrated output of the survey and interpreted.

IV. After the results have been described, the research question and the aim of the research are considered. This will help to formulate the conclusion. Finally, the discussion establishes the limitations of the research and validation.

2.4 Literature review strategy

Literature research focuses on analyzing texts, books and articles that themselves already contain interpretations of research (Verhoeven, 2019, pp. 150-155). The purpose of the literature study has two goals: first, to gain insight into cyber security awareness and the activities associated with it. Second, we looked at human behavior and the absorption of knowledge, but also how these behaviors relate to cyber security awareness.

In order to conduct the literature study, tools such as ScienceDirect, ResearchGate, Google Scholar search engine IEEE, white papers, scientific publications and journals were used. The literature has been checked whether the information is relevant, reliable, topical and complete. Also, whether the articles have been placed in magazines or in a peer-reviewed scientific literature. The literature of this research is divided into four categories:

- Industry standards;
- Scientific publications;
- Gray literature;
- Book.

Figure 4 shows a roadmap in order to select relevant studies to the literature search.

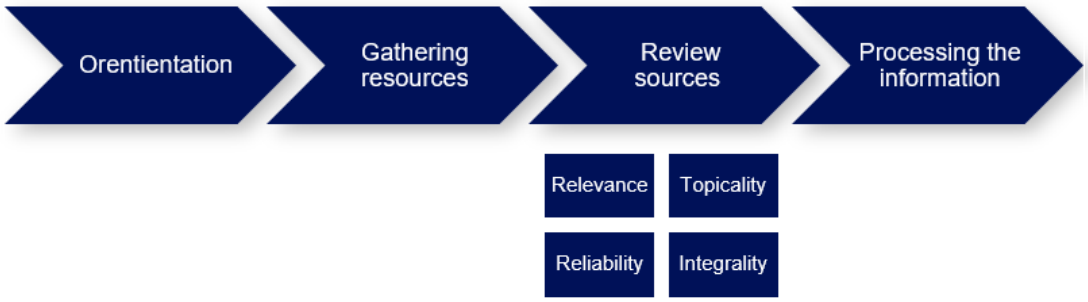


Figure 4 Roadmap literature review

Further in the literature review, the content of the definitions of this subject is explained. In view of the fact that most of the publications use this particular language, the language of the study was determined to be English.

2.5 Data collection and data sources

In this research, we make a distinction between the defender and the user. The defender refers to professionals who develop cyber awareness programs and make decisions about the professionals (employees) who can fall victims to cyber security attacks are referred to as users. This is illustrated in Figure 5.

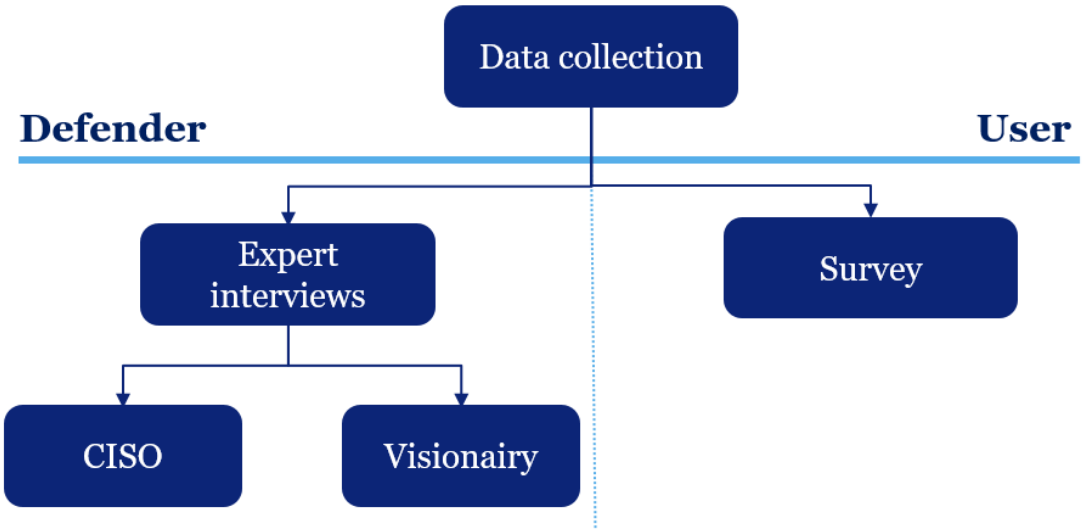


Figure 5 Data Collection Illustration

2.5.1 Interview

The defenders have been interviewed. The expert-interview method will be used to collect data from the professionals. An expert interview is a popular research tool in business-to-business research. It may look a lot like the in-depth interview (one-on-one conversation) in design, but it serves a completely different purpose. An expert interview does not focus on the respondent's perception, but on his or her specific knowledge, expertise or background. The interviewee therefore requires in-depth knowledge about a specific topic (Verhoeven, 2019, pp. 150-155).

Interview design

Semi-structured, one-on-one, online, and recorded interviews were conducted. To maintain uniformity in the interviewing process and to decrease researcher bias, a semi-structured interview was employed rather than an unstructured interview. One-on-one interviews were conducted to capture the perspective of only the interviewee and to reduce the possibility of the interviewee's opinion being swayed by outside influences. Because to government

constraints imposed by the COVID-19 epidemic, the interviews were conducted online utilizing conferencing software. The interviews were recorded for the purpose of analysis.

Two options were provided to the interviewees in order to promote their comfort. The first decision was whether or not to allow video. The interview could also be conducted in either English or Dutch. If the participant did not specify a preferred language, the interview was conducted in Dutch.

A brief introduction was given before the interview began. During this introduction, participants were reminded of the study's goal, asked to express as much about cyber security awareness as they knew during the interview (there were no wrong answers), and were reminded that the interview would be recorded.

For several reasons, questions on the meaning and necessity of cyber security knowledge within an organization were posed. First, the questions and answers served as a springboard into the subject, allowing the professional to assess the meaning and importance of cyber security awareness. Second, questions were posed in order to better understand the efficiency of cyber security awareness efforts. Finally, questions were posed about characteristics that are critical to the success of cyber security awareness, such as culture and technological aspects.

The interview began with the question, "how would you characterize cyber security awareness?" This question was purposefully broad in character in order to avoid biasing the interviewee. The participants were invited to expound on each of the topics stated. The interviewee was asked to define an idea after it was named. The interviewer moved on to the following question when no new topics were brought up.

The remaining questions were designed to be of a different sort in order to add variation and to be as neutral as possible in order to avoid biasing the interviewee. The interviewer tried remaining as passive as possible and only keep the oral fluency of the interviewee. The interviewer attempted to encourage the interviewee to continue talking and clarify themes by using neutral continuation suggestions. The interview protocol includes examples of neutral continuation prompts.

The participants were asked at the end of the interview if they knew anything else concerning cyber security awareness activities that had not been mentioned. Finally, the participants were thanked for their time and the interview was concluded when no additional issues were raised. Appendix l contains the English and Dutch interview protocol.

Prominent figures from different industries

There are two different categories for experts, namely the CISO and Visionary categories. The CISO category specifically means that this concerns a person with a leading position in the field of cyber security within an organization. They should be responsible for cyber security awareness programs/decisions. Furthermore, we set as criterion for this category that the professionals work within a multinational. These criteria were chosen because multinationals are complex in nature and have different target groups. In order to prevent a one-side image, the professionals from the CISO category have to come from different industries. Table 1 shows the interviewed professionals who participated in the survey. This also shows the date on which the interview took place, as well as the organization and the type of industry.

Table 1: Detailed interview schedules

Interviewee	Date	Position	Company	Industry
1	25.03.21	NSO[1]	Microsoft	Technology
2	26.03.21	CISO	IKEA	Retail
3	08.04.21	CISO	Eneco	Energy
4	08.04.21	CISO	Loyens & Loeff	Legal services
5	15.04.21	CISO	Ahold Delhaize	Food retailing
6	19.04.21	CISO	AkzoNobel	Chemistry, oil and gas
7	21.04.21	Head of Operational Excellence	Philips	Electronics and medical equipment
8	21.04.21	Teamlead CISO Strategy and Policy	KPN	Telecommunications

9	22.04.21	Head of Security Office[2]	ASML	Industry
10	22.04.21	CISO	Schiphol Group	Aviation
11	03.05.21	CISO	PwC	Professional services
12	03.05.21	CISO	Vodafone Germany	Telecommunications

[1] The abbreviation for NSO is National Security Officer.

[2] In this meeting, ASML's Security Awareness Manager also attended the interview.

Three different perspectives from visionaries

The visionaries category includes prominent figures, who are not directly responsible for security decisions within a single organization, but instead share their experience and vision via some channels (e.g., being cyber awareness consultants, public speakers). When selecting the visionaries, we opted for professionals who are active in the world of cyber security, human behavior or both.

Three different professionals were chosen to be interviewed, all of whom come from different angles and therefore have a different view of the problem. From the technical part, the American Chris Roberts is interviewed. Chris Roberts has made headlines both at home and abroad by hacking into Tesla, NASA and even a plane. Nowadays Chris is involved in the strategic field of cyber security. Lance Spitzner has a technical background but has been committed to creating more cyber security awareness in organizations for more than 20 years. He is director of security awareness at the SANS Institute in the United States. Finally, Inge van der Beijl has a psychological background, but later in her career dedicated herself to creating cyber security awareness at organizations at Northwave in the Netherlands.

Table 2: Detailed interview schedules

Interviewee	Date	Name	Position	LinkedIn
1	25.03.21	L. Spitzner	Director Security Awareness at SANS institute	https://www.linkedin.com/in/lance-spitzner-0ab0ba1/
2	26.03.21	C. Roberts	Chief Security Strategist	https://www.linkedin.com/in/sidragon1
3	29.04.21	I. van der Beijl	Director behavior & training	https://www.linkedin.com/in/ingevanderbeijl/

Sample size

In qualitative research, data collection is done until the point at which no new concepts emerge from the data. which is referred to as theoretical saturation (Bryman, 2012; Strauss & Corbin, 2008). As a result, the number of interviews to be held was not decided in advance. The goal was to collect and evaluate data repeatedly in order to detect when no new concepts arose after three interviews. Theoretical saturation was achieved if no new concepts surfaced during these three interviews.

Theoretical saturation has been reached, as no new concepts have been developed in the last three interviews. Therefore, when looking at the complete sample, theoretical saturation has been reached.

The interviews have been recorded and transcribed. This transcript was then analyzed using the thematic analysis method. This method is used for qualitative data. It is usually applied to a set of texts, such as interview transcripts. The researcher closely examines the data to identify common themes – topics, ideas and patterns of meaning that come up repeatedly (Verhoeven, 2019, pp. 292-299). The whole process involves the following steps:

1. Familiarization;
2. Coding;
3. Generating themes;
4. Reviewing themes;
5. Defining and naming themes;
6. Writing up.

To prevent the transcripts from being coded with bias, this was done together with a peer. After this we did a cross check, evaluated and merged the codes.

Ethical considerations

Participants were recruited via an informative e-mail after their name was provided by a contact person. When a participant agreed to be interviewed, an email was sent 7 days in advance with the interview questions. Furthermore, Participants were informed they could withdraw at any point without the need to provide a reason. Participants were not compensated for their participation.

Four types of data were gathered. The first type is the email addresses of the participants. Second is a PDF file of the informed consent email. Third is demographic information of the interviewees. Demographic information consisted of educational qualification, education area, role in the firm, and years active in the firm. Fourth is the recording of the interviews, which included audio and video if video was enabled during the interview.

Furthermore, the participant was asked for permission to process data and which data will be processed. The data was anonymized as much as possible. With the approval of the participants, it was decided to name the position and organization of the participants. If the text refers to an interesting finding to the participant, explicit permission for the quotation will be requested from the participant. There was a follow-up session with each participant who wished to discuss the findings.

Lastly, the survey only collected how long the participant works for the organization and what position the participant holds. The reason for this is to see whether the overall picture of the respondents is a good reflection of the department. These answers could not be traced back to the participant.

Survey design

In quantitative analysis, surveys are used to gather quantitative data, which is then analyzed by the researcher. This research used the online survey tool Qualtrics, for which Leiden University has a license, to create a survey. Qualtrics is a quantitative statistical analysis tool that allows researchers to construct online surveys or questionnaires. The full questionnaire can be found in Appendix lll. The overview by Verhoeven (2019) was used to design the survey. The overview can be seen in Figure 6.

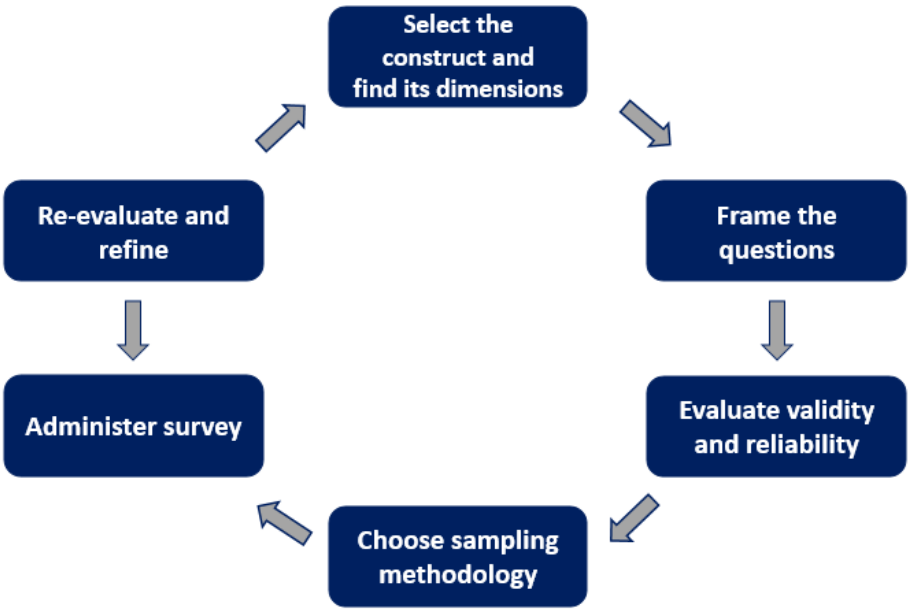


Figure 6 Design Survey Overview (Verhoeven, 2019)

The overview has different dimensions. The first is the introduction message that the respondent will see. This makes clear to the respondent what the purpose of the survey is, the length of the survey and how the data will be handled. If the respondent agrees, he will click on the next page. In the second dimension, the respondent will be asked how the organization deals with cyber security awareness. Given the data from PwC, it was the wish not to include this result in the thesis.

In the next dimension, extra information will be given about a number of cyber security awareness activities, so that no alternative interpretation can be made about the cyber security awareness activities. The next dimension will address the respondents' work on the activities. For example, the function must first be filled in per activity using the “Likert scale”, after which the respondent will have to consider which activity he or she considers most effective. This question can be seen in Figure 7 as well as in appendix lll. Finally, the respondent will indicate which combination of activities (or single activity) is needed to create sufficient awareness of cyber security for a new employee during a period of 12 months. The answers of this dimension are ultimately used as input for the model.

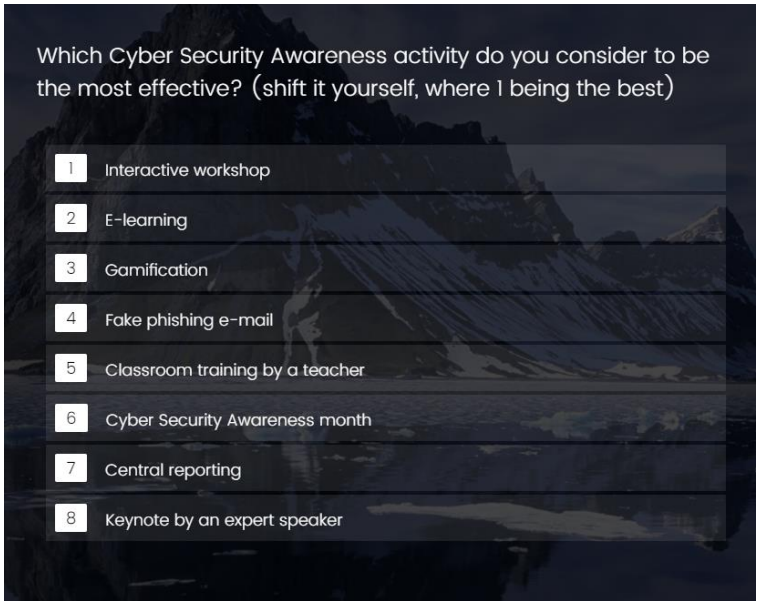


Figure 7 Part of the Survey

In the last dimension, space is given to the user to add something in the field of Cyber security awareness, if there is a need. The last questions are answered with what role the user has and how long this respondent has worked within PwC. This was asked to view the group composition of the respondents.

In the next step, these questions were validated and evaluated among a number of potential respondents. Feedback has been generated from this and has been incorporated into the survey. During the survey, a questionnaire will be administered online from several professionals.

The questionnaire will be administered online from several professionals of the Risk Assurance department within PwC to collect data about the research topic. During the design of the survey, it was continuously evaluated and refined.

The purpose is to recruit as many participants as we could, and the target was to have at least 50 respondents to ensure sufficient representation. To get this number at first point, the author of this dissertation distributed through PwC mail within Risk Assurance. Ultimately, 65 respondents completed the survey in February and March 2021.

3. Literature review

This chapter describes an in-depth study detailing the previously mentioned topics as well as laying a basis for answering the aforementioned sub-questions (see chapter 1.3).

3.1 Cyber awareness activities

A cyber security program consists of one or more activities. There are various methods that can contribute to awareness for cyber security. In the study by Nachin (2019) five methods are discussed, these are:

- Conventional delivery method;
- Instructor-led delivery method;
- Online delivery method;
- Game-based delivery method;
- Simulation-based delivery method.

Combining the methods with literature research and informal discussions, activities have been chosen for this research to determine its effectiveness. These activities will be described. The figure below shows which cyber security awareness activities are discussed for this research.

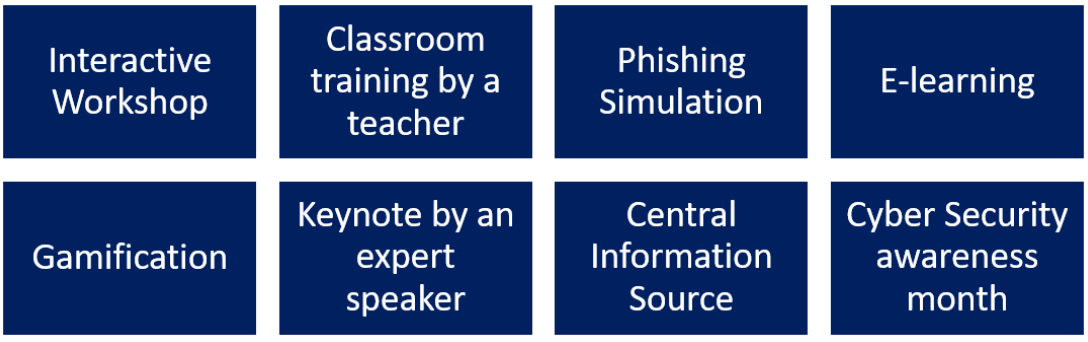


Figure 8 Overview cyber security awareness activities

Interactive workshop

A workshop is an interactive form of work in which the active participation of the participants plays an important role. It is a method in which theory and practice can come together. A research of Baird and Munir (2015) measured the effectiveness of workshops in a general sense. The results provide evidence that participators perceive that seminar-based

learning is effective in improving generic skills, including problem solving, critical thinking, and analytical skills.

However, the interactive workshop also has challenges. If the moderator does not take up his role sufficiently, there is a risk that various discussions will be mixed up, themes will not be discussed, ideas will not be explored. Furthermore, the presence of hierarchically high-ranking persons can act as a brake for the other participants to participate effectively in the workshop. Quite often it then happens that participants only repeat the opinion of the responsible person. Such workshops provide only limited added value.

(Online) classroom training by a teacher

A classroom training is a form of training in which participants are taught in groups by one of our teachers. The teacher first discusses a topic theoretically with examples, after which the participants get started with exercises (Bowden, 2017). Classroom training is a powerful means of empowering people with knowledge on focused topics, according to the study by Abawajy (2012). Almost all participants had a good understanding of phishing and its dangers for both individuals and organizations after the course.

The main challenges in this activity are shy students who have a hard time standing out in class (by not asking questions). It is also important that the teacher can dictate properly. (Bowden, 2017).

Phishing simulation

Wash (2010) argues that in order for a user to defend against a threat, the user must first be exposed to the threat. A phishing simulation operates in a way that allows users to receive phishing e-mails and record their actions. When the attack falls, users who respond "insecurely" receive a "training message".

Each simulated phishing email serves not only as a training tool, but also as a test to decide whether the user has learned how to separate legitimate messages from phishing messages. Therefore, only those users who continue to fall for simulated phishing attacks can be detected and provided with training interventions (Jansson & von Solms, 2013).

Chatchalermpun and Daengsi (2021) demonstrated with phishing simulations that cyber exercises and cyber security knowledge transfer can increase cyber security awareness. With a high level of awareness among all employees, it is more likely that a potential victim would report a suspected incident, and the necessary incident response would be initiated in time to limit the damage.

E-learning

Technology-enhanced learning (e-learning) has become one of the most common techniques of teaching and learning in higher education today. Indeed, without adopting the latest educational innovations that have come to characterize teaching and learning in the information and knowledge age, it appears that no higher education institution will thrive.

Abawajy (2012) conducted a study on the user preference of cyber security awareness delivery methods. The findings show that video presentation is the most preferred method for delivering security awareness training; however, the training delivered through the various methods appears to have been mostly successful in helping participants gain a better understanding of what phishing is and how best to mitigate its dangers.

On the other hand, self-discipline is required. It is therefore important that the person is enthusiastic enough about the subject matter, so that there will be enough motivation to easily follow and complete the e-learning attention. Also, taking e-learning can feel impersonal. Another disadvantage of online learning can be that the professional do not always have personal interactions with the teacher or fellow students (Bowden, 2017).

Gamification

Gamification has emerged as a modern approach that can supplement educational or computer-based safety training by offering a fun environment in which players learn and practice concepts of cyber security through the game. It is the application of game thinking and game techniques in non-game environments. Gamification use game elements to motivate users and enrich their experience. The principle of gamification is not new, people have been playing games for centuries. In fact, 72% of households play video games. We experience how effective games are in seducing, grasping, motivating and binding their players (Brown, 2017).

Applying those techniques and stimulating behavior in the real world is what gamification is all about. Gamification is not a game. It is more than that. It is a way to make the job more challenging and get significantly more work done (Hart et al., 2020).

Furthermore, participants in gamification may be so focused on the reward that all they have left is that they have won in the game and the essence of teaching or becoming aware of something goes beyond its purpose (Hart et al., 2020).

Keynote by an expert speaker

The purpose of a keynote speaker is to literally set the "keynote" for the conference or event. He or she is responsible for setting the tone and tenor of the meeting. The role of other speakers is to provide undertones and themes that complement the keynote, resulting in a cohesive body of conference content and messaging (Rossdawson, 2020).

Although some speakers are extremely captivating, there are plenty who are not. Attendees will quickly tune out if a speaker is less than engaging. This is particularly simple because of the essence of "passive" listening, that is, listening without interference or contact with others for an extended period of time. Due to learning decay, much of the data (about 95 percent) gained by passive listening is not retained. If the organization wants the corporate event to be entertaining and leave a lasting impression, it may not be the best option for a speaker who does not have a lot of audience interaction and movement. Passive sessions, in short, do not always lead to enthusiasm (Wigston, 2018).

Cyber security awareness month

It has been established nationally that October is the month of cyber security awareness. In this month, activities are organized both within and outside the organization to create employees more aware. For example, security officers can walk past laptops to see if they are locked. If not, a flyer is posted outlining what someone with bad intentions might do. This should be done with good intentions and not to create a culture of fear.

On the other hand to hit employees with the message, the sender have to cut through a lot of noise. Work which tends to be more urgent and time-sensitive is thrown their way. The sender is up against the abundance of distractions that make up our modern world, even outside of work: messages, emails, blogs, social posts and more. The message needs to be attention-getting, unforgettable, persuasive and concise to build a campaign that resonates (Smith, 2018).

Central information source

Awareness is mainly created through messaging in this activity. Sending messages can range from a newsletter by e-mail to posting on the intranet. However, this is not popular, as newsletters have a low opening rate. Not every newsletter is read. Especially if it feels like an obligation and do not seen as important. If the content is not interesting to readers and offers no added value, there is little success in this activity (Tyagi, 2020).

In short, there is no best activity to increase awareness among employees. Pratt's research (2021) says that lessons are much easier to absorb than when they are all packed into a long annual training event. Everyone learns differently, so those broad avenues of delivering are important. To the best of our knowledge, we could not find research papers that focused on the effectiveness of cyber security awareness month and central information source.

3.2 Human behavior

For this research, two aspects have been identified for improving cyber security awareness: learning ability to enhance cyber security awareness and changing behavior. This section deals with the human aspect without directly involving cyber security awareness.

Learning ability

A good base for formulating learning objectives is Bloom's Taxonomy. There are three main domains in learning, according to Bloom's (1956) taxonomy: affective, cognitive, and psychomotor domains, as shown in Figure 9. Attitude and emotions are part of the affective domain, while critical thinking skills and knowledge are part of the cognitive domain. The psychomotor domain includes a variety of physical tasks, such as manipulating objects. Each domain is organized in a hierarchical order to reinforce the idea that students must have a solid foundation in each area before moving on to the next (Odhabi, 2007, p. 1129).

Figure 9 Domain of Learning (Hoque, 2017)

All these categories, according to the latter, complement each other, but for this research the focus will mainly be on the cognitive part. The cognitive domain includes knowledge, understanding, application, analysis, synthesis, and evaluation. Also known as remembering, understanding, applying, analyzing, evaluating, and creating (see Figure 11). The two sets of terms reflect different groups of Bloom's Taxonomy, with the first set being the originals and the second set being established later as researchers refined the system. A revised version of Bloom's taxonomy was published in 2001. The main difference is that it is argued that thinking is an active process, so the revised version of Bloom's taxonomy uses verbs to replace nouns.

The "Knowledge" level in the original Bloom's taxonomy does not indicate a level of thinking and is therefore replaced by the word "remember". Each stage implies a distinct set of cognitive skills, such as the ability to acquire and commit new information to memory (Mualem et al., 2018, p. 4).

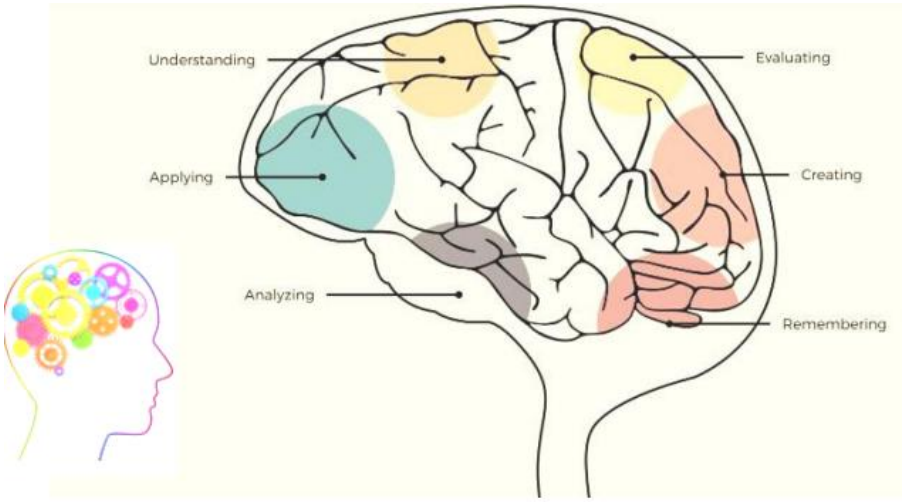


Figure 10 Revised Taxonomy (Krathwohl, 2001)

It is an interesting observation that the mentioned categories (which can be seen in the pyramid) are also active in different parts of the brain. The different activities in the brain can be seen in Figure 10.

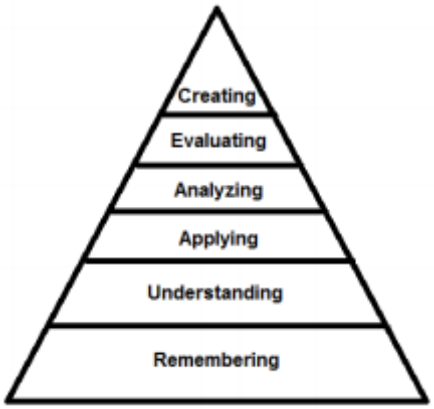


Figure 11 Cognitive Domain Brain Analysis (Hoque, 2017)

The higher the stage, the more complex mental activity is probably needed in the chart shown. Higher levels are not inherently more beneficial than lower levels, since, without the ability to use the lower levels, one cannot reach the higher levels. However, as one goes up to higher levels, the more important the skills are to those needed in everyday life. The cognitive domain involves learning abilities specifically linked to mental (thinking) processes (Hoque, 2017). Six stages of cognitive complexity exist: knowledge, comprehension, application, analysis, synthesis, evaluation. The taxonomy of Bloom focused on defining stages of achievement rather than process skills and did not discuss the way in which the learner proceeds from one stage to the next in a substantial way.

Cognitive ability is important in the concept of “Learning Agility”. Learning Agility means that an employee is agile and resilient. That he or she has the ability to convert new experiences into effective behavior.

An article by Harvard Business Publishing (Amato and Molokhia, 2016) describes what essential Learning Agility is. In addition, Learning Agility has three essential components:

1. **Potential to learn:** An open and responsive mentality is necessary to learn. We also gain knowledge and maturity through years of experience, but we may become myopic in our failure to see alternative, potentially better ways of enhancing processes or even achieving new goals.

2. **Adaptability to learn:** Employees with adaptability to learn consistently focus on the usefulness of their skills rather than merely adopting a business-as-usual schedule. This helps decide whether certain competencies need to be built and new approaches to increase productivity and produce better results need to be found.
3. **Motivation to learn:** It is hard work to change ingrained behaviors and long-held habits. They should stimulate the learning agility of their employees to the degree that companies can make learning more enjoyable.

Given the average level of education of the professionals, the constant updating of the field and the dynamic environment in which the professionals find themselves, the first two components should not be a challenge. The bigger challenge is mainly in how to get a professional motivated to take up the material that he needs to be aware of. Motivation appears to be a key crucial advantage for successfully participating in the learning process, in time and mind: a driven learner cannot be prevented. Enthusiastic, concentrated and engaged are inspired learners. Motivation also contributes to the activation of appropriate cognitive techniques for long-term memory disorders, such as knowledge monitoring, elaboration and organization. In video games, for instance, motivation is successful because it deals more with entertainment, a powerful source of intrinsic motivation, whereas conventional education frequently fails to include the fun element and is often out of context as well. Research shows that when the content is presented in imagined ways that are of interest rather than in a standardized decontextualized form, learning is more successful (Hagen et al., 2011, p. 152).

Changing behavior

The Triade model (Poiesz, 1999) can also be used to predict (route choice) behavior. This behavioral theory states that motivation, capacity and opportunity must all be present at a certain threshold value, otherwise behavior will not take place. The variables are explained in more detail:

- **Motivation** refers to a person's interest in (the outcome of) a particular behavior.
    - o Knowledge;
    - o Consciousness;
    - o Skills.

- **Capacity** refers to how well an individual possesses the necessary characteristics, strength, expertise, and tools to carry out the behavior.
    - Intrinsic;
    - Extrinsic;
    - Self-efficacy;
    - Self-determination.

- **Opportunity** refers to the degree to which time and conditions allow for the behavior to take place.
    - Context;
    - Culture.

In the next section, more insight will be provided on human behavior in relation to cyber security awareness.

3.3 Human behavior on cyber security awareness

The first paragraphs in this chapter showed that technology alone can never prevent all mistakes, humans are also an important link. Human behavior is unconsciously trapped in habits. The social context also plays a role. Examining how effective each cyber security awareness activity and why people do what they do (or not) will help in policy making. Human behavior is riddled with thinking errors and blind spots. Interventions that increase cyber security by targeting it are an important part of effective cyber policy. An essential starting point is imparting knowledge about cyber threats and security and training the necessary skills to apply this knowledge. Training employees also increases the resilience of the organization. This includes dealing with phishing mail, increasing alertness to suspicious situations, and optimizing knowledge of cyber threats and vulnerabilities within the organization.

To better understand the impact of human behavior on cyber security protection, a model has been developed by Li et al. several. The research contains a conceptual model that shows which factors influence cyber security behavior. Figure 12 shows this model. The model shows seven protection motivation factors. These hygiene factors can be taken into account when setting up a policy.

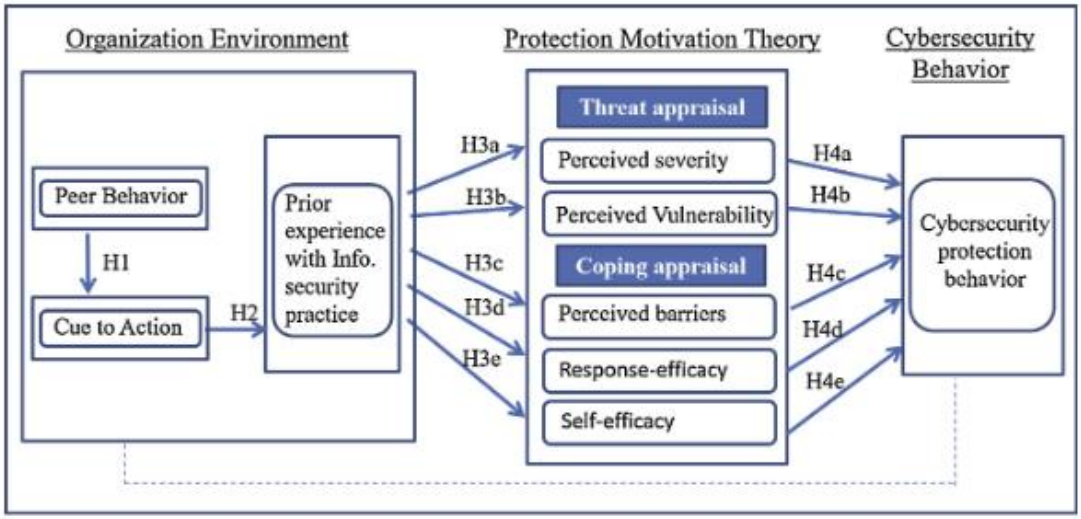


Figure 12 Conceptual model (Li et al., 2019)

This model contains three components:

- Organization environment;
- Protection motivation theory;
- Cyber security behavior.

For this research, we attended the webinar “Psychology, attitude and behavior for security” given by the PvIB platform (Wetzer & Broersma, 2021). It is suggested that the first step to behavioral change is defining the specific desired behavior. For example, wear a mandatory badge, report incidents or lock the PC. An employee often wants to adhere this desired behavior; however, this is not possible due to a barrier (comparable to the hygiene factor in the conceptual model). By examining the three prior mentioned variables of an employee that can be used to predict a particular behavior, a barrier can be removed. A common mistake is to make assumption(s) as to why an employee does not display the desired behavior. It is therefore important to investigate this further.

According to Li et al. (2019), creating an information security policy in an organization and making employees aware of the policy has a positive impact on employees' beliefs about information security and their information security protection behavior. If policy positively contributes to employee's beliefs about information security and their information security protection behavior. Then why do the professionals fail to change behavior?

One reason for failing behavior among employees is that some organizations continue to view training as merely a compliance requirement, an activity to pursue to check the box. They do not truly value training as an opportunity to educate users on how they could help strengthen the enterprise security posture through understanding and following security controls and adopting best practices. As a result, these organizations generally do not invest much in developing robust programs that could make a difference (Pratt, 2021).

However, even organizations that do value training as a way to improve enterprise security often find their programs are not as strong as they would like. The simple transfer of knowledge regarding effective cyber security practices is far from enough. Correctly answering questions does not mean that the individual is motivated to act according to the information learned during a cyber security awareness program (Wilson & Hash, 2003). The assumption that employees change their behavior by following an e-learning is already a possible reason why behaviors fail within organizations. Knowledge and awareness are a prerequisite but not inherently necessary to improve behavior, and therefore it must be applied in combination with other methods of control.

It is important that constructive cyber security habits are implemented, which can lead to thought becoming a habit and a part of the cyber security culture of a company (Bada et al., 2015). In addition to this, Nachin (2019) also describes in his article that training may not be sufficient for organizations to deal with cyber security threats and attacks. It is important that it is close to the employee's perception. For example, Nachin indicates that it is important that the content of a training is relevant and should fit the perception of a person. For example, attention should be paid to Whaling Phishing at a CEO and social engineering at a receptionist. The goal for a CISO is to ensure that employees correctly implement information security practices as they fully understand and agree with the way things are done in the organization and their behavior is second nature to them.

Culture extends beyond awareness. The secure culture of an organization must be recognized by looking at the overall culture(s), methods and policies within the organization in order to create a secure culture. It is undeniably important to have a shared understanding between senior management, cyber security experts and staff with positions and responsibilities relevant to defending cybercrime. While senior management sets the tone, it is important to shape a secure culture with employees rather than force it on them.

Senior management is merely responsible for investment decisions, and for modeling the responsibilities related to secure culture within the organization.

On the other hand, forming and implementation is an organization-wide task. The various stages of achieving a secure culture are threefold. In order to build awareness and a positive attitude towards cyber security in general, it is important to first establish a feeling of secure culture, as illustrated in Figure 13. Employee knowledge of the significance of cyber security is promoted through exchanging user accounts of data breaches and securing confidential data. Specialized secure culture programs should be developed in addition to regular security awareness training, taking into account new developments in the field of secure culture (Building a Human Firewall, 2021). Finally, the information would stay present in their minds by engaging employees.

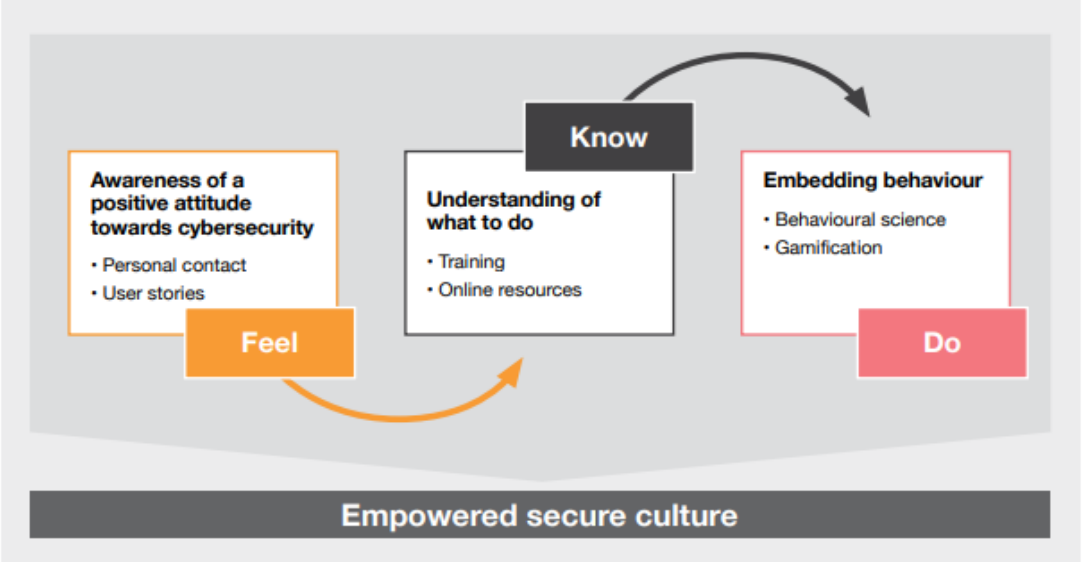


Figure 13 Stages of achieving an embedded cyber security culture (Building a Human Firewall, 2021)

The result of these three steps is an empowered secure culture. The interventions, when tailored to organizational needs and properly implemented, allow secure culture to become part of the corporate culture within organizations instead of achieving cyber security awareness (Building a Human Firewall, 2021).

In increasing the efficacy of current and future campaigns, the following can be helpful (Bada et al., 2015, pp. 218):

1. Awareness raising on cyber security can only work if it is professionally organized and coordinated.
2. It is not a successful tactic to evoke fear in individuals, because it may scare people who can least afford to take risks.
3. Cyber security education must be more than providing users with information; it must be focused, actionable, feasible and provide feedback.
4. Once individuals are ready to change, preparation and continuous input are required to support them through the time of change.
5. When designing cyber security awareness campaigns, focus is required on different cultural contexts and features.

A secure culture transformation is complex and requires a change in values and beliefs, an alteration in behavior, and a reshaping of the underlying assumptions regarding cyber security. Cyber security awareness program should use simple, consistent behavioral rules that individuals will obey. This means deploying effective activities that contribute to people's awareness of cyber security. This study identifies what is needed to make someone sufficiently aware and what other factors are needed to make this a success.

4. Results

In this chapter, the findings of the interviews and survey are described after applying the methods that have been discussed previously. First, the results of the interviews are discussed, providing more context to the problem and the questions. The survey provides direct input in points weight for the model. Finally, the data collected through various methods will be combined to create a model that will be described in chapter 5 (Feldman et al., 2018).

4.1 Interviews

Chapter 3.5 describes the design of the interview. The interview protocol can be found in Appendix l. The thematic analysis method was used to understand and analyze the transcript. Various themes have emerged from this method. These will be discussed in the next subsection.

Results of thematic analysis

The coding process started with the so-called “open coding”. For this, the transcribed interview is read through and labels (codes) are attached to text fragments. These codes indicate per fragment what the main theme is. This is done for all interviews.

The next step is “axial coding”. In axial coding the assigned codes are compared with each other and codes that belong together are combined within a common code.

To avoid the chance of traceability to the participant or organization, only the axial codes and selective codes will be shown in Appendix II.

Cyber security awareness

Cyber security awareness was defined in different ways by the interviewees. However, it can be concluded that the traditional approach, earlier discussed in the research by Bada et al. (2015), of simply churning out a few campaigns or events and training does not necessarily achieve the desired impact. The goal of awareness is not to create awareness. The goal of awareness programs is ultimately to change human behavior. That is why the interviews clearly showed that cyber security awareness consist of two aspects: enhancing cyber security awareness and changing behavior.

'The goal of awareness is not to create awareness.
The goal of awareness programs is ultimately to change human behavior.'

L. Spitzner

The first domain "cyber security awareness" is generally extended to mean that entire body of activities designed to a mindset and behavior change with respect to security, and in this case cyber security. According to ASML's Security Awareness Manager, any initiative to change behavior will best succeed with the right leadership sponsorship, integration with an organization-wide initiative, awareness education, insights into drivers of behavior, investment into technology that facilitates the right behaviors, consistent messaging and metrics.

Importance of cyber security awareness

According to Lance Spitzner and Chris Roberts, one of the biggest drivers of risk is the human side. Robotization and automation in the workplace have ensured that technology has played an increasingly important role in business operations. This development is good for time and cost savings and has made work easier, but this means that organizations are also vulnerable to cybercrime.

Cyber security awareness is therefore the most critical part of cyber security for the interviewees. For example, the CISO of IKEA stated that the other components within cyber security are measurable, but that this is more difficult to apply to cyber security awareness. 'We have a beautiful dashboard. We have all kinds of algorithms running, but in the end, employees is one of the most critical success factors for a safe environment' said the CISO of the Swedish furniture giant.

Unfamiliarity, ignorance or underestimation of the risk of a security breach can be almost deadly to an organization. For a commercial organization this can lead to reputation damage or loss of money. For a health care system or other critical infrastructure, this can lead to deaths. The prominent hacker Chris Roberts said in an interview for this thesis that the dependence we humans have on IT poses a serious threat to the survival of organizations and can even cost human lives. Chris estimates that this threat will only increase. It is the actions that mainly make an impact in combating human error.

Cyber security awareness is often an addition to all the other duties of the person responsible for managing and coordinating cyber security awareness activities. According to Lance Spitzner, cyber security awareness is still too much seen as a part-time job. Therefore, the biggest challenge is that people underestimate the importance of cyber security awareness with the result that they are not dedicating the resources to it.

Since technology is not able to prevent all attacks from touching end users, it is extremely important for organizations to train humans how to react and to build muscle memory. Training can be done through various activities. The findings on the activities during the interviews are discussed in the next section.

Cyber security awareness activity

The interviews revealed that the experts did not identify an activity that they consider to be the most effective. According to Lance Spitzner, it is by definition the combination of activities, but there are activities that stand out a bit more. One need to have a comprehensive type of activities and different type of activities, depending on who is one's audience in order to be efficient.

In addition to determining who one's audience is when setting up a cyber security awareness activity, it is also important to describe what the goal is. Is the goal to change people or just to increase the knowledge level of the employees? One aspect that one has to take into account when increasing the knowledge level is the relevance for the employee, that they feel addressed and that it is relevant to what they do in their work. Therefore, it is important to not ram all (irrelevant) knowledge to employees. It is also important that one keeps repeating the message and preferably in the same message in a different form. Several interviewees have noticed in their own experience that an activity can be effective in the first year, but when it is repeated in the same form, the engagement drops and therefore also the essence of the activity.

The most controversial cyber security awareness activity was e-learning. The interviewees were skeptical about this but the value is seen in this activity because it is scalable. According to Chris Roberts, an e-learning quickly becomes ineffective when one has to sit through the video, but it cannot be ignored, because every three minutes there have to be an answer on a question. It gets worse when the video is made mandatory every year. That

is why it is important that the e-learning should be interactive and fun. In addition, it is also important that it is specific to the targeted audience. The professional must feel addressed.

Noticed during the interviews, phishing simulations are widely used within companies. Virtually all CISOs agree that phishing simulations do have added value. The added value is mainly in the scalability and measurability of the activity. Direct awareness is also created with the person concerned, because this comes close to the professional's perception of the world. Extra attention can also be given with additional cyber security awareness activities. The culture of the organization is important. There must be room for the professionals to make mistakes. If the culture is not included in the context when considering the phishing simulation, this could possibly lead to a shame culture.

The central information source activities are used within organizations but are not considered effective. According to the CISO of Loyens & Loeff, these channels should preferably be used to share the lessons one have learned from incidents from that organization.

The interviewees were positive about the gamification and interactive workshops activities. According to Chris Roberts, entering a reward element can work effectively for this activity. A reward element is important for engagement and fun. On the other hand, it is important an organization does not take this too far as this eventually becomes too complex. It is possible to have too much of a good thing.

The findings about the cyber security awareness activities are in line with what is described in the literature in chapter 3.2. It is insufficient to implement cyber security awareness activities within the organization without taking organizational practice into account. This will be discussed in the next section.

Organizational practice

When it comes to cyber security awareness within organizations, compliance attitude is still too frequent. An example of this is that it is made clear by visionaries that any initiatives that are purely compliance driven, tick box activities do not help the organization reach its cyber security awareness goals.

The definition of a compliance attitude is that information is given (in this case often in the form of an e-learning course) but the adoption of good behavior is insufficiently measured and, as described earlier, the ultimate goal is for cyber security awareness to change behavior. This is where capability should be developed. It was noted from the interviews that many CISOs are hiring external professionals to map out and improve behavior.

“Compliance is important, but protecting an organization requires much more. According to Ahold Delhaize's CISO, a key part of a successful program is about building a resilient human firewall that makes our associates continuously aware of the critical cyber security risks that we face and how their behavior can impact the organization.”

‘Just because people are aware, does not mean they care’.

Perry Carpenter

People need to be educated, that they know what to do, what is required, that one cannot just email anything, that an employee cannot just start any chat program. So, it is important to put energy into learning to make people aware of the threats. It is not only important to create awareness, but also to see if we can change that behavior. because that people are aware, does not mean they care. We see the three elements that were mentioned earlier in the literature among the interviewees. Learning behavior is difficult but should be positively influenced by the factors of the Triade model. Motivation is important in behavior to want to do things safely. However, it is also about learning and that people know what the right behavior is. Professionals must also have the ability to have the right thoughts and work the right way. So, it affects various aspects.

When showing the wrong behavior it is important that this does not happen again, but also how an employee should react when one sees something and who the employee should reach. That is why it is important to explicitly describe the desired behavior. Even more ideal is that cyber security can bring it into the daily situation and talk to people about it. As an example, people are not afraid to name a suspicious situation. An effective relationship between the cyber security department and the employees is important, but are rather enthusiastic to call the cyber security department every now and then. It is a behavioral change program or perhaps even a little further, a culture change program.

According to the interviewees, the cyber security awareness culture is not a culture in itself. The cyber security awareness culture must complement the existing culture of the organization. This is in line with the literature described in chapter 3.4. Different maturity models should help with this and describe the various indices of a mature security culture. It is especially important that cyber security is recognized by employees. The recognition could be through a logo, mascot or ambassadorship to get the attention. The trick is to make it fun and approachable enough that people would tell others and they would want to join, because there is a lot of word-of-mouth when one think about awareness. So, it needs to grow on its own.

This way the company ensure that everyone gets involved and engaged, and the other part of it is as well is the cyber security department has a role to help a company understand. The cyber security department should not act like a police officer. Employees should be confronted with this in a positive way. It is important to not name and shame because the cyber security department want people to be free to report that they have clicked. The approach also differs per continent. An international organization that operates in different parts of the world must take cultural differences into account when setting up a cyber security awareness program. Within the culture, physical security is also an important aspect of cyber security awareness. Indicators of a good awareness culture is when a person physically step into an organization, that the person can already see that people handle their physical environment safely. Examples of a safe work environment are registration for visitors, the mandatory wearing of an employee badge, etc. that do not have sensitive information. It is also important that it is alive and that people address each other about it.

The trick is to keep it at the right level and remain steadfast in it. And that's leadership. In the next section, several important factors are identified for an effective organizational practice.

Important factors for cyber security awareness

The following important factors have been identified for an effective organizational practice:

1. Involvement from executive board;
2. Target audience;
3. Relevance;
4. Technical aspect and cyber security;

5. Incident reporting;
6. Hacking threats.

1. Involvement from executive board

Getting the executive board on board was seen as the biggest obstacle when it comes to the journey to an effective cyber security awareness culture. It is therefore important that executives see the importance of cyber security threats. The CISOs of the multinationals have experienced when there is no awareness in the executive board, that the sense of urgency is not present among those administrators. Because if it is not simultaneously stimulated from above (executives), promoted or fine-tuned, then the professional responsible for cyber security awareness has a problem, because then one remain a lone voice in the wilderness.

Realistically, top management must find it important and that starts with the CISO. There are CISOs who are mainly technically oriented and therefore simply believe in technical migratory measures.

2. Target audience

There is no one size fits all for different reasons according to the CISO of Ahold Delhaize. First, because not everybody has the same top three risks. A distribution center with mechanization is going to have different top risks compared to someone sitting at the corporate headquarters. Awareness must fit the role that the professional has and that is why organizations should work more with target groups according to the CISO of Eneco. In this way it is possible to focus better on what is relevant to the employee. It will also important how the target group can be approached.

3. Relevance

The CISOs of Schiphol Group and AkzoNobel said in an interview that the relevance of the content is important to an employee. The employee must be able to identify with the threats. So, the more one can bring it to the perception of the target audience, the more effective it is. The CISO of Schiphol emphasized in the interview: 'Make sure it is practicable and that people recognize the threats'. The further away the professional is, it can still be fairly effective, but it sometimes remains incomprehensible to some, because they do not recognize the organization imagery and do not recognize the given examples. It is far from the professional his or her world.

4. *Technical aspect*

There are times when organizations need to invest into the right technology and also have the right change management strategies to support the implementation of these solutions, to ensure that they work in the desired way. An undesirable situation is that the technological interventions get in the way of the user. For example, the title of an email cannot be read in the message center because it says "warning, this is an external email". A technical intervention should not be seen as an obstacle. These obstacles can be prevented by designing the technological interventions also from a user perspective.

Technical aspect and cyber security awareness go hand in hand. They strengthen each other enormously was told by Philips' head of operational excellence. But when this is done badly, one makes the other worse. Ideally, according to the NSO of Microsoft and Mrs. van der Beijl would be to apply technological measures at the front door, so that phishing e-mails do not have the chance to reach the target group.

In short, nudges, prompts and actual technological interventions are essential to influencing security behaviors, as long as it does not get in the way of the end user.

5. *Incident reporting*

The findings show that incident reporting is an important aspect of cyber security awareness because this is the first line of defense. When no incident reports are made, it does not mean that the cyber security department is doing it right. An organization should focus on the incident reporting, there should be an increase in the number of incidents. It is important that professionals are able to reach out to the right stakeholders when they see something suspicious. According to the CISO of IKEA and Ahold Delhaize, an indicator of an effective cyber security risk awareness culture is that professionals are comfortable to report an incident.

It is the cyber security department's job to evaluate and facilitate cyber security awareness processes for professionals. According to Microsoft's NSO, it would be even nicer if feedback could be given on the incident report, stating whether the reporter is right or not. The intention with this is to motivate the employee to continue reporting.

'If you see something, say something and as a security team:
be ready to listen and act.'

National Security Officer at Microsoft

6. Hacking threats

Another important factor to take into account are the cyber security threats. For example, the interviewees were asked which cyber security threat people should be aware of. The following findings emerged from this.

According to Lance Spitzner, the human element is the primary attack vector. And the reason they are the primary attack vector is it is hard to hack technology. And because we have done little with people, it is much easier to hack the human OS. The top three risks human related is phishing, passwords and simple human error. The biggest risk at the moment within the end users is that the criminals are using the same channels that the company often uses. That can look similar to the real purpose that people can hardly see the difference anymore.

Chris Roberts sees that the balance between work and private life is becoming increasingly thin. The threat is that there is no border between the digital professional world and digital personal world. By sharing our lives on social media, we set ourselves targets for both personal and work.

4.2 Survey

For this study, a survey was conducted with 65 respondents within the PwC Risk Assurance department. This survey was used as a qualitative method to flesh out the model discussed in chapter five. The questions and the interface of the survey can be seen in appendix lll.

The respondents

Before sharing the findings of the survey, it is important to describe the background of the respondents. The survey was conducted within the Risk Assurance department at PwC. The department consists of educated professionals, working as IT auditor or consultant. These facts were not collected during the survey. An email has been sent to the department with an invitation link for the survey. The composition of the group is a good reflection of the department, with the largest group consisting of senior associates. The composition could be seen in Figure 14.

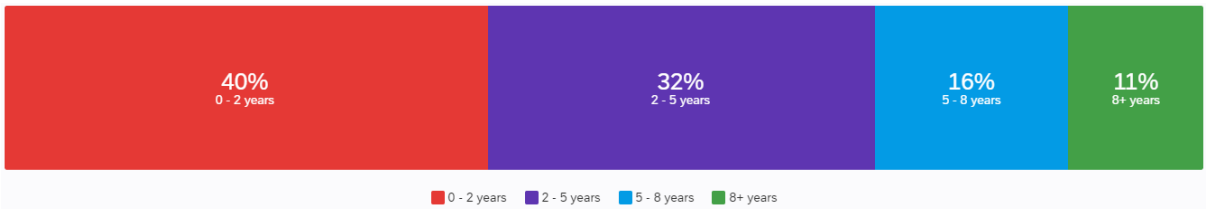


Figure 14 The division of the respondents from the Risk Assurance discipline at PwC

From this group composition, 40% work less than two years at PwC, while 27% have worked at PwC for more than 5 years. The composition is illustrated in Figure 15.

Figure 15 The division of how long someone has been employed within the Risk Assurance discipline at PwC

Effectiveness per activity

For sub-question three: "How much do these activities contribute to the cyber security awareness of a person?" The following questions were asked to the respondent:

- How effective do you think the following activities would be in contributing to your cyber security awareness?
- Which cyber security awareness activity do you consider to be the most effective (shift it yourself, where 1 being the best)?

The first question serves as validation for the second question. The findings for the first question could be seen in Figure 16. From this figure it becomes evident that the participants of the cyber security awareness program, also referred to as users in this thesis, consider interactive workshops, gamification and phishing simulation to be effective.

In the interviews, e-learning was seen as the most controversial activity that could be used. For example, Figure 16 illustrates that e-learning is considered to be the least effective method of enhancing cyber security awareness. As well, central information sources are considered to be ineffective because few people read these messages.

#	Field	1	2	3	4	5	6	7	8
1	Interactive workshop	21	21	12	5	4	1	0	0
2	E-learning	1	2	5	15	10	9	12	10
3	Gamification	20	22	8	3	7	1	2	1
4	Phishing Simulation	12	9	15	9	7	7	3	2
5	Classroom training by a teacher	2	5	8	12	12	13	8	4
6	Cyber Security Awareness month	6	3	5	6	10	14	10	10
7	Central Information Source	0	0	3	7	3	11	16	24
8	Keynote by an expert speaker	2	2	8	7	11	8	13	13

Figure 16 The effectiveness per cyber security awareness activity

In addition to the above, the central tendency per individual activity is shown. Table 3 shows this activity and the ratio of the average to each other.

Table 3: The central tendencies for each individual activity based on figure 18

Activity	Mean[1]
Interactive workshop	2,3
Gamification	2,6
Phishing simulation	3,5
E-learning	4,3
Classroom training by a teacher	4,8
Cyber security awareness month	5,2
Keynote by an expert speaker	5,6
Central information source	6,6

[1] *On a scale of 1 to 8, with 1 being the most effective*

In the second question, the respondent was able to shift himself, as this time the respondent had to make a trade-off between the effectiveness per activity. Comparing Figures 16 and 17 shows similar results, in which we see that interactive workshops, subsequent gamification and phishing simulation are among the most effective according to the user. On the other hand, keynote by an expert speaker, e-learning and cyber security awareness month are among the least effective.

#	Field	Not effective at all	Slightly effective	Moderately effective	Very effective	Extremely effective
1	Interactive workshop	0	6	10	38	10
2	E-learning	3	28	26	7	0
3	Gamification	0	2	7	35	20
4	Phishing Simulation	1	6	10	30	17
5	Classroom training by a teacher	2	13	25	19	5
6	Cyber Security Awareness month	6	14	21	18	5
7	Central Information Source	8	22	20	13	1
8	Keynote by an expert speaker	6	13	19	21	5

Figure 17 The tradeoffs between the most effective of cyber security awareness activities

The effectiveness per cyber security awareness activity will be visualized in the figures below.

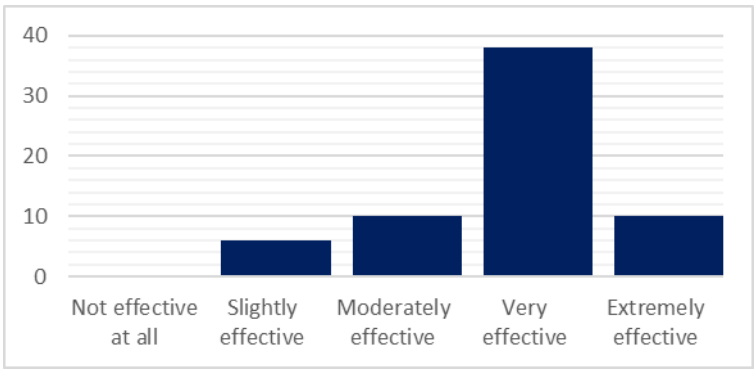


Figure 18 The effectiveness of interactive workshop

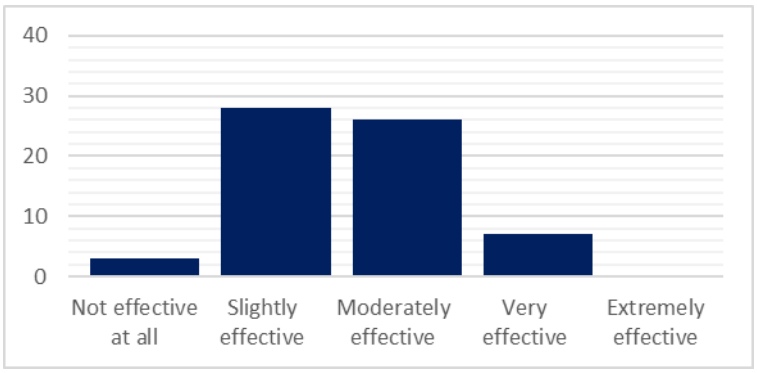


Figure 19 The effectiveness of e-learning

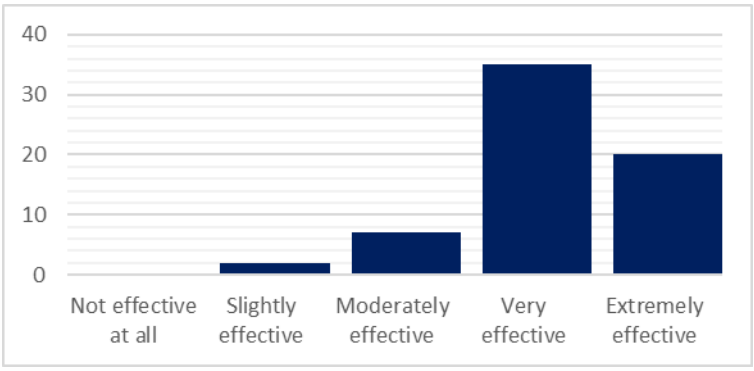


Figure 20 The effectiveness of gamification

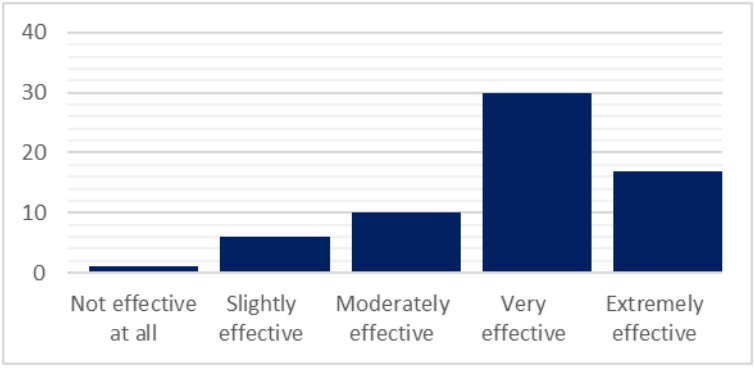


Figure 21 The effectiveness of phishing simulation

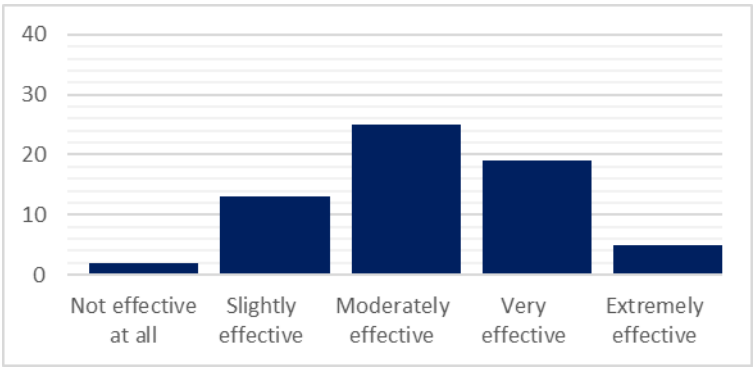


Figure 22 The effectiveness of classroom training by a teacher

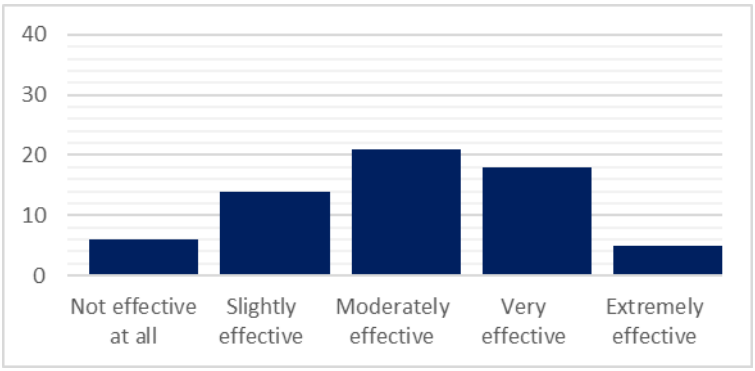


Figure 23 The effectiveness of cyber security awareness month

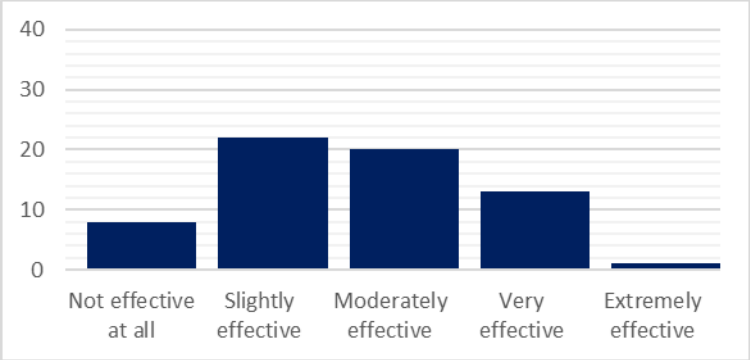


Figure 24 The effectiveness of central information source

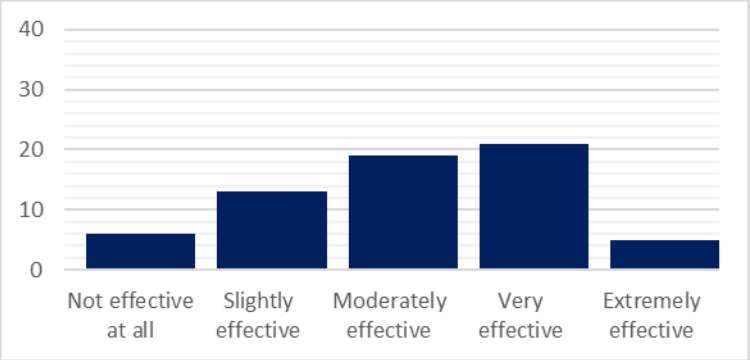


Figure 25 The effectiveness of keynote by an expert speaker

In addition, the central tendency for each individual activity is displayed. Table 4 shows this activity as well as the average to average ratio.

Table 4: The central tendencies for each individual activity based on figure 18

Activity	Mean[1]
Gamification	4,1
Phishing simulation	3,9
Interactive workshop	3,8
Classroom training by a teacher	3,2
Keynote by an expert speaker	3,1
Cyber security awareness month	3,0
Central information source	2,6
E-learning	2,6

[1] *On a scale of 1 to 5, with 5 being the most effective*

When table 3 and table 4 are compared, we see a lot of comparisons when it comes to ranking the activities. we see the same top 3 activities when it comes to the central tendency for each individual activity. Table 4 confirms what table 3 shows. However, the e-learning activity is noteworthy, which ranks fourth in the average in table 3 and has the lowest average in table 4. A direct explanation for this can be taken from section 4.1, namely that e-learning is scalable for a larger audience.

The sufficient level of cyber security awareness

For sub-question four: “What level of cyber security awareness is deemed “sufficient”?” The following question were asked to the respondent:

- What combination of activities (or singular activity) is necessary to create sufficient awareness in the field of cyber security for a new employee over a period of 12 months?

The data in Figure 26 indicate that the activity interactive workshop is seen as the most important activity to create sufficient awareness. Gamification then follows. These findings are in line with the previous findings from the previous questions and the interviews. Both defenders and users agree that e-learning is necessary to create sufficient awareness for a new employee, despite its slightly effectiveness.

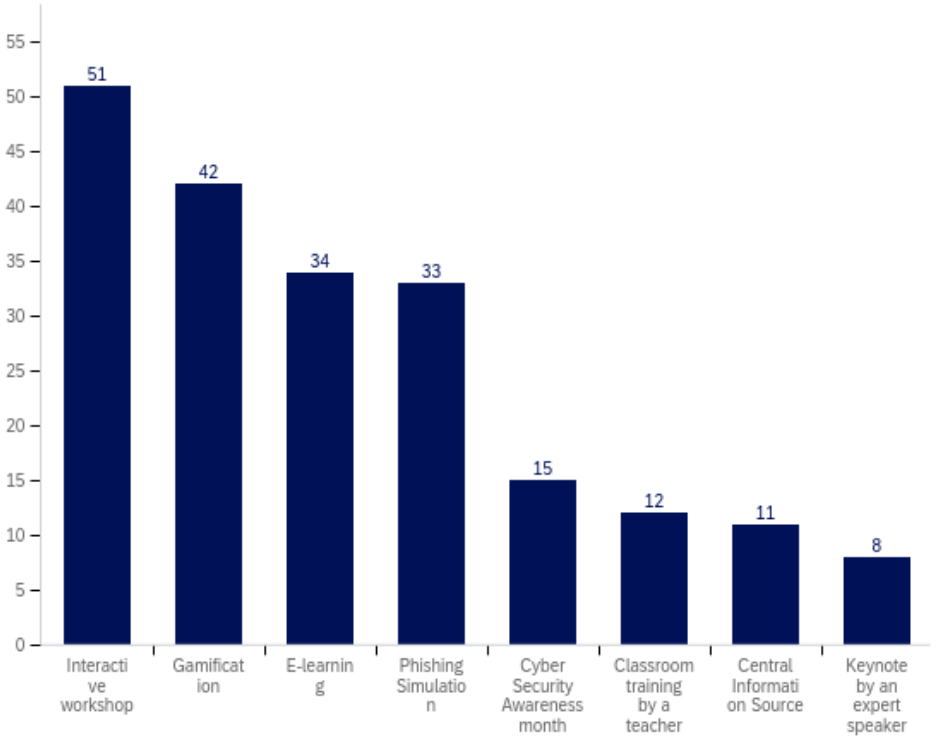


Figure 26 Sufficient level of cyber security awareness per cyber security awareness activity

A remarkable insight into the data is that the majority (52%) of our respondents recommended an effective combination consisting of a minimum of 2 activities, namely: interactive workshop and gamification. In addition, 80% of the respondents recommended the interactive workshop for a combination of multiple cyber security awareness activities, meaning this is to be the base to which other activities can be supplemented.

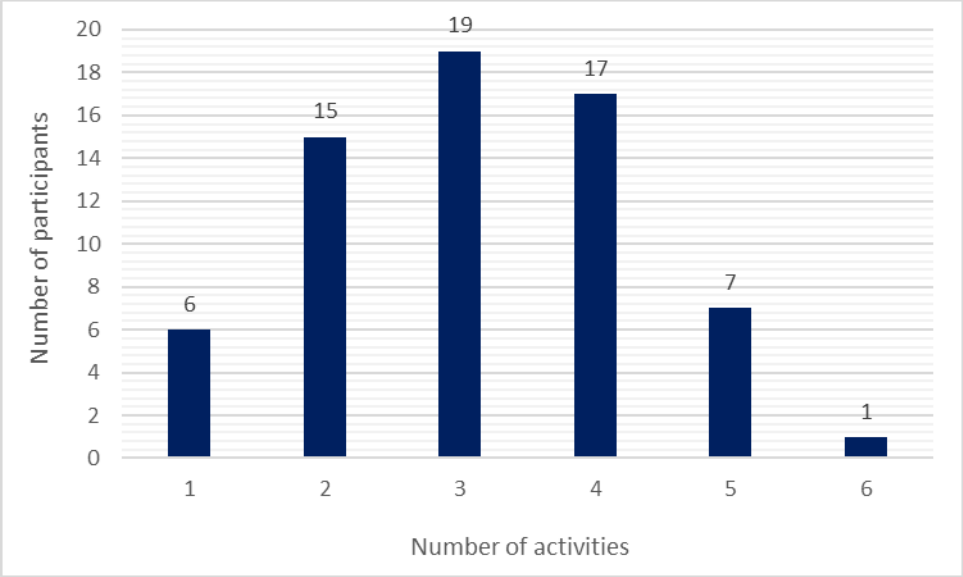


Figure 27 Number of activities recommended by participants

Figure 27 is showing how many activities have been recommended by participants to create awareness. For example, 6 participants recommended 1 activity, 15 participants recommended 2 activities, etc.). From this data, it can be read that the majority believes that more than one activity is needed to create awareness.

The answers of the respondents are ultimately used as input for the model. The model will be illustrated in the next chapter.

5. The model

For sub-question five: “What combinations are possible to achieve a solid result for sufficient cyber security awareness?” a model was created as illustrated by Fig. 28. The survey was used as input for both: the number of points per activity and what is needed to be sufficiently aware of cyber security risks. Each activity has its own weight. In total there are 140 points needed to be sufficiently categorized as a cyber security risk. Based on the context and budget, the defender could determine for himself which activity best suits the organization, as long as it exceeds 140 points. The realization of the model can be found in appendix IV under model statement calculation. The assumptions regarding the process will be discussed later on.

	Number of points per activity	Choose activities (min. 140 points)*
Interactive workshop	56	
Gamification	54	
Phishing simulation	48	
Clasroom training by a teacher	39	
Cyber Security Awareness month	37	
E-learning	36	
Keynote by an expert speaker	35	
Central information source	28	
Total points		

**Ultimately, 140 points are needed to be sufficiently aware of cyber security risks*

Figure 28 The effective cyber security awareness model

Findings of the interviews has shown that effective cyber security awareness activities will be driven by the organization's culture, what they are trying to achieve and who is running the program. If one is just starting with the absolute fundamental basics, one is going to start with more basic training, computer-based training, lunch and learns, things like that for more mature programs and or outgoing cultures. Once this is in place, gamification and phishing simulations could be implemented.

5.1 Important factors

Also for sub-question six: “Which factors influence the success of implemented cyber security awareness activities?” a model was created as illustrated by Figure 29. There are four factors that have a major influence on the success of the activities. The factors most frequently identified among the interviewees have been chosen as the top four factors to consider when setting up the model within the organization.

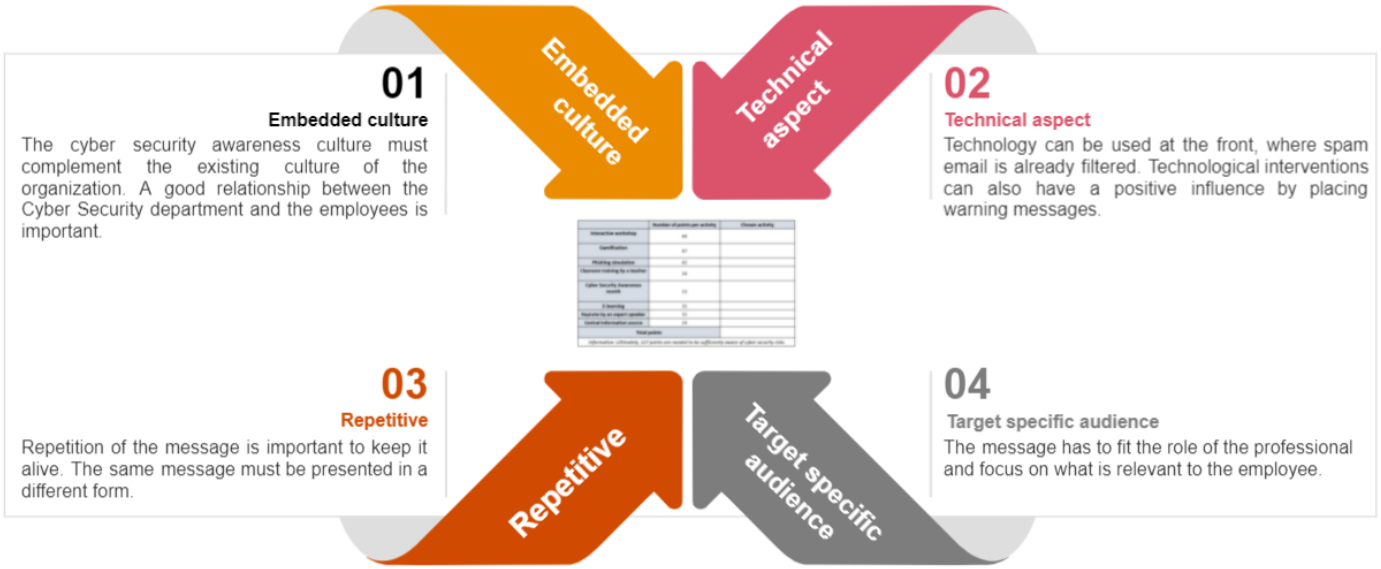


Figure 29 Important factors affecting the model

1. Embedded culture

The embedded culture aspect illustrates that it is not so much about the activity, it is rather about the engagement. A computer-based training could be extremely effective if it is well designed and engaging. If it focusses on people their need, relevance and on how people should benefit. On the other hand, one could have an interesting interactive escape room. However, if the engagement is confusing and it is boring or if it is teaching the wrong behaviors. Ultimately, the purpose of a cyber security awareness program is to change behavior. Therefore, even though the interactive game is effective, when one learns the wrong behavior, then one is wasting everyone's time. An indicator of an efficient cyber security risk awareness culture is that professionals are comfortable to report an incident.

A detailed explanation of how to create an embedded culture can be found in section 4.1 under organizational practice.

2. Technical aspect

The technical aspect is important. It strengthens each other enormously. Technical aspect and cyber security awareness go hand in hand. Technology can be used upfront, where unwanted e-mails are already filtered. Nonetheless, technological interventions can also have a positive influence by placing warning messages when a professional receives an external e-mail. Nudges, prompts and actual technological interventions are essential to influencing security behaviors, as long as it does not get in the way of the end-user.

3. Repetitive

It is important that the consciousness does not subside. Repetition of the message is important to keep it alive. It should be taken into account that the same message is always presented in a different form.

4. Target specific audience

There is no one size fits all for different reasons. First, because not everybody has the same top three risks. Getting a message out to everyone is therefore not effective. The cyber security awareness activity which comes close to the perception and the work of the professional is the most effective cyber security awareness activity. Therefore, the more one should bring it to the perception of the target audience, the more effective will be. The further away the professional is, it can still be fairly effective, but it sometimes remains incomprehensible to some, because they do not recognize the organization imagery and do not recognize the given examples. It is far from the professional his or her world.

6. Discussion

This chapter discusses the main findings of the Results presented in Chapter 6 and the research limitations.

6.1 Results discussion

While previous related research focused more on cyber security awareness, this research has focused on the needed activities to enhance cyber security awareness. The results that have emerged are in line with previous related research. Particularly in the field of cyber security awareness activities, where gamification and interactive workshop are popular. But it was also reflected in the literature that culture also plays an important role in the success of cyber security awareness. Overall, the bottom line is that cyber security awareness is difficult to manage, as there are various factors such as engagement, embedded culture, the right activities, etc. that play a role in a successful cyber security awareness program. In comparison with previous related research van Pratt (2021), we see that interviewees are awakened from a compliance attitude, while professionals are taking this topic more seriously. This is reflected through enhanced budgets aimed at cyber security awareness and the hiring of external professionals to map out and improve behavior.

We noticed the following while conducting this research. The approach of the professional that is the most responsible for cyber security awareness differs enormously. This approach stems from a perception that is influenced by experience, background, and the definition assigned to the subject. For example, when the defender is not technically oriented, he or she focuses more on e-learning cyber security awareness activities. When the defender is technically oriented, he or she focuses more on the technical possibilities within cyber security awareness. The number of factors: target audience of the organization, culture, broadest sense of the definition, etc. indicate that cyber security awareness takes time and a lot of collaborative effort is necessary in order to be successful. These factors and their interrelationship can become a focus of future research.

Due to the approach of the data collection method for interviewees, everything went as planned. Due to the use of theoretical saturation, no new findings have emerged on the subject in the last three interviews. The distinction between the CISO and Visionary categories and the number have provided a complete picture.

Furthermore, 65 respondents from a department completed the survey. A larger number of respondents from different industries would provide a better picture of the user side. To ensure consistency of replies, we decided to focus on a single department in a single (but large) organization. In this way, we can expect that the respondents have similar experiences with the considered cyber security awareness activities.

Apart from the scientific research, we looked at how this research could be made practical for businesses. This is the reason a model is created, that organizations can use for the effective use of the cyber security awareness activities. The model itself has not been validated in practice, so the usefulness of the model is unknown. This can be a focus for future research.

6.2 Limitations

We now discuss key limitations and threats to the validity of this research. A survey is always subject to a degree of subjectivity, which means that random biases can never be totally eliminated. They can, however, be controlled. It is also possible that there is a small sample size bias, since a small sample is taken and analyzed. Another limitation or threat is referral bias because these people often differ from people who were not referred to the survey (Krishna, Maithreyi, & Surapaneni, 2010). The reader should take into account that the survey is based on respondents working within PwC's Risk Assurance discipline. This gives an incomplete and limited picture from the user side. When filling in the survey, respondents who work in different industries could provide a more complete picture of the situation from the so-called user side.

Furthermore, because survey question three was on a 5-point Likert scale, there could be a central tendency bias, as most items were placed in the middle of the scale to avoid extremes (Statistics How To, 2016). No measures have been taken in this regard because question three was as support for question four. The details of this confirmation can be found in section 4.2.

For the interviews, professionals were interviewed who are responsible for (cyber security) awareness on behalf of an organization. However, there is a basic human tendency to show oneself as successful and the best version of oneself, even if this is not true in every setting. This has the potential to have a significant impact on the research (Fisher, 1993). To mitigate

this problem, we tried to design the interview questions in such a way that they do not include an evaluation of one's own success, but are a broader reflection of what works and what does not work in this area.

Further, the study cannot include all cyber security awareness activities. Therefore, the choice was made to include a wide selection of eight cyber security activities that are often used within organizations and are reflected in literature. This means that there are activities which may score better than the current top three. Without further research, we will not find out how effective the underexposed cyber security awareness activities are.

Because of time limitations, the amount of work to be done, and the availability of the professionals questioned, it was decided to not do a second round of interviews, where items may have been double-checked and misconceptions or questions uncovered.

Furthermore, this research was conducted in the Netherlands. The culture and norms play an important role in the development of the model. If this study were performed in another country, the model's activities and associated weights may be different.

Moreover, there is an assumption that on average all users would assign similar weights to the same activity. Furthermore, there is a way to quantify a general level of "awareness" for an average user expressed in the same kind of points as individual activities can be measured. Also, a drawback of this model is that there is no difference noted in how different activities are implemented within the organization: the number of points is always the same.

Lastly, as mentioned earlier, the model itself has not been validated in practice, which implies that it is unclear how useful it is. Therefore, this will be indicated in the next chapter for further research. This research has shown that there is no best activity to increase awareness among employees. Multiple activities are needed to enhance cyber security awareness efficacy. The results of this research, including the model created, enable organizations to quantify the effectiveness of cyber security awareness activities on human behavior.

7. Conclusion

Section 7.1 concludes this research by providing the answers to the research questions. Lastly, section 7.2 provides suggestions for future research to improve the model.

7.1 Conclusion

In this concluding chapter, the research question posed in the first chapter of this study will be revisited and answered comprehensively. The research question that served as the starting point of this project is:

"How can the effectiveness of cyber security awareness activities on human behavior be quantified?"

The goal of awareness programs is ultimately to change human behavior. That is why the interviews indicated that cyber security awareness consists of two aspects consisting of enhancing cyber security awareness and changing behavior. During the research it was determined which activities are relevant. The following cyber security awareness techniques were included in this research: interactive workshop, classroom training by a teacher, phishing simulation, e-learning, keynote by an expert speaker, cyber security awareness month, gamification and central information source.

A survey was used to determine which cyber security awareness activity is considered to be most effective to employees. The answers of the respondents are then used as input for a model. According to the model, 140 points are needed for someone to be sufficiently aware of cyber security risks. Activities should be weighted, where each activity has its own weight of points, in order to meet the set minimum requirement of 140 points.

There are four factors that have a major influence on the success of the activities. These have been determined based on the interviews and literature. These four factors are: creating an embedded culture, technical aspect, repetition and target specific audience.

In comparison to previous related research, we see that defenders awaken from a compliance attitude, while professionals are taking this topic more serious. This is reflected in the freeing up of more budget and the hiring of external professionals to map out and

improve behavior. It was also determined that getting the executive board on board is seen as the biggest obstacle to an effective cyber security awareness culture.

As a final point, the number of factors: target audience of the organization, culture, broadest sense of the definition, etc. indicates that cyber security awareness adoption takes time and collaborative effort to succeed. By using the model and taking into account these important factors, the effectiveness of cyber security awareness activities on human behavior can be quantified.

7.2 Further research

During the writing and execution of this research three points that require further research were identified. These were:

1. Survey extension;
2. Practical implementation;
3. Improvement model.

1. Survey extension

As mentioned earlier, the respondents within a department of one organization provided a one-sided view of the situation from the user side. The survey should be conducted in a larger number with professionals working in different industries, in order to generate different insights.

2. Practical implementation

This study has currently aimed to develop a model. The model itself has not been validated in practice, so the usability of the model is unknown and this can become a focus of future research. It is also possible to evaluate the relationship of this model with existing cyber security awareness maturity models. A question may be: “at which level in an existing maturity model is the use of this research model the most effective?”

3. Improvement of the model

The most frequently used cyber security awareness activities during the writing of this thesis were included in this research. Future work can focus on the further development of the model. The model should be expanded with more cyber security awareness activities, for example with cyber security awareness assessments and red teaming/mystery guests. Finally, the model statement calculation could be revised, whereby a more complex calculation method can be applied.

8. References

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237–248. https://doi.org/10.1080/0144929x.2012.708787

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., & Musa, A. (2018). Understanding Awareness of Cyber Security Threat among IT Employees. *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 188–192. https://doi.org/10.1109/w-ficloud.2018.00036

Amato, M. A., & Molokhia, D. (2016). *How to cultivate learning agility*. Harvard Business Publishing. https://www.harvardbusiness.org/insight/how-to-cultivate-learning-agility/

Anderson, L. W., & Krathwohl, D. R. (2001). *A taxonomy for Learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives.* New York: Addison Wesley Longman.

Auld, A., & Smart, J. (2020). *Why has there been an increase in cyber security incidents during COVID-19?* PwC. https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

Bada, M., Sasse, A., & Nurse, J. (2015, January). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society.

Baird, K., & Munir, R. (2015). The effectiveness of workshop (cooperative learning) based seminars. *Asian Review of Accounting, 23*(3), 293–312. https://doi.org/10.1108/ara-03-2014-0038

Bloom, B. S., Krathwohl, D. R., Engelhart, M. D., Furst, E. J., & Hill, W. H. (1956). *Taxonomy of educational objectives: Handbook I: Cognitive domain*. New York: David McKay.

Bowden, P. (2017, October 18). *Advantages and Disadvantages of Online and Classroom Learning*. Online Learning Success. http://onlinelearningsuccess.org/advantages-and-disadvantages-of-online-and-classroom-learning/

Brown, A. (2017, September 11). *Younger men play video games, but so do a diverse group of other Americans*. Pew Research Center. https://www.pewresearch.org/fact-tank/2017/09/11/younger-men-play-video-games-but-so-do-a-diverse-group-of-other-americans/

Bryman, A. (2016). *Social Research Methods*. Oxford University Press.

Bryman, A., & Bell, E. (2015). *Business Research Methods*. Oxford University Press.

Building a Human Firewall. (2021). PwC. https://www.pwc.nl/nl/assets/documents/pwc-whitepaper-secure-culture.pdf

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*, *16*(3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Chatchalermpun, S., & Daengsi, T. (2021, February). *Improving cybersecurity awareness using phishing attack simulation* (No. 1088). IOP Conference Series. Materials Science and Engineering. https://www.researchgate.net/publication/349703173_Improving_cybersecurity_awareness_using_phishing_attack_simulation

Corbin, J., Strauss, A., Wijngaert, L., & de Wijngaert, L. (2008). *Basics of Qualitative Research*. SAGE Publications.

Feldman, A., Altrichter, H., Posch, P., & Somekh, B. (2018). *Teachers Investigate Their Work*. Routledge.

Fisher, R. J. (1993, September). *Social Desirability Bias and the Validity of Indirect Questioning.* Retrieved from JSTOR: https://www-jstor-org.ezproxy.leidenuniv.nl/stable/2489277

Furlow, C., & Disparte, D. (2019, August 23). *The Best Cybersecurity Investment You Can Make Is Better Training*. Harvard Business Review. https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security*, *19*(3), 140–154. https://doi.org/10.1108/09685221111153537

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hoque, M. (2017). Three Domains of Learning: Cognitive, Affective and Psychomotor. *The Journal of EFL Education and Research*, *2*(2), 45–51. https://www.researchgate.net/publication/330811334_Three_Domains_of_Learning_Cognitive_Affective_and_Psychomotor

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Jones, S. L., Collins, E. I. M., Levordashka, A., Muir, K., & Joinson, A. (2019). What is “Cyber Security”? *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1. https://doi.org/10.1145/3290607.3312786

Krishna, R., Maithreyi, R., & Surapaneni, K. M. (2010, April 5). *Research Bias: A Review For Medical Students.* Retrieved from Citeseerx: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.610.8597&rep=rep1&type=pdf

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mgquba, S. K., & Underwood, P. G. (2016). Enhancing information research and learning skills through e-learning: the case of Monash University Library. *South African Journal of Libraries and Information Science*, *81*(2), 39–45. https://doi.org/10.7553/81-2-1561

Morgan, S. (2021, April 27). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Mualem, R., Leisman, G., Zbedat, Y., Ganem, S., Mualem, O., Amaria, M., Kozle, A., Khayat-Moughrabi, S., & Ornai, A. (2018). The Effect of Movement on Cognitive Performance. *Frontiers in Public Health*, *6*, 1–6. https://doi.org/10.3389/fpubh.2018.00100

Nabe, C. (2020, December 15). *Impact of COVID-19 on Cybersecurity*. Deloitte Switzerland. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Nachin, N. (2019, March 1). *How to Increase Cybersecurity Awareness*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-to-increase-cybersecurity-awareness

NOS. (2021, May 2). *Bol.com maakt 750.000 euro over aan oplichters*. https://nos.nl/artikel/2379078-bol-com-maakt-750-000-euro-over-aan-oplichters

Odhabi, H. (2007). Investigating the impact of laptops on students? learning using Bloom's learning taxonomy. *British Journal of Educational Technology*, *38*(6), 1126–1131. https://doi.org/10.1111/j.1467-8535.2007.00730.x

Poiesz, T. B. C. (1999). *Gedragsmanagement. Waarom mensen zich (niet) gedragen*. Inmerc.

Pratt, M. K. (2021, February 22). *Undervalued and ineffective: Why security training programs still fall short*. CSO Online. https://www.csoonline.com/article/3606377/undervalued-and-ineffective-why-security-training-programs-still-fall-short.html

Rossdawson. (2020, December 9). *What is a keynote speaker? . . .and how to find the best speaker for your event!* https://rossdawson.com/keynote-speaker/what-is-a-keynote-speaker/

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. Prentice Hall.

Smith, A. (2018, March 12). *Pros and Cons of Starting a Cyber Security Awareness Campaign*. IT Security Central - Teramind Blog.

https://itsecuritycentral.teramind.co/2017/12/28/pros-and-cons-of-starting-a-cyber-security-awareness-campaign/

Spremić, M., & Šimunic, A. (2018). *Cyber Security Challenges in Digital Economy*. International Association of Engineers (IAENG). http://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf

Swinhoe, D. (2019, August 14). *Humans are the weak link: Security awareness & education still a challenge for UK companies*. CSO Online. https://www.csoonline.com/article/3430596/humans-are-the-weak-link-security-awareness-education-still-a-challenge-for-uk-companies.html

Statistics How To. (2016, July 18). *What is Central Tendency Bias?* Retrieved from Statistics How To: https://www.statisticshowto.com/central-tendency-bias/

Thomson, K.-L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security*, *2006*(5), 11–15. https://doi.org/10.1016/s1361-3723(06)70356-6

Tyagi, S. (2020, May 3). *Newsletter - Advantages And Disadvantages by*. RankBro. https://rankbro.com/newsletter-advantages-and-disadvantages/

Verhoeven, N. (2019). *Doing Research* (1st ed.). Boom Lemma.

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1–16. https://doi.org/10.1145/1837110.1837125

Wetzer, I., & Broersma, M. (2021, April 22). *Psychologie, houding en gedrag voor beveiliging* [Webinar]. PvIB, Online, Nederland. https://www.pvib.nl/actueel/evenementen/psychologie-houding-en-gedrag-voor-beveiliging

Wigston, S. (2018, June 13). *The Pros and Cons of Hiring Event Speakers for Your Next Corporate Event*. Eaglesflight. https://www.eaglesflight.com/corporate-events/blog/the-pros-and-cons-of-hiring-event-speakers-for-your-next-corporate-event

Wilson, M., & Hash, J. (2003, October). *Building an Information Technology Security Awareness and Training Program*. National Institute of Standards and Technology. http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf

9. Appendix

Appendix l – Interview protocol

Interview protocol English

Interviewer name:	M. Ben Touhami
Interviewee's name:	
Date:	
Location:	Google Meet video meeting

Introduction:

In the context of privacy, I would like to ask you how I can position you in this thesis.

- Can I put your position in the transcript?
- Can I put the company in the transcript?

It is always possible to reconsider the above after this interview if you change your mind.

Recording started

Question:

Can you introduce yourself?

- *what does your job entail?*
- *How much experience do you have with cyber security (awareness)?*
- *How does your function interact with cyber security (awareness)?*

Question:

How would you define cyber security awareness?

Question:

Describe the importance of cyber security awareness in your experience?

Question:

Cyber security awareness is generated by activities that an organization or individual can undertake to enhance their awareness. Which activities do you think enhance cyber security awareness the most/best? Please motivate your answer.

Question:

Have you tried cyber security awareness activities that in your opinion were not effective? If so, can you explain more about the activities and why it was not effective?

Question:

Which aspects would you take into account when drawing up a cyber security awareness program?

Question:

A technical aspect of cyber security awareness is warning messages when you receive an external email.

To what extent does the technical aspect influence the usefulness of cyber security awareness?

Question:

What do you see as the biggest cyber security threat that people should be aware of?

Please do not mention a threat that people cannot do anything about, such as a DDoS attack.

Question:

What are the indicators of an effective cyber security risk awareness culture within an organization?

Based on what aspects are these indicators chosen?

Question:

What would be the biggest obstacle to the transition of an effective cyber security awareness culture?

Question:

What else would you like to mention about cyber security awareness program and their effectiveness? Do you want to add something, or tell a story that you think illustrates this area well?

Thank you for participating the interview.

Interview protocol Dutch

Interviewer:	M. Ben Touhami
Geïnterviewde:	E. Staats
Datum:	8 april 2021
Locatie:	Google Meet video meeting

Introductie:
In het kader van privacy wil ik u vragen hoe ik u in deze thesis kan positioneren.

- Mag ik uw positie in de thesis vermelden?
- Kan ik het bedrijf in de thesis vermelden?

Het is altijd mogelijk om na dit gesprek het bovenstaande te heroverwegen als u van gedachten veranderd.

Opname gestart

Vraag:
Kunt u zich voorstellen?

- Wat houdt uw rol in?
- Hoeveel ervaring heeft u met cyber security (Awareness)?
- Hoe werkt uw functie samen met cyber security (awareness)?

Vraag:

Hoe zou u cyber security awareness definiëren?

Vraag:

Beschrijf het belang van cyber security awareness in uw ervaring?

Vraag:

Cyber security wordt gegenereerd door activiteiten die een organisatie of individu kan ondernemen om hun bewustzijn te vergroten. Welke activiteiten verbeteren volgens u het cyber security awareness het meest / beste? Motiveer uw antwoord.

Vraag:

Heeft u activiteiten op het gebied van cyber security awareness geprobeerd die naar uw mening niet effectief waren? Zo ja, kunt u meer uitleggen over de activiteiten en waarom deze niet effectief waren?

Vraag:

Met welke aspecten zou u rekening houden bij het opstellen van een bewustwordings-programma cyber security?

Vraag:

Een technisch aspect van cyber security *awareness zijn waarschuwingsberichten wanneer u een externe e-mail ontvangt.*

In hoeverre beïnvloedt het technische aspect het nut van cyber security bewustzijn?

Vraag:

Wat ziet u als de grootste bedreiging voor cyberveiligheid waarvan mensen zich bewust moeten zijn?

Buiten beschouwing voor deze vraag zijn dreigementen waar mensen niets aan kunnen doen, zoals een DDoS-aanval.

Vraag:

Wat zijn de indicatoren voor een goede risicobewustzijnscultuur voor cyberveiligheid binnen een organisatie?

Op basis van welke aspecten worden deze indicatoren gekozen?

Vraag:

Wat zou u nog meer willen zeggen over het cyber security awareness programma en de effectiviteit ervan? Wilt u iets toevoegen, of een verhaal vertellen waarvan u denkt dat het dit gebied goed illustreert?

Bedankt voor uw deelname aan het interview!

Appendix ll – Coding results of thematic analysis

In this appendix, the reader will find the result of the coding on the transcripts.

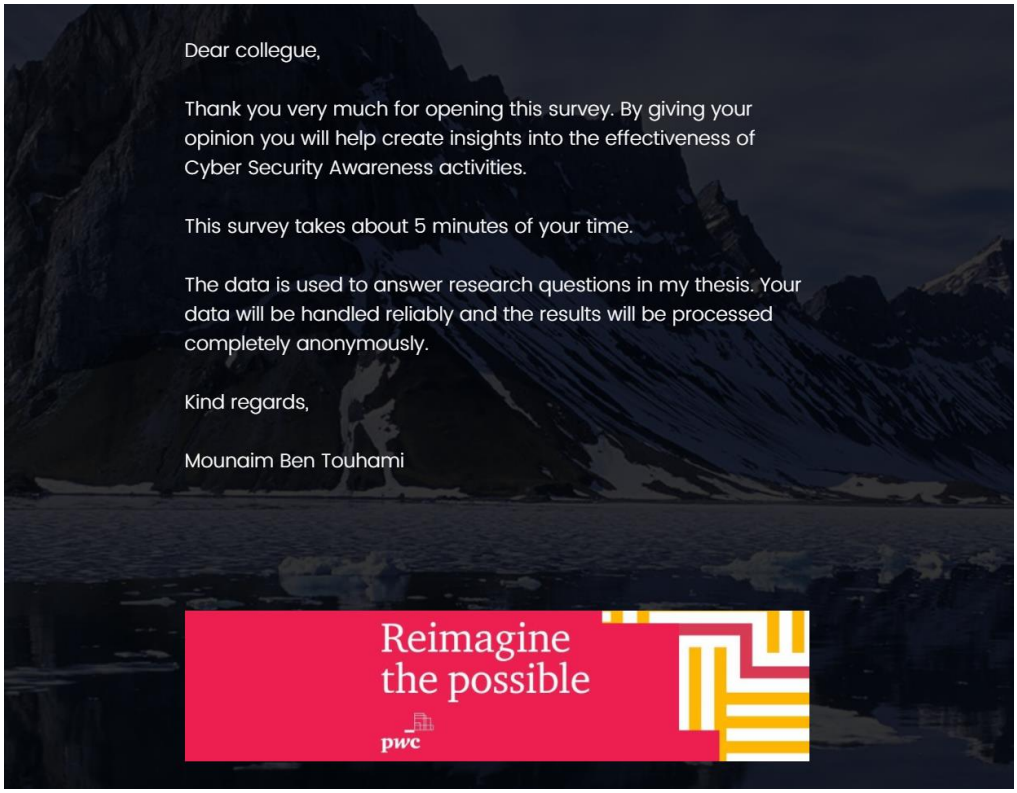
Axial codes:

- Cyber security awareness definition;
- Importance of cyber security awareness;
- Cyber security awareness culture;
- Cyber security awareness activity;
- Cyber security awareness program;
- Technical aspect;
- Incident reporting;
- Involvement from executive board;
- Importance of cyber security awareness;
- Technical aspect;
- Relevance for the employee;
- Target audience;
- Hacking threats;
- Behavior;
- Compliance attitude is not a good attitude;
- Technical aspect;
- Password.

Selective codes:

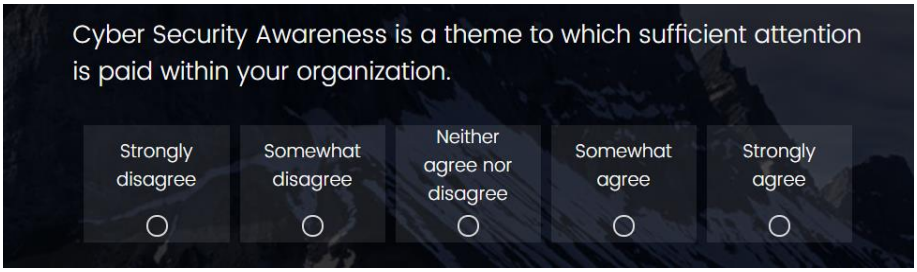
- Cyber security awareness program;
- Importance of cyber security awareness;
- Cyber security awareness activity;
- Organizational practice;
- Important factors for cyber security awareness.

Appendix lll – Survey template

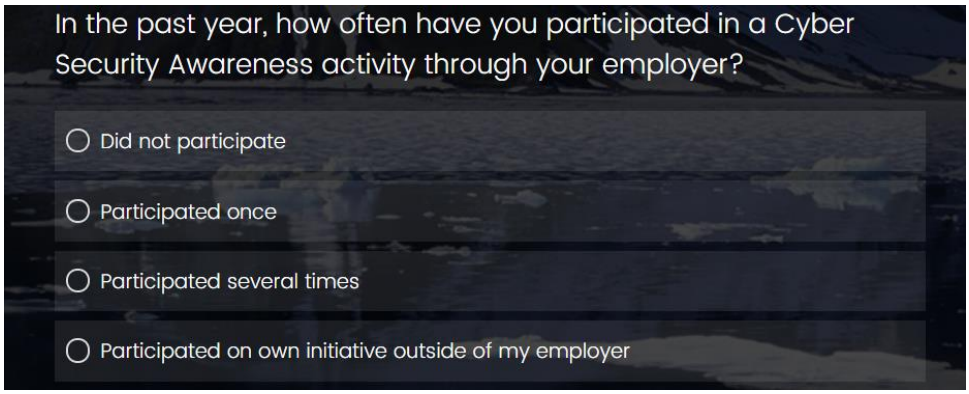


Page Break

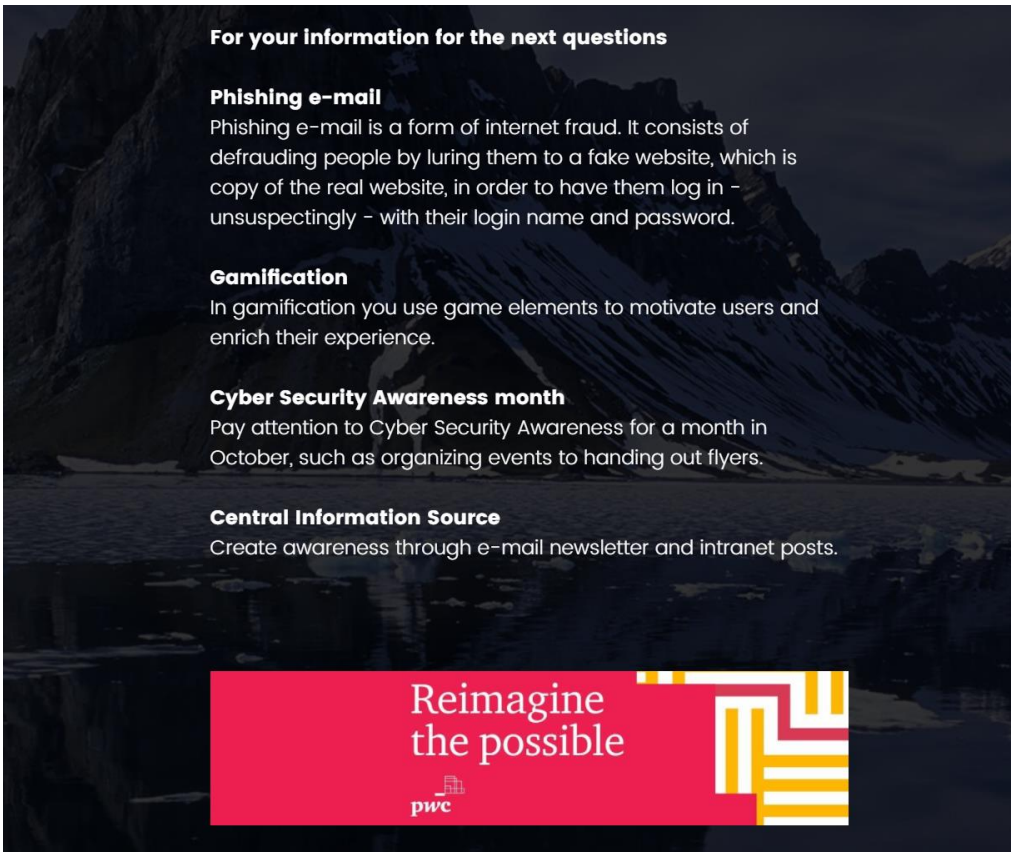
Question 1



Question 2



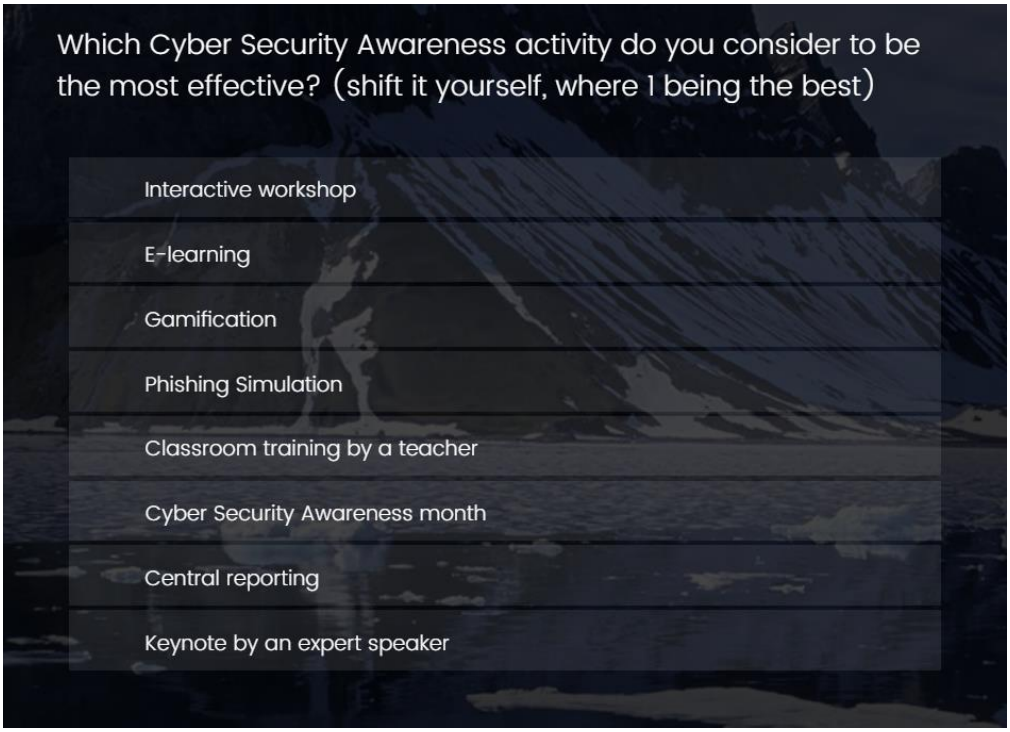
Page Break



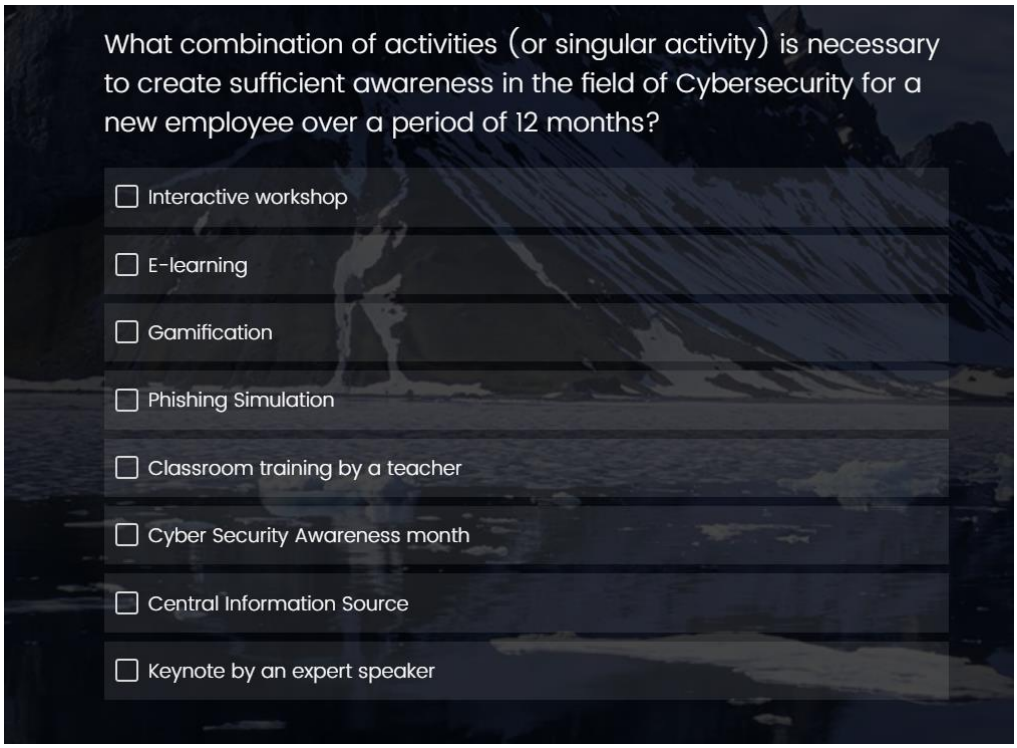
Page Break

Question 3

Question 4

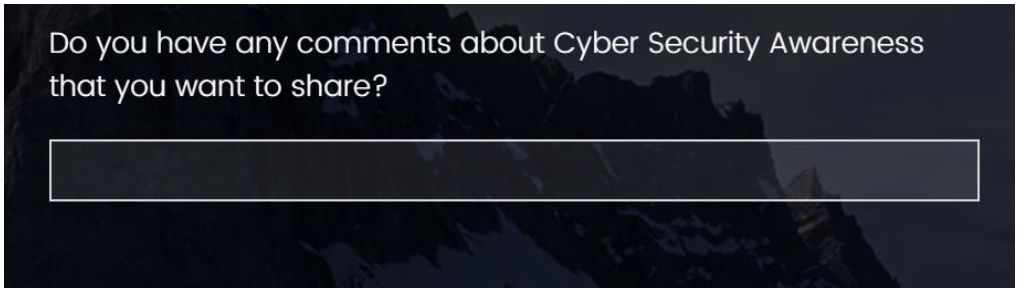


Question 5

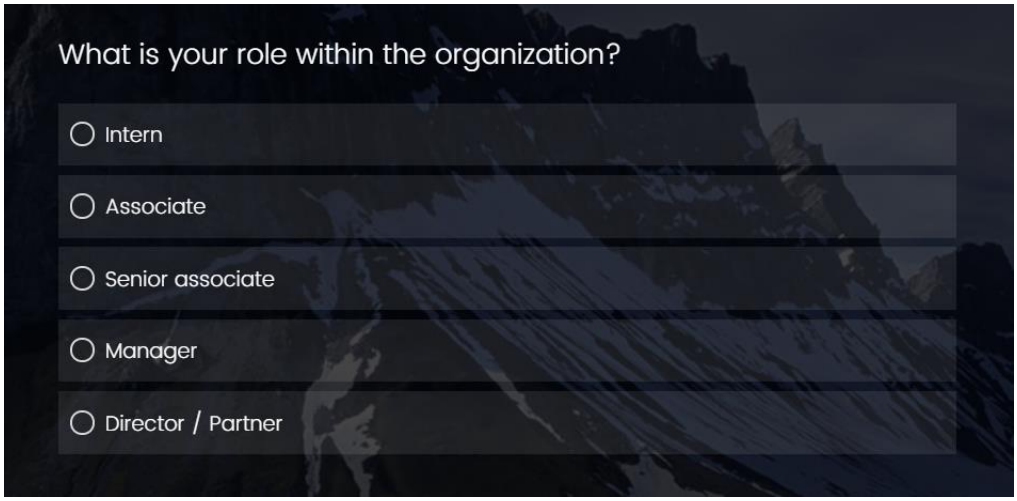


Page Break

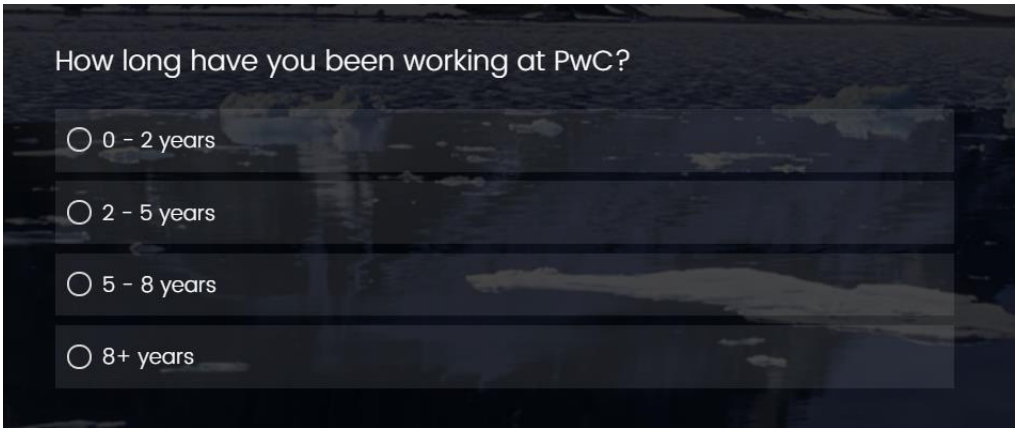
Question 6



Question 7



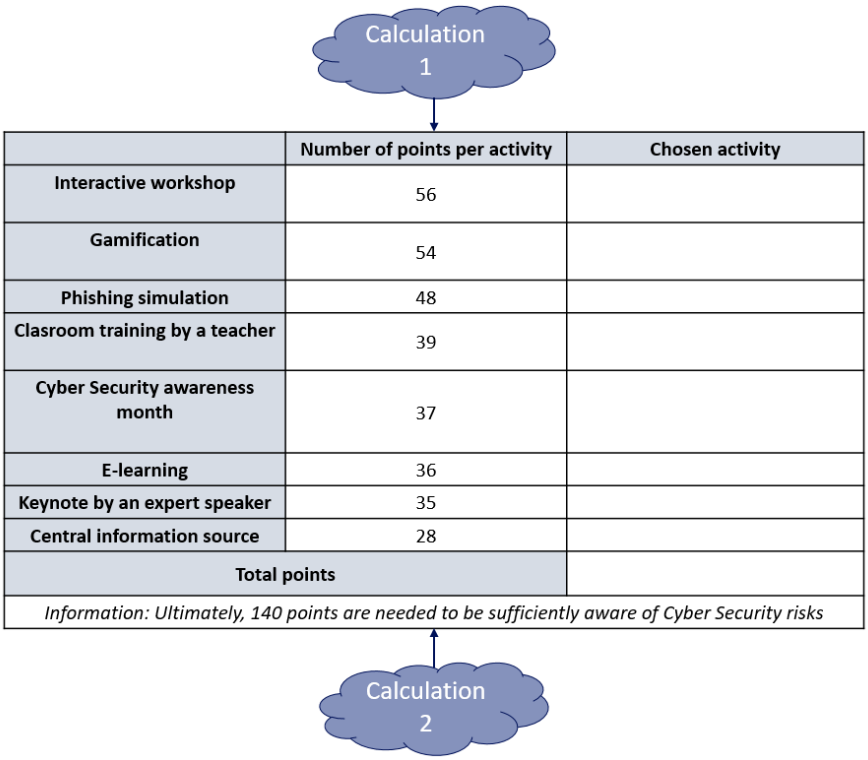
Question 8



End of Survey

Appendix IV – Model statement calculation

In this appendix, further explanation will be given about the development of the model and the rationale behind the model. The model mainly consists of two different calculations, which can be seen in the figure below. The first calculation consists of determining the allocation of points per activity. The second calculation will show how many points are needed to get someone sufficiently aware.



	Number of points per activity	Chosen activity
Interactive workshop	56	
Gamification	54	
Phishing simulation	48	
Clasroom training by a teacher	39	
Cyber Security awareness month	37	
E-learning	36	
Keynote by an expert speaker	35	
Central information source	28	
Total points		
Information: Ultimately, 140 points are needed to be sufficiently aware of Cyber Security risks		

Calculation 1

We have sent a survey within PwC, wherein we asked professionals which cyber security awareness activity they themselves had considered to be the most effective. The professionals were given the opportunity to sort the activities themselves and prioritize them as being relatively more or less effective. The question asked can be found in Appendix III, question 4. For verification, the respondent was asked to individually assess the activity, this is question 3 from the survey. This was done in order to conform to question 4 that an activity is actually perceived (in) effectively and was not clicked by the respondent out of laziness.

From the data, it can be seen which activities were placed in which position by the respondents. By way of illustration, the figure below shows that 20 respondents ranked gamification as the most effective.

#	Field	1	2	3	4	5	6	7	8
1	Interactive workshop	21	21	12	5	4	1	0	0
2	E-learning	1	2	5	15	10	9	12	10
3	Gamification	20	22	8	3	7	1	2	1
4	Phishing Simulation	12	9	15	9	7	7	3	2
5	Classroom training by a teacher	2	5	8	12	12	13	8	4
6	Cyber Security Awareness month	6	3	5	6	10	14	10	10
7	Central Information Source	0	0	3	7	3	11	16	24
8	Keynote by an expert speaker	2	2	8	7	11	8	13	13

We used the following scale to weight individual activities. The activities ranked number one are worth 10 points, the activities ranked number two are worth 9 points, etc. We multiply the number of votes obtained per activity being ranked in a certain position by the number of points awarded for this position. Then we aggregate the votes per each activity. This can be seen in the figure below.

	1 vote for # 1 = worth 10 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	21	10	210
2	E-learning	1	10	10
3	Gamification	20	10	200
4	Phishing simulation	12	10	120
5	Classroom training by a teacher	2	10	20
6	Cyber Security awareness month	6	10	60
7	Central information source	0	10	0
8	Keynote by an expert speaker	2	10	20

	1 vote for # 2 = worth 9 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	21	9	189
2	E-learning	2	9	18
3	Gamification	22	9	198
4	Phishing simulation	9	9	81
5	Classroom training by a teacher	5	9	45
6	Cyber Security awareness month	3	9	27
7	Central information source	0	9	0
8	Keynote by an expert speaker	2	9	18

	1 vote for # 3 = worth 8 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	12	8	96
2	E-learning	5	8	40
3	Gamification	8	8	64
4	Phishing simulation	15	8	120
5	Classroom training by a teacher	8	8	64
6	Cyber Security awareness month	5	8	40
7	Central information source	3	8	24
8	Keynote by an expert speaker	8	8	64

	1 vote for # 4 = worth 7 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	5	7	35
2	E-learning	15	7	105
3	Gamification	3	7	21
4	Phishing simulation	9	7	63
5	Classroom training by a teacher	12	7	84
6	Cyber Security awareness month	6	7	42
7	Central information source	7	7	49
8	Keynote by an expert speaker	7	7	49

	1 vote for # 5 = worth 6 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	4	6	24
2	E-learning	10	6	60
3	Gamification	7	6	42
4	Phishing simulation	7	6	42
5	Classroom training by a teacher	12	6	72
6	Cyber Security awareness month	10	6	60
7	Central information source	3	6	18
8	Keynote by an expert speaker	11	6	66

	1 vote for # 6 = worth 5 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	1	5	5
2	E-learning	9	5	45
3	Gamification	1	5	5
4	Phishing simulation	7	5	35
5	Classroom training by a teacher	13	5	65
6	Cyber Security awareness month	14	5	70
7	Central information source	11	5	55
8	Keynote by an expert speaker	8	5	40

	1 vote for # 7 = worth 4 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	0	4	0
2	E-learning	12	4	48
3	Gamification	2	4	8
4	Phishing simulation	3	4	12
5	Classroom training by a teacher	8	4	32
6	Cyber Security awareness month	10	4	40
7	Central information source	16	4	64
8	Keynote by an expert speaker	13	4	52

	1 vote for # 8 = worth 3 points	Votes obtained	Points	Points obtained
1	Interactive Workshop	0	3	0
2	E-learning	10	3	30
3	Gamification	1	3	3
4	Phishing simulation	2	3	6
5	Classroom training by a teacher	4	3	12
6	Cyber Security awareness month	10	3	30
7	Central information source	24	3	72
8	Keynote by an expert speaker	13	3	39

	CS awareness activity	Total points	Model points
1	Interactive Workshop	559	56
2	Gamification	541	54
3	Phishing simulation	479	48
4	Classroom training by a teacher	394	39
5	Cyber Security awareness month	369	37
6	E-learning	356	36
7	Keynote by an expert speaker	348	35
8	Central information source	282	28

The activity with the most points is awarded 56 points and the activity with the lowest points is awarded 28 points.

Calculation 2

The second calculation is to determine when a person is sufficiently aware of cyber security. The question was asked in the survey (question 5): what combination of activities (or singular activity) is necessary to create sufficient awareness in the field of cyber security for a new employee over a period of 12 months? The combination per respondent can be seen in the figure below.

In the first calculation, a weight was assigned per activity. The weight of the chosen activity (s) per respondent is added together. This effect can be seen in the figure below. The average of this summary is taken, which is 140 points. This means that in this model 140 points are needed to create awareness.

Respondent	Combination of activity to create sufficient awareness							
1	Interactive workshop							
2	Interactive workshop	E-learning						
3	Interactive workshop	E-learning						
4	Interactive workshop	E-learning	Phishing simulation					
5	Interactive workshop	E-learning	Phishing simulation					
6	Interactive workshop	E-learning	Phishing simulation	Classroom training by a teacher				
7	Interactive workshop	E-learning	Phishing simulation		Cyber Security Awareness month			
8	Interactive workshop	E-learning			Cyber Security Awareness month			
9	Interactive workshop	E-learning				Keynote by an expert speaker		
10	Interactive workshop	E-learning		Classroom training by a teacher				
11	Interactive workshop	E-learning					Gamification	
12	Interactive workshop	E-learning					Gamification	
13	Interactive workshop	E-learning	Phishing simulation				Gamification	
14	Interactive workshop	E-learning	Phishing simulation				Gamification	
15	Interactive workshop	E-learning	Phishing simulation				Gamification	
16	Interactive workshop	E-learning	Phishing simulation				Gamification	
17	Interactive workshop	E-learning	Phishing simulation	Classroom training by a teacher			Gamification	
18	Interactive workshop	E-learning	Phishing simulation	Classroom training by a teacher			Gamification	
19	Interactive workshop	E-learning	Phishing simulation	Classroom training by a teacher			Gamification	
20	Interactive workshop	E-learning	Phishing simulation	Classroom training by a teacher			Gamification	
21	Interactive workshop	E-learning	Phishing simulation				Gamification	Central Information Source
22	Interactive workshop	E-learning	Phishing simulation				Gamification	Central Information Source
23	Interactive workshop	E-learning	Phishing simulation				Gamification	
24	Interactive workshop	E-learning	Phishing simulation		Cyber Security Awareness month		Gamification	
25	Interactive workshop	E-learning	Phishing simulation		Cyber Security Awareness month		Gamification	Central Information Source
26	Interactive workshop	E-learning		Classroom training by a teacher			Gamification	
27	Interactive workshop						Gamification	
28	Interactive workshop						Gamification	
29	Interactive workshop						Gamification	
30	Interactive workshop						Gamification	
31	Interactive workshop						Gamification	
32	Interactive workshop						Gamification	
33	Interactive workshop		Phishing simulation				Gamification	
34	Interactive workshop		Phishing simulation				Gamification	
35	Interactive workshop		Phishing simulation				Gamification	
36	Interactive workshop		Phishing simulation				Gamification	
37	Interactive workshop		Phishing simulation		Cyber Security Awareness month		Gamification	
38	Interactive workshop			Classroom training by a teacher			Gamification	Central Information Source
39	Interactive workshop					Keynote by an expert speaker	Gamification	
40	Interactive workshop					Keynote by an expert speaker	Gamification	
41	Interactive workshop			Classroom training by a teacher			Gamification	
42	Interactive workshop					Keynote by an expert speaker	Gamification	Central Information Source
43	Interactive workshop				Cyber Security Awareness month	Keynote by an expert speaker	Gamification	
44	Interactive workshop				Cyber Security Awareness month			Central Information Source
45	Interactive workshop				Cyber Security Awareness month			Central Information Source
46	Interactive workshop				Cyber Security Awareness month	Keynote by an expert speaker		Central Information Source
47	Interactive workshop				Cyber Security Awareness month			
48	Interactive workshop		Phishing simulation					
49	Interactive workshop		Phishing simulation	Classroom training by a teacher	Cyber Security Awareness month			
50	Interactive workshop		Phishing simulation		Cyber Security Awareness month			Central Information Source
51	Interactive workshop			Classroom training by a teacher		Keynote by an expert speaker		
52		E-learning						
53		E-learning					Gamification	
54		E-learning					Gamification	
55		E-learning	Phishing simulation				Gamification	
56		E-learning	Phishing simulation				Gamification	Central Information Source
57		E-learning	Phishing simulation				Gamification	Central Information Source
58		E-learning						
59		E-learning						
60		E-learning		Classroom training by a teacher	Cyber Security Awareness month			
61							Gamification	
62			Phishing simulation				Gamification	
63			Phishing simulation				Gamification	
64						Keynote by an expert speaker	Gamification	
65					Cyber Security Awareness month			

	Interactive workshop	E-learning	Phishing simulation	Classroom training	CS Awareness month	Keynote speaker	Gamification	Central Information Source	
Respondent	Weight = 56	Weight = 54	Weight = 48	Weight = 39	Weight = 37	Weight = 36	Weight = 35	Weight = 28	Enumeration
1	56								56
2	56	54							110
3	56	54							110
4	56	54	42						152
5	56	54	42						152
6	56	54	42	39					191
7	56	54	42		37				189
8	56	54			37				147
9	56	54				36			146
10	56	54		39					149
11	56	54					35		145
12	56	54					35		145
13	56	54	42				35		187
14	56	54	42				35		187
15	56	54	42				35		187
16	56	54	42				35		187
17	56	54	42	39			35		226
18	56	54	42	39			35		226
19	56	54	42	39			35		226
20	56	54	42	39			35		226
21	56	54	42				35	28	215
22	56	54	42				35	28	215
23	56	54	42				35		187
24	56	54	42		37		35		224
25	56	54	42		37		35	28	252
26	56	54		39			35		184
27	56						35		91
28	56						35		91
29	56						35		91
30	56						35		91
31	56						35		91
32	56						35		91
33	56		42				35		133
34	56		42				35		133
35	56		42				35		133
36	56		42				35		133
37	56		42		37		35		170
38	56			39			35	28	158
39	56					36	35		127
40	56					36	35		127
41	56			39			35		130
42	56					36	35	28	155
43	56				37	36	35		164
44	56				37			28	121
45	56				37			28	121
46	56				37	36		28	157
47	56				37				93
48	56		42						98
49	56		42	39	37				174
50	56		42		37			28	163
51	56			39		36			131
52		54							35
53		54					35		89
54		54					35		89
55		54	42				35		131
56		54	42				35	28	159
57		54	42				35	28	159
58		54							54
59		54							54
60		54		39	37				130
61							35		55
62			42				35		77
63			42				35		77
64						36	35		71
65					37				37

Mean	140