TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

TUT Centre for Digital Forensics and Cyber Security

ITC70LT

Andres Sumin 143649IVCM

EVALUATION METHOD FOR CYBER AWARENESS COURSE

Master thesis

Supervisor:

Sten Mäses, MSc

Junior Researcher, TUT

Co-supervisor:

Liina Randmann, PhD

Psychology Chair, TUT

Tallinn 2016

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Andres Sumin

Date:

Autorideklaratsioon

Olen koostanud antud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud. Käesolevat tööd ei ole varem esitatud kaitsmisele kusagil mujal.

Autor: Andres Sumin

Kuupäev:

Abstract

In the past years the cybercrime landscape has developed rapidly and increasing security breaches have leaded to major losses suffered by the affected organizations. The human factor in cyber security incidents is rising, around 95% of all cyber security related incidents involve human error. Human factor plays a significant role in cyber security: individual difference (e.g. knowledge and previous experiences), cognitive abilities (e.g. attention) and personality traits (e.g. narcissistic personality traits).

In the case of the human factor, there are various control measures, most of which are related to training and education. In 2015, Estonian Ministry of Defense started implementing Estonian cyber security awareness initiative called Cyber Hygiene. The goal of the initiative is to develop a common standard for safe cyber behavior, as well as to create an e-learning environment in order to minimize the cyber incidents caused by the human factor. In 2016, the first version, a prototype, of Cyber Hygiene e-learning course was completed.

Estonian Ministry of Defense and other key partners in the initiative have emphasized the need to expand the methodical foundation of the e-learning course. The objective of this thesis is to improve the Cyber Hygiene e-learning course with evaluation method, which will take under consideration different psychological aspects and methodical principles in order to create a scale for structural evaluation method to measure the participant's self-reported behaviors, support the study process and evaluate the acquired information of the participants. Based on developed method the author increased the volume of the questions used in the e-learning course. The questions were evaluated with cyber security experts and the author conducted pilot test on Tallinn University of Technology undergraduate IT students. Results from 69 participants indicated that the method proves to be valid as an assessment method for measuring the self-reported behavior and knowledge of the course participants. The developed method and questions will be taken into use by the BHC Laboratory, who is the developer of the e-learning course.

This thesis is written in English and is 73 pages long, including 9 chapters, 5 figures and 3 tables.

Annotatsioon

Infoturbe koolituse hindamismeetodika

Viimastel aastatel on küberkuritegevuse osakaal arenenud suure kiirusega, millest tulenenud turvaintsidentide kasv on põhjustanud palju kahju organisatsioonidele. Inimfaktor mängib olulist rolli infoturbes, see on mõjutatud mitmete inimestele omaste aspektide kaudu: individuaalne erinevus (näiteks teadmised, kogemused), kognitiivsed võimed (näiteks tähelepanuvõime) ja isiksuseomadused (näiteks nartsissism).

Üks efektiivsemaid lahendusi vähendamaks inimfaktoriga seotud riske, on infoturbe alased koolitused. Aastal 2015, algatas Eesti Kaitseministeerium projekti Küberhügieen, mille eesmärgiks on arendada välja ühtne standard küberkeskkonnas ohutuks käitumiseks ning luua e-õppe keskkond töötajate paremaks harimiseks küberohtudest. Aastal 2016, valmis esimene versioon protoüüp Küberhügieeni e-õppe kursusest.

Eesti Kaitseministeerium koos partneritega on väljendanud vajadust laiendada Küberhügieen e-õppe kursuse struktuurset ja metoodilist alust. Selle lõputöö eesmärk on täiendada Küberhügieeni e-õppe kursust struktuurse hindamismeetodi kaudu. Töös võetakse arvesse erinevad psühholoogilisi aspekte ning metoodilisi printsiipe, et luua hindamismeetod, mis mõõdab kursusel osalejate käitumist, toetab õppeprotsessi ja hindab kursusel omandatud informatsiooni mahtu. Tuginedes arendatud metoodile, suurendas autor e-õppe kursusel olevate küsimuste arvu, mis valideeriti infoturbe valdkonna ekspertide poolt. Lisaks viis autor läbi pilootuuringu Tallinna Tehnikaülikooli IT üliõpilaste seas. Tulemused 69 osaleja põhjal näitasid, et metood osutus efektiivseks hindamaks käitumist ja kursusel omandatud teadmisi. Arendatud metood ja küsimused võetakse kasutusele BHC Laboratooriumi poolt, kes on Küberhügieeni e-õppe arendaja.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 73 leheküljel, 9 peatükki, 5 joonist ja 3 tabelit.

Table of abbreviations and terms

Sample	Set of observations drawn from a specific population.
Individual	A single person, especially when compared to the group or set to which they belong.
Respondent	An individual providing responses to specific information collection attributes.
Participant	An individual providing responses to specific information collection attributes.
Regular user	Are considered as all members of the organization who are using computers and computer systems for their everyday work.
Methodical principles	Is a system of broad principles from which specific methods or procedures may be derived to interpret specific results or solve different problems within the scope of a particular discipline.
Method	A structural approach to something, the specific systematic way of doing something.
TUT	Tallinn University of Technology.
BHC	BHC Laboratory, is a cyber capabilities' development company.
Cyber security	Processes or methodologies which purpose is to protect cyber environment, organization and user's assets (e.g. technological devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment).
Prototype	An original or first model of something from which other forms are copied or developed.
Social desirability	Individual's desire to be viewed in a positive light by other individuals.
Cyber Hygiene Standard	Document, which is prepared by a team of experts led by TUT and strives to provide a universal approach to cyber hygiene, applicable to large number of organizations by promoting responsible human behavior to avoid exposure to the threats emanating from the cyber space.

Confidential information	Any non-public information pertaining to organization's business. Is related to the business of the company or any subsidiary relating to research and development, processes, trade secrets, customers, suppliers, finances and business plans and strategies.
Cyber security expert	Individual who has attained superior performance in a cyber security field. Expertise is accomplished by instruction and extended practice.

Table of Contents

List of figures

List of tables

1. Introduction

1.1. General background

In the past years, cyber security has received a lot of attention from various business areas, enterprises and governments, largely because of the rapid development of the cybercrime landscape and increasing security breaches leading to major losses suffered by the affected organizations [1]. For example, the market for cybercrime-as-a-service (CaaS) is advancing rapidly with the competition between malware vendors leading to increased innovation [2]. That is one of the reasons why the vast majority of organizations are exposed to cyber-attacks more than ever before, but this does not end here. Additionally, based on RSA 2015 cybercrime trends, the other popular trends were mobility, large scale attacks and targeted attacks. [2][3] Criminals are exploiting the speed, anonymity and convenience of the Internet to commit wide range of criminal activities. [4] As cybercrime landscape progress speeds, the organizations must be accompanied with security measures in order to maintain and improve their security level.

Security is an ever changing issue, which has evolved enormously over the last few decades. One of the historical problems with the cyber security is that it is often approached as a purely technical issue, with almost no consideration of social aspects (e.g. people-related issues). Businesses have tried to focus on technical aspects for years to provide effective protection against the security threats: building highly complex infrastructures, implementing more sophisticated intrusion prevention mechanisms, using greater automation in infrastructure automation etc. All technical aspects can work effectively as security measures, but technical aspects alone cannot provide a comprehensive solution. [5] Cyber security is a multi-dimensional parametric equation which aims to ensure the information confidentiality, integrity, availability, and aims to deliver actual business benefits. The security equation also involves people and the human aspects of cyber security, which need to be balanced with the technical solutions in order to provide a comprehensive solution. [6]

The 2015 IBM Cyber Security intelligence report shows, that around 95% of all information security related incidents involve human error. Many of these incidents were caused due to attacks, which are conducted using directly human weaknesses to gain unauthorized access to sensitive environments or data [7]. These attacks have been successful because of several factors: some of them are because users are disregarding the best practice's, users are ignorant, distracted, or just curious [8]. An organization's greatest assets are its employees; at the same time the employees are the weakest link in the security chain. All this takes place in an era where the mobility and accessibility plays a great role in enhancing the productivity of the employees. [9], [10]

In the case of the human factor, there are various control measures, most of which are related to training and education. The training and education involves not only technical training of IT personnel, but also general cyber security awareness training and other awareness campaigns which should become a must for everyone. This has been proven to be a mandatory criterion in international Information Security Management System standards. [11] In the past years, many organizations, communities and countries have started to acknowledge the human factor in cyber security and are taking steps to mitigate the weakest link in the security chain, either with awareness campaigns, trainings or group projects. [1] For example, some of the global cyber awareness projects are Cyberstreetwise [12], StaySafeOnline [13], Futurelearn awareness training [14], Symantec security awareness program [15] and many more. Over the years there have also been conducted several cyber awareness campaigns and projects in Estonia: IT planet [16], Save Liisa ID [17], Assa Pauk [18] and many more. Their main goal is to train users through games, questionnaires and video trainings. These campaigns and projects are effective and available for everyone, but because many organizations still undervalue the importance of the security awareness trainings, they have not gained enough global attention and have not been widely adopted [19].

In 2015, Estonian Ministry of Defense started implementing Estonian cyber security awareness initiative called Cyber Hygiene. The goal of the initiative is to develop a common standard for safe cyber behavior, as well as to create an e-learning environment in order to minimize the cyber incidents caused by the human factor. The e-learning course educates the public and the private sector employees, specialists and management

about cyber threats. It is estimated that by implementing Cyber Hygiene, an organization or institution can prevent 70-80% of the risk profile of cyber threats. [20], [21]

In 2016, the first version of the e-learning course was completed – a prototype. The prototype consists of training videos, materials and related tests. As the e-learning course is in a prototype status and still under the development, it needs improvement in several areas. In order to improve the course materials and measure the results properly, the course needs to contain scientific methodical principles, which supports the purpose of the course and enables to systematically produce components to the course and measure the results.

The purpose of this thesis is to develop an evaluation method for Cyber Hygiene e-learning course.

1.2. Importance of human factor

The numerous technical advances in information sciences do not always result in improved security. Therefore, cyber security cannot be described solely as a technical problem. Computer systems are developed and operated by people who, as physical systems, are vulnerable to certain factors. This makes cyber security also a human factor issue. Human factor plays a significant role in computer security: individual difference (e.g. knowledge and previous experiences), cognitive abilities (e.g. attention) and personality traits (e.g. narcissistic personal traits) can impact behavior. Humans' security behaviors are straightly related to an individual's perception of risk. Organizations need to develop a culture where positive security behaviors are endorsed. Employees need to be educated about the importance of security awareness, and this should incorporate behavioral training. [22], [23]

People are the key factor to either success or failure of cyber security in organizations. Every security problem is associated more or less with humans, not only with technology. Any organization which is mitigating information security risks through technological countermeasures will fail eventually [24]. In any organization, every employee should be aware of the required security practices and implementations. Many studies have shown

[25] that in order to gain such a contribution from employees, employees must pass a proper awareness trainings and other awareness mechanisms on a regular basis. [1]

As found in a research conducted by Jim Blythe, Ross Koppel and Sean W. Smith [26], there is a great discrepancy between how security regulations work in theory and in practice. The research suggested that, e.g. despite the fact that security systems require people to use unique and strong passwords and keep them in safe place, people are still finding the ways to circumvent and use security regulations in their organizations. In many cases, employees still store passwords on sticky notes on monitors and keyboards, or they share them with friends. Therefore, the real situations in organizations does not always match the expectations of the security specialists (e.g. while security specialists insist on regulations in password behavior, people still intentionally or unintentionally open doors to security breaches in systems and work environments, trying to make their lives easier). Human behavior related security issues can be mitigated by regular and effective training that covers important areas (e.g. password management) and best practices (e.g. identification of strangers) which create broad base of knowledge for employees to draw upon when confronted by security related situations or issues. [27]

1.3. Problem statement

As the Cyber Hygiene initiative is one of the largest cyber awareness outreach campaigns in Estonia, focusing on organizations, it needs to be not only technically but also scientifically legitimate and proficient. BHC Laboratory (hereinafter BHC) in collaboration with Tallinn University of Technology (hereinafter TUT) have finished the first prototype of Cyber Hygiene e-learning course. Because it is the first prototype of the project it is still under development and needs improvement with scientific approach. Given the complexity of the cyber security, changing security environment and international nature of the effort, the Estonian Ministry of Defense and other key partners in the initiative have emphasized the need for further development of the Cyber Hygiene e-learning program. The further developments should not only introduce “routine updates” but should further expand the methodical foundation of the e-learning program, explore its development potential in assessing and mitigating human risk behavior, etc.

The prototype is divided into three parts: Questionnaire measuring existing knowledge and behavior, learning module and knowledge evaluation test. The first implementation of the e-learning course contains basic materials and questions measuring the existing behavior and assessing the acquired information from the course. In order to provide legitimate results to the organization which is conducting the course, the course needs to contain more psychological and structural approach. Thus, in order to evaluate the participant's real behavioral patterns, the behavior assessment questionnaire must contain all topics described in the course with targeted questions towards every topic. The questions need to be developed using psychological factors which will focus on getting the real and honest answers, addressing the most important factors in every topic in order to provide results which will show self-reported behavior patterns. Based on that, the management can assess the current cyber security level of the organization. Similar psychological and structural approach needs to be used with other questions in the course (e.g. the control questions which are used as a study method in learning module and a test which evaluates the acquired information). These two last modules need to be conducted in a way which will support the learning method and measure the knowledge acquired during the course.

As the Cyber Hygiene initiative suggest, that the Cyber Hygiene e-learning course needs to be conducted at least once a year for every organization, in order to avoid the questions recurrence for the participants, the course needs to contain large volume of different questions for every topic. This will eliminate the automatic answers for the familiar questions and raise the diversity of the questions.

In short, the main problems addressed in this thesis are following:

- Human factor as a vulnerability in cyber security.
- Shortcomings of the Cyber Hygiene prototype e-learning course:
    - lack of psychological and structural approach,
    - insufficient methodical approach,
    - small volume of unique questions,
    - not scalable,
    - no results evaluation method.

1.4. The contribution of the author

The lack of the scientific approach in educational programs makes it fairly difficult to improve the content and objectively measure the results of the programs. Therefore – this master thesis is one part of the scientific contribution to the Cyber Hygiene e-learning program. Developers of the program have expressed the need to further scientific research in the field, in particular with respect to the methodical principles of the questions used in the program.

The purpose of this thesis is to develop an evaluation method for Cyber Hygiene e-learning course. This will improve the course questions modules, evaluate the results and in turn will raise the cyber awareness and readiness of the organizations.

The specific contribution of the author is following:

- Developing a method which will take under consideration different psychological aspects and methodical principles in order to create a scale for structural evaluation methods to measure the participant's self-reported behaviors, support the study process and evaluate the acquired information of the participants.
- Based on developed method the author increases the volume of the questions used in the e-learning course, after which will evaluate the questions with experts and conduct pilot test on the students to verify the effectiveness of the method.

Additionally, the author creates a concise cheat sheet (manual) of the methodical principles for the BHC, which can be used in further development process or analysis of the course and questions. Due to the legal restrictions based on agreements with the BHC, the cheat sheet is not presented in this thesis.

2. Overview of the Cyber Hygiene e-learning course

2.1. General overview

In 2015, the Estonian Ministry of Defense launched an initiative, with the aim to develop a common standard for safe cyber behavior as well as to create e-learning environment to better educate employees about cyber threats. The initiative was signed in addition to Estonia by six states: Netherlands, Austria, Finland, Latvia, Lithuania and in the name of the European Union, by the EU High Representative Federica Mogherini. Estonian and Latvian ministries of defense will start using the standard for performing in cyberspace and will make it compulsory for employees to pass the corresponding e-learning course once a year. The aim is to expand the cyber hygiene initiative to cover all Europe. [21]

The development of the first e-learning platform was done jointly between Estonian Ministry of Defense and Latvian Ministry of Defense, who participated in the special working group set up for that purpose. The effort to address the issue of Cyber Hygiene was approached in two phases: (1) a comprehensive "Cyber Hygiene Standard" document, providing the conceptual basis was developed [28], the document has been later adopted in the Estonian Ministry of Defense by the Ministerial Decree; (2) E-Learning platform was developed. [20], [21]

Since the states signed the initiative, the Estonian Ministry of Defense disclosed a public procurement in January, 2015 to obtain a Cyber Hygiene awareness training e-learning platform. Necessary requirements were met by the TUT and BHC, who were the main contractors for the course development and have created the first version of the course, a prototype. [29]

2.2. Structure

The Cyber Hygiene e-learning course is an interactive, engaging and effective tool. It consists of a training module and two separate test modules. The course targets three different categories of employees: regular users, specialists, and managers; and addresses the specific concerns and threats associated with each of these groups. The course is not in depth technical course on cyber security aspects. It mainly focuses on basic cyber

security topics that every organization faces every day. The e-learning course goal is to give a basic understanding and concepts of cyber threats which surround us every day, which is the very basics of cyber security concepts that everyone should know. Hence the name “Cyber Hygiene”. The course can additionally serve as an effective management tool for creating the security profile of the organization, risk assessments and decisions on implementing cyber security in the organization. [28]

The course is conducted in three parts. The first part starts with the questionnaire which is aimed to measure the users existing knowledge and behavior patterns towards cyber security. The questionnaires goal is to measure participant’s behaviors in order to assess the potential risk level of the organization. Once user has successfully finished the behavior assessment test, one will be directed to the main module of the course. The main module of the course concerns 14 different topics. These topics are selected by the Cyber Hygiene initiative working group, by taking under consideration what is actual, important in the working environment and what has an impact on organizations cyber security tolerance. The course will give a proper overview of the topics and describes how to mitigate topic related risks. Topics described previously are: Password risks, USB related topics, Bring your own device (BYOD), Security etiquette, E-mail related risks, Self-discipline, Open Wi-Fi, Bad identification culture, Losing of data (security of devices, back-ups), Culture of communication, Harmful website, Internet of things (IoT). [28]

In the main module, every topic consists of informational animated video, which describes wrong behavior to the related topic, followed by control question. The control question is related to the video or similar situation and is used as learning method. After the question, an explanation comes next which describes the wrong behavior and explains the question content. This is followed by the informational text related to the topic. This text will give an overview of all the main threats related to the topic and instructions on how to properly act, to protect oneself against them in everyday life. This part of the module will occur for every topic, together 14 times. The last part of the e-learning course is the test, which will measure the understanding and knowledge of how user has acquired the information from the course and gives a conclusion whether the course has been completed successfully or not. [28]

2.3. Defining the limits

The main goal of the thesis is to develop a structural evaluation method to improve e-learning course. Based on the method, the author will raise the volume of the questions in the course and do pilot test based on new material. This thesis focuses only on previously mentioned goals. Although the e-learning course is still in prototype stage, therefore many substantive aspects of the course may need additional improvement, the purpose of this thesis is not to redefine, validate or change the topics, videos or informational study materials presented in course.

3. Previous work

It is difficult to effectively measure the human risk behavior because of different beliefs, perceptions and irregular behavior. In addition, different incidents like data breaches and social engineering attacks go often undetected, making it hard to determine the points of failures. Often these attacks become explicit much later when the damage is already done. There have been created different cyber security evaluation methods in the past for measuring the awareness of the regular users: awareness trainings and standalone questionnaires. States, communities and companies are approached differently on raising user awareness towards cyber security. There are many quizzes for measuring the security awareness level, commercial and free training programs with the aim to educate and train users, but not many behavioral measuring methodologies. Many of these programs include different tests to verify that the participants have understood the concepts, other programs do not include these tests. Because current thesis focuses on improving cyber awareness course (Cyber Hygiene), the author will look into projects with similar purposes. The author gives a brief overview of approaches that are done by different companies.

Several cyber awareness training programs and questionnaires have been developed to evaluate the cyber awareness and behavior patterns. SANS institute has developed a training program called “Securing the human”, which is aimed to improve the cyber awareness of the end users. Although the first goal was to develop the course for the regular users, they have also developed awareness courses for developers and ICS engineers. On the other hand, the regular user training program does not contain methodical principles to measure the existing awareness level of the user. Alongside with Securing the human program, SANS institute has developed a standalone security awareness survey which is measuring organization’s security awareness programs’ effectiveness and strength. The survey asks how employees respond to specific security related questions and situations. But the context is fairly general and does not involve questions about user’s behaviors, more technical aspects, such as if the user has found a malware from his computer. The results of the survey can determine the areas which involve employees and need improvement. [30], [31]

Trustwave offers a Security awareness education (SAE) program which covers core concepts, awareness topics, best practices and much more [32]. By default, the courses do not offer any tools for measuring user awareness level and behavior patterns, although some of the modules include quizzes for testing users understanding of the processed materials.

Multiple frameworks have developed best practice guidelines on implementing a security awareness program. First one was developed by PCI security standards council, which developed best practice guideline for implementing a Security Awareness program. Their focus with the guidelines is to formulate a security awareness team inside an organization, which will be responsible for developing in-house training materials. Similarly to Cyber Hygiene project, PCI guidelines involve different levels of content for different types of organization roles, for example: IT administrators, developers, and management. The approach is mainly technical and focuses on educating the users about security standards and best practices, for example: "Secure browsing practices". They do not focus so much on assessing the users' behavioral aspects and current situation in organization. [33]

Mäses developed an evaluation method [34] for human aspects of information, which was a low cost online framework to measures the participant's cyber awareness level and provides personalized feedback. The framework was developed using KAB model (knowledge, attitude, behavior). The framework is suitable for assessing individuals' cyber awareness level on 7 categories (Password management, E-mail use, Internet use, Social networking site use, Incident reporting, Working remotely and information handling). As he defines in his thesis, a proper evaluation method needs an underlying methodical principles – some sort of model that would provide it the conceptual basis and an overall structure. Thus, the developed framework works as a standalone framework but not in this thesis context. Due to the nature of the purpose of this thesis, the method is not considering 14 topics described in the Cyber Hygiene e-learning course, do not contain more deep guidelines on the statements design and biases that can be problematic on surveys. [34]

There are available many different training materials, frameworks and researches which are measuring the awareness, guidelines how to develop cyber awareness programs, courses which will educate users how to manage cyber security in their work lives, and

much more. Nevertheless, all of these guidelines and programs are focusing on separate areas and are lacking of systematic approach which would include all of the aspects like situation assessment and results assessment systematically. However, none of these does not match with Cyber Hygiene target evaluation goals, which would include user awareness and assessment of self-reported behavior together with assessing the understanding of the course materials. This is why a systematic approach to measure the user awareness and behavior before and after the course needs to be developed to fulfill the needs and scope of this thesis.

4. Methodical principles objectives

Subjects for social research may arise from the need to understand the relationship between an individual's experiences and the complex flow of actions of others in social environment [35]. These are usually things that trouble people in their lives. It is important to understand how these troubles take shape in organized social systems and how these affect our actions. Social sciences apply different scientific methodical principles to get the needed data. These include a variety of research approaches, tools, and techniques, such as qualitative and quantitative data, statistical analysis, experiments, field surveys, case research, and so forth. The selection of methods largely depends on the type of a problem and the kind of data needed to explain or solve the problem. Survey research can describe the attitudes and behaviors of selected representatives and soliciting their responses to a set of questions. Surveys are not used merely to describe, but also to explain studied phenomena. The aim of surveys mostly is to evaluate the presence and effects of various factors. To be successful any researcher has to carefully design a set of questions (questionnaire) and have a plan how to study these questions. Good research in social sciences depends also upon good measurement, which often depends upon careful and effective scale construction. The chosen response formats used in surveys depend on the type of questions being asked.

Research problem and objectives guide the selection of instrument format. For e-learning course to evaluate the acquired knowledge, the self-administered standardized test is most suitable and for online survey, measuring individuals' actual digital security behavior the questionnaire form is most appropriate. Both measurement forms allow to collect large dataset of information at the same time with relatively little effort. The differences between these two are in psychological attributes and broadness of the instrument. Test is classically an instrument based on competence which will reflect the ability to provide right answers to specific questions. It is the most suitable for gathering information about specific knowledge. Questionnaire is a broad method which includes set of different instrument types (e.g. scales, inventories). It can be effectively used to measure and assess behavior, opinion and attitude towards specific situation or topic. Both of them are used as a method that is administered without the involvement of interviewer/researcher and used to collect standardized data from large numbers of participants, which will spare

resources (e.g. time and money) and permits to collect the same information in similar way, therefore allows making generalizations based on collected information. [36], [37]

Questionnaire can be an effective mean of measuring individuals' behavior, attitudes, preferences, opinions and intentions. Tests are effectively used to measure individual's knowledge, skills or aptitude. Tests and questionnaires may be standardized, but can also be designed specifically for a particular study. The main advantages of the questionnaires and tests are: large amount of information can be collected from large sample with low time and financial consumption; results can be quickly quantified; allows to analyze the information more scientifically and objectively than other forms of research; quantified data can be used to compare and contrast other researches. The main disadvantages of the questionnaires are: there is no way to tell how truthful the participant is; how much effort the participant expressed towards the questionnaire; ambiguousness. Questionnaires can be carried out in different forms: face-to-face interviews, paper and pencil questionnaires and online questionnaires. On-line questionnaires provide more anonymity than other survey forms. Respondents also tend to feel safer providing honest answers in an online environment. Although the effect of social desirability is weaker on web questionnaires, one should not underestimate individual's desire to be viewed in a positive light. Therefore, when creating a questionnaire, one has to implement techniques for reducing social desirability (e.g. indirect questions, promising anonymity, employing face-saving strategies, etc.). [36], [37]

In order to provide legitimate results and fulfill the research purposes, it is vital to conduct the research methods in a best practice way and take under consideration all of the potential negative aspects (e.g. respondent bias, respondent error). As this thesis is using the questionnaire and assessment test as the assessment methods, the content of these methods need to be formatted in proper type and form, structural, as long and time consuming as needed and as short as possible, use the right measurement methods and types, unambiguous etc. [37]

5. Question types and requirements

In order to develop the evaluation method for the Cyber Hygiene e-learning course, it is important to take under consideration the existing approaches and solutions in the existing course prototype. As the prototype already uses questionnaire for behavior assessment and separate test for knowledge assessment, then the author builds current method upon existing solutions in the course. Existing questions in Cyber Hygiene course can be divided into three categories: the behavior assessing questionnaire, control questions and the test. Each of these have different purpose and requirements. Methodical principles characteristics of these three categories are described below.

5.1. Behavior assessment questionnaire

The goal of the behavior assessment questionnaire is to assess the employees understanding, attitude and self-reported behavior towards cyber security in their everyday lives. With this information the organization obtains an overview of their employee's real cyber security awareness level, behavior practices based on what can address their organization's weakness points, and plan countermeasures.

The questionnaire measures participants' present attitudes regarding cyber security topics and their self-reported behavior patterns towards cyber security in their everyday life. There are three main reasons for that need. First, users often acknowledge the threats, they know how to act in order to mitigate them, but for some reason they do not act accordingly – this can be because of the low motivation and the related attitudes, e.g. not fully understanding of the need and the beliefs that these threats might not affect them. Secondly, the users might be aware of the need and have high motivation in securing themselves, but do not know exactly how to act accordingly, e.g. do not have the technical knowledge and having technical skills based obstacles. Last, the users are not aware of the threats and do not have the technical knowledge on how to act accordingly, thus they cannot act correctly, e.g. no knowledge, technical skills. [38]

Although these kinds of actions may seem immaterial in individuals' personal life, it can be essential for an organization. If the organization is not aware of these behavior patterns, it is very hard or even impossible to ensure the organization security level [28]. In order to achieve the previously mentioned goals – acknowledgment of the need, assessment of the obstacles and thereby giving the organization a tool to map the issues, the questionnaire needs to complete the requirements described below.

5.1.1. Number of questions per topic

When developing a questionnaire, it is important to understand that the questionnaire needs to be long enough to get necessary information but short enough that it would not lose the focus of the respondent [39]. There is no one right answer how long the questionnaire should be. The length of a questionnaire mostly depends on the specific needs of an organization or a project. There are several important factors that should be taken under consideration when developing a questionnaire. They include questionnaire length, objectives, passing time, respondent burden and many more.

There is much research done about the effects of questionnaire length in on-line surveys, but the effect sizes in various studies range from strong to weak [39]. Elisabeth Deutskens found in their study about "Response Rate and Response Quality of Internet-Based Surveys" [43] that the response rate was higher when the questionnaire length was 15 to 30 minutes and lower when it was 30 – 45 minutes. But they also found that the length of the questionnaire did not have a negative effect on the quality of responses. The results revealed that longer questionnaire version (30 – 45 minutes) had more "Do not know" (midpoint answers) answers as well as more item non-responses, but the differences compared with shorter version were non-significant. Data shows that the longer a survey is, the less time respondents spend answering each question. This means that questions asked later in the questionnaire bear the risk of producing lower quality data [44]. These obstacles can be avoided if the respondents are well motivated and the topics under evaluation are important to them. The salience of a topic is one of the most important factors that influence the response rate and the quality [45], [46].

As current questionnaire is developed for organizational use and is part of a longer training program, the salience of the topic cannot be over-looked. It is much up to management to get their employees engaged in filling in the survey. And it is also known from number of studies that more engaged respondents tolerate longer surveys [46]. The second factor avoiding these obstacles is survey presentation [48]. Respondent-friendly surveys are easier to complete and thus reduce survey fatigue. The question type (e.g. ranking questions), the content involved, question wording and question ordering, and the length of the survey questions are all important when aiming for a respondent-friendly survey.

Respondent burden is an effort required by the respondent to answer the questionnaire. This is why the questionnaire cannot be excessively difficult. Another factor which affects the respondent burden is the number of the questions. The more questions the longer the questionnaire the more time and effort it will take for the respondent to finish the questionnaire. More questions do not definitely correlate always with higher accuracy of the results, at the same time the questions with right focus are much more likely to measure the topic of interest purposefully. [49], [50]

The last vital part of the questionnaire length is the clear objective. One of the most effective way to keep the questionnaire in a reasonable length is by having a clear objective, what and how the questionnaire is exactly going to gather the information and measure the results. 14 basic predefined Cyber Hygiene topics were used in creating a questionnaire in current thesis. As the main goal of the questionnaire is to evaluate the user's self-reported behavior then questions in every category need to contain behavioral questions. When developing evaluation method, it is important to keep in mind the uniqueness and experience of the users towards these topics. There can be situations where users are not exposed to certain devices or situations, the questionnaire needs to take this chance under consideration. Thus questions for every topic should take under consideration the potential number of users exposed to certain topic and devices and combine the behavior assessment questions with the theoretical fact based questions together. At the same time there can be situation where the topic is too broad and it is hard to ask relatable question, in that case only theoretical type of questions should be used. [51]

Taking under consideration the number of topics presented (14 topics), the uniqueness of the questionnaire objective (measuring self-reported behavior), the time constraint – (cannot be too long), and the respondent burden, the most optimal number of questions per topic is 3, which will make total of 42 questions per questionnaire. The estimated passing time of the questionnaire is ~20-30 minutes. In order to provide continuous legitimate results on assessing participants' behavior the questionnaire content needs to be static. This means that the questions will not change in the questionnaire, only in minor improvements. If there is a need to add topics or change questions entirely, then the whole questionnaire structure needs to be revised again.

5.1.2. Type and form

The types of questions used in a questionnaire will play an important role in producing unbiased and relevant responses. It is essential to know what is the exact purpose of a questionnaire and to use appropriate question types and forms in order to achieve the desired purpose. As the goal of this questionnaire is to measure the user's behavior, the form and the type of the questions have to support the measuring of user behavior. The question types and forms vary from direct and indirect questions to grammatical person views. Behavioral based questions are designed to assess the participant's behaviors — how the individuals act in everyday life and how this can affect the organization. Assessing how the individual handles situations provides valuable insight on how individual behaviors can influence an organization. In order to gather this information, the questionnaire questions should be unique, focused around the behavior aspects and use proper structure. Therefore, the questions need to be behavioral type questions which will directly ask how the participant has acted in a specific situation. [52], [53]

Although the main aim is to measure the individual's self-reported behavior it can occur that individuals have not exposed to certain topics or situations, thus cannot measure their behavior related to specific topic or situation. It is important to take under consideration that some topics can be less common among some individual's groups (example Internet of things in older generation [54]), thus the answers to the questions can be in negative manner. In order to take into account this situation, the behavioral questions should have either an answer option that the participant does not use specific device and/or service or additionally bind a theoretical knowledge based question with the behavioral questions.

This allows to assess the theoretical knowledge even if respondents lack of personal contact towards the specific situation.

One of the main types of questions used in questionnaires are direct and indirect questions. Direct questions are main clauses, whereas indirect questions are part of a larger matrix sentences. Direct questions are generally used to elicit information, which are also associated with characteristic intonation contours, which in turn are represented in standard orthography by a question mark. A direct question is usually marked by one or some combination of three signals: a rising intonation of the voice, an auxiliary verb inverted to a position before the subject, or an interrogative pronoun or adverb (who, what, why, when, how, and so on). The main advantage of the direct question is that it allows to ask specific situation related questions from the respondent. The author uses direct questions in the behavioral questionnaire, as the direct questions provide clear output for the participants. The direct behavioral questions come with some downsides – these are described in chapter 5.1.3 as respondent biases. [55], [56]

Next important part of the behavioral questionnaire is to combine direct type question with interrogative sentence and grammatical person. An interrogative sentence is a grammatical form which uses a direct question and always ends with a question mark. More precisely the questions grammar indicates that it is a question. Interrogative questions usually serve as YES/NO questions – which asks a question in a polarized way, waiting an answer as yes or no or WH questions – which use question words like who, which, how in order to ask the information. An example of an interrogative question would be: “Who has seen your smartphone?”. A second side of the question structure involves a grammatical person. Grammatical person is the grammatical distinction between deictic references to participants during an event. Typically, the speaker is the first person, the addressee the second person and the others the third person. In behavior assessment questionnaire it is important to ask direct questions from the respondent using the second person form to address the reader. As example, often used pronouns used with second person view are: you, your, yours. All the questions in the behavior assessment questionnaire are written in the second person form. [55], [57], [58]

5.1.3. Respondent bias

Respondent bias is defined as a systematic tendency to respond to a range of questionnaire items on some basis other than the specific item content, in other words it is a result of the respondent's inability or unwillingness to provide accurate or honest answers to the questions. The respondent bias is divided into 2 broad categories: response style and response set. [59] Response style is a situation where the respondent distorts responses to particular direction regardless of the content. The response set is a conscious or unconscious desire to produce a certain picture of oneself, to achieve certain goals, for example social desirability. The respondent bias is prevalent in types of studies that involve respondent self-report.

There are several strategies to limit and minimize the effect of the respondent bias, such as scale based answers and the randomized response technique. The empirical approach [60] was selected to develop the behavior assessment questionnaire. Based on 14 topics predefined by the Cyber hygiene standard, cyber security domains key features (outcomes) were worked out – behavior patterns that best reflected the right security behavior. With respect to each salient behavioral outcome, items were formulated to assess the understanding of right and wrong behavior. The development of questionnaire was based on Domain Sampling Theory. This theory states that if the object being measured has multiple components, or if a single object is being assessed using attributes that have multiple components, multiple survey questions are required [61]. By Domain Sampling Theory, human error is minimized by asking the respondents more than one question about each component of interest assuming that any error will average out over multiple questions [62] in order to minimize the response bias. [63]

The most suitable strategy for the behavior assessment questionnaire discussed in this thesis is the forced choice items which will be combined with scale based answers. Forced choice items are effective, because they force respondents to choose an answer which indicates a definitive option, in turn will eliminate the "Do not know" response options because these are designed to force the participant to express an opinion or attitude. Forced choice items can also significantly reduce the impact of numerous biases. For example, uniform biases such as acquiescence responding and can increase operational validity by reducing ''halo'' effects [64]. Another reason why the forced choice items are

useful is because the behavioral questionnaire will be passed online. Using forced choice items, allows to save a lot of effort and time on analyzing the results and administrating the course. [63], [65]

5.1.4. Answers

The answers in the behavior assessment questionnaire need to reflect individual's potential behaviors in their everyday life. The answers have to be as accurate and honest as possible. Additionally, it is important to take under consideration the respondent bias where the respondent might not provide honest answers. In order to mitigate the occurring of respondent bias, the author uses forced choice items together with scale based answers for the behavioral questionnaire. A rating scale was selected to measure cyber security behavior in order to minimize the respondent bias. Rating scale offers respondents the opportunity to select a response among several possibilities arranged in hierarchical order [66]. A rating scale with 4 response options was used. Rating or frequency scales use fixed choice response formats and are mostly designed to measure behavior, attitudes or opinions [67]. The list of response options has to cover all possible response options. With 4-option rating scale the options were restricted to 4. For further analysis, the response options were quantified with numerical values (1-4). In the rating scale 1 stands for completely incorrect behavior, 2 stands for incorrect behavior, 3 stands for correct behavior and 4 stands for absolutely correct, even ideal behavior. This ordinal rating scale measures behavior from completely incorrect to an absolutely correct and is assumed that the intervals between the rankings are equal and will eliminate the neutral answer in order to be easier to measure the results.

In some of the domains, the "not applicable" answer options were offered as some questions may not be relevant to all respondents (e.g. not everyone owns a social media account). Every security topic in the course is measured with three questions where the results are summarized. For feedback on organizational level, frequency distributions are created for each domain. For individual feedback, ranges were calculated pursuant to the principle of normal distribution. Individual feedback is effective incentive that can affect the motivation and answer quality of respondents [68]. On problem with rating scales is that they can lead respondents to positive evaluation or to the most correct answer. Acquiescence bias is a form of response bias where the survey respondents have a tendency to agree with all questions or indicate a positive connotation [69]. To prevent

the acquiescence bias the answers in the questionnaire were not listed in logical order, but the answers were presented in a random sequence.

5.1.5. Measuring the results

There can be several measurement errors in different self-administered questionnaires due to respondents lack of motivation, comprehension problems, etc. In order to minimize the respondent error, the questionnaire instrument must be easy to understand and complete. While the importance of question wording in influencing respondent answers is well recognized, many researchers suggest that the design of the questionnaire instrument (e.g. placement of questions etc.) also play important role. Researches have shown that unintended design or layout changes can affect the responses obtained both in interviewer-administered and in self-administered surveys. [70]

The main goal of the behavior assessment questionnaire is to measure the real behaviors towards cyber security, of the users (e.g. if they exchange confidential work information in social media or if they use personal devices at work). The entire questionnaire structure needs to support that goal. As mentioned in chapter *5.1.4 Answers*, a rating scale with 4 response options was used. Rating or frequency scales use fixed choice response formats and are mostly designed to measure behavior, attitudes or opinions. The list of response options has to cover all possible response options. With 4 option rating scale the options were restricted to 4. For further analysis, the response options were quantified. The measurement is based on the ordinal rating scale, which measures the self-reported behavior from completely incorrect to a completely correct and is assumed that the intervals between the rankings are equal and will eliminate the neutral answer in order to be easier to measure the results. Additionally, some questions also contained a fifth answer, as an exception. That implies that the user has not exposed to specific situation or do not own specific devices – 0. In this thesis, the respondents who used the 0 as an answer were excluded from the statistical results for specific topic, because in order to trustworthy measure the results, the user needs to provide three answers per topic.

The participants were divided into 4 groups based on their answers on the scale from one to four. The groups were calculated based on the summary characteristics. In order to do that, the author compounded all the answers' numerical values for every user together per topic and divided the respondents into 4 groups based on their scores. The minimum number of points per topic in the analysis was 3 and the maximum 12. The main initiative was to provide an employee's cyber security behavior assessment to the organization, which showed the level of every topic in the course. Corresponding pointing scheme is described in the Table 1. For the group division the author used normal distribution, which defines the numerical step between groups as in the middle larger step and in the sides smaller one. Normal distribution is an important characteristic in statistics which is often used in natural and social sciences. In general, about 68% of values drawn from a normal distribution are within one standard deviation away from the mean. The author calculated 4 response range groups per topic, based on normal distribution. This means that usually very high results and very low results are rare, main results will be in the middle. This follows from the normal distribution which is used in live and social sciences. Based on this, the middle score will be 68% (2x34%) and extreme scores 16% each. [72]

Table 1. Pointing scheme for the behavior assessment questionnaire.

Types	**Numerical range**	**Percentage**	**Step**	**Numerical range (rounded)**
Completely incorrect	3-4.44	16%	1.43	3-4
Incorrect	4.45-7.50	34%	3.05	5-7
Correct	7.51-10.56	34%	3.05	8-10
Ideal	10.57-12	16%	1.43	11-12

In order to measure the results of the questionnaire and get a better overview of the topics, the author has analyzed 14 topics in the course and divided them into four bigger groups, based on their characteristics: Malicious websites and information sharing, access to the information, human behavior, network and physical devices. Exact distribution is provided in *Appendix 1 – Topics distribution*. This classification helps to assess the organization situation from a broader angle. All of the results are provided firstly in the 4 general topic groups and separately in 14 specific topics.

It is recommended by the Cyber Hygiene standard that the e-learning course, thus the behavior evaluation questionnaire should be conducted twice on the same participants. The aim of the first time conduct of the behavior assessment questionnaire is to find out the baseline security behavior in any organization. The answers will reveal how prevalent any problem and positive tendency concerning security behavior is in given organization. Measured baseline behavior is the standard against which the organization will measure all subsequent changes implemented by any digital security improvement program. Experts generally consider determining baseline measures of behavior to be the first phase in any sort of behavior modification program, followed by implementation of the program and finally a follow-up phase in which the results are measured and analyzed. When conducting the course on the same participants second time, it becomes possible to compare the results with baseline behavior (to see if and how much the behavior patterns have changed) and evaluate the effectiveness of training.

5.2. Control questions

A question is a type of a sentence that is expressed in a form that requires (or appears to require) an answer. A question is generally distinguished from a sentence that makes a statement, delivers a command, expresses an exclamation [73]. Using questions as a teaching method is an age-old practice and has been a cornerstone of education for centuries. Questions have been long used as a teaching method to assess students' knowledge, promote comprehension and stimulate critical thinking. Well-crafted questions lead to new insights, generate discussion, and promote the comprehensive exploration of subject matter. Poorly constructed questions can stifle learning by creating confusion, intimidating students, and limiting creative thinking. [75]

The second category of questions are presented in the Cyber Hygiene course right after the videos (in the main module). These control questions are used as teaching method, fulfilling the role of teaching the concepts. More precisely, the control questions explain the wrong behavior related to the topic. The content of the question is mainly related to the video or to the similar situation described in the video. It is important to keep in mind, that the video will describe the wrong behavior and the user will answer the questions based on his or her existing knowledge, because one has not passed the informational part of the course yet. Thus the answer cannot be evaluated, because the question is used as

teaching method and not as knowledge assessment. Right after the participant has answered the control question, the system provides the right answer with explanation. This makes the course learning process more interactive. [74]

5.2.1. Number of questions per topic

The control question has a supportive and instructive role in the course. Taken under consideration of time aspect and the goal of the question, it is important that the main module cannot take too much time for the participant to finish. That is why the author uses one question per topic in the course. As the course contains 14 different topics it makes 14 different control questions for the main module. Otherwise, if the course contains more control questions then the overall module passing time will increase and the participant's attention will fade, resulting with inefficient results.

5.2.2. Similarity

The control questions and final test has a common core: both of them are used for learning purposes. The main difference relies on the output. Control questions are used as teaching method, which defines a problem and helps the respondent to understand the problem. Followed by the exact explanation of the wrong behavior. The final test, on the other hand, uses similar characteristics but is assessing the final understanding of the material. The final test will provide an output which states whether and to what extent the user has acquired new concepts. Although both of these question type outputs vary a little, they are created using the same principles, thus making them similar. Because the question creation methodical principles are almost the same for the both of these question types, the remaining part of the control questions methodical principles are described in chapter *5.3 Test*.

5.3. Test

The third and final category of questions in the Cyber Hygiene e-learning course are knowledge assessment questions. Knowledge assessment test is an assessment method, which measures the participant's knowledge, skill or aptitude towards specific topic. Test commonly refers to a set of items or questions under specific questions [75]. The main intention of the test in this course is to assess the participants understanding of the learned materials. The test will give an overview, whether the participants have acquired and understood the new information and concepts from the course or not and to what extent. The knowledge assessment test is the last part of the e-learning course.

In general, there are five main types of tests: Multiple-choice, true-false, short answer, completion and matching tests. Multiple-choice tests are quick and easy way to score and conduct electronically, can cover lots of content areas with a single test. The downside is that it is time consuming to generate good questions. True-false questions are quick and easy to score, but are considered as the most unreliable forms of assessment. Short answer questions are easy to write and grade, but the understanding often remains superficial because the size of the questions and answers. Completion usually requires the respondent to answer or finish an incomplete statement by filling a blank with the correct word or phrase. It is more time consuming to score when compared to multiple-choice or true-false items. Matching type items consist of a column of stimuli presented on the left side of the page and a column of responses the other side of the page. Participant is required to match the responses associated with a given stimulus. This type has difficulty measuring learning objectives requiring more than a simple recall of information. [76], [77], [78]

Given that the Cyber Hygiene e-learning course is an online course and consists of a many materials and will have a large amount of participants, the most efficient processing and teaching method needs to be selected. Therefore, the most suitable choice is the multiple choice test. Multiple choice is an assessment form, which provides a participant a list of potential answers, where the participant needs to select the best possible answer or answers from a choices list. This format is mainly used in educational testing. This allows to develop an online course with automatic assessment and reduces different biases, which as a result provides reliable results and is cost and time efficient. [76]

5.3.1. Number of questions per topic

The main goal of the final test is to measure the understanding of the concepts described in the Cyber Hygiene e-learning course. Based on the principles described in chapter *5.1.1 Number of questions per topic*, the main concerns of the test are the length of the test and the passing time. Thus, the author uses the same number amount of questions described in behavior assessment questionnaire chapter. The final test will consist of three questions per topic, together 42 question per course. This allows the optimal passing time of the test and accurate results. Although one set of questions per respondent session uses 42 unique questions, the author raises the final test questions volume significantly. This allows to provide more unique questions for every respondent session. The next version of the e-learning course will include a functionality which chooses randomly three questions from predefined set of questions for every topic. This functionality raises significantly the scalability of the final test. The same approach applies also to control questions, only with difference that the system will choose one question from predefined question list. The scalability of the course is vital in order to be sustainable, because the course should preferably undergo at least once a year [29], and if necessary, even more often. With larger variety of questions, every participant will get more unique questions every time they take the course.

5.3.2. Method

A multiple choice question is composed of two parts: a stem which identifies the question or problem, and a set of alternatives or possible answers which contain a key that is the best answer to the question, with number of distractors that are plausible but incorrect answers to the question. Often stem consists of extended or ancillary content like vignette, case study or a graph. Stem usually ends with lead-in question with instructions on how the respondent should answer. Example of a lead-in question would be: “Which of the following is true:”. [79]

Psychological science methodologists tend to use a variety of methods to develop and refine questions, surveys, tests in order to provide unambiguous and relatable content for the participants. One effective method to use when assessing the participants’ knowledge is vignette [80]. Vignettes have been used a long time in social sciences for researches. Vignettes are brief stories or scenarios that describe hypothetical characters or situations

to which a respondent is asked to react. Because vignettes embody hypothetical situations, they offer a less threatening way to explore sensitive topics. Their peculiarity allows contextual influences on judgments to be inspected. To preserve realism, researchers often create vignettes based on realistic situations. Although vignettes typically contain detailed descriptive information, they may vary in degree of elaboration. [81] Incorporating vignettes can be difficult, because it is vital to keep the length of a vignette as brief as possible. This way the participant will not lose the attention. When developing vignettes, it is important to include as much detail as possible. Vignettes can be developed in different ways and for different purposes. Main differences between vignettes are: whether they are used as an independent method or a complement to other research techniques; how the story or situation is presented; at what stage in the data collection process they are introduced; how responses are structured. Nevertheless, vignettes generally fulfill three main purposes: interpretation of actions and occurrences that allows situational context to be explored and significant variables to be identified; clarification of individual judgments, often in relation to moral dilemmas; discussion of sensitive topics or experiences comparing to the ‘normality’ of the vignette. [82], [83]

Main principles of developing vignettes [83], [84]:

- Stories must appear believable and be as realistic as possible to participants. This means that the vignette needs to be relatable for the participant. Some researchers have constructed their vignettes around realistic experiences, either directly, for example by using situations provided by participants in the pilot stage of the research.
- Stories need to avoid depicting eccentric natures and disastrous events.
- Vignettes need to contain sufficient context for respondents to have an understanding about the situation being described, but be vague enough to force participants to provide additional factors which influence their decisions.
- It is important that the stories presented in the vignettes are easily understood, internally consistent and not too complex. Research has found that more than three changes to a story line was often proved to be too confusing for participants to remember.

The Cyber Hygiene e-learning course prototype is already using vignettes in the form of videos. It is very effective way to describe wrong behavior in a situation for study purposes. The author uses vignette's in the control questions and final test questions, because using vignettes is an effective way to describe a difficult situation or topic to the participant, and thus makes the questions more unambiguous. Research has shown that for respondents it is easier to assess the behavior of other people as their own. Thus providing more honest and precise answers. [84]

5.3.3. Type and form

The test is assessing the participants understanding of the concepts described in the course. In order to produce trustworthy results, the type and form of the questions plays an essential role in the test. The final test consists questions about the topics described in the course. The test questions need to be either factual or theoretical and straightly related to topics and facts in the course. A factual or theoretical question offers a theoretical situation and asks for respondents' opinion. It is important not to use behavioral type of questions in this test, because all the questions per category need to follow the same principles and be similar, also the behavioral question could introduce problems where the user has not exposed to specific situation or device.

As mentioned in the chapter *5.1.2 Type and form*, questions are generally divided into two broad groups: direct and indirect. Direct questions are generally used to elicit information and indirect question or declarative sentence is a question where the question is embedded inside a statement or another question. Example of indirect question would be: "Tomas has not decided yet, which computer he should buy.". As the final test uses vignette's and describes a situation for the respondent, there cannot be used a direct question, thus the final test needs to apply indirect questions together with third person viewpoint. As mentioned in the chapter *5.1.2 Type and form*, the grammatical person is the distinction between deictic references to participants during an event. As the final test uses vignettes to tell a story about a situation, it is more effective to use the third person form together with vignette. The third person form gives a better opportunity for the respondent to evaluate others' behavior or different situations, which the respondent would be doing more likely than answering random questions about facts. [85], [86]

5.3.4. Answers

The final test uses answers as a tool to assess the participant's knowledge. As discussed previously, the final test uses multiple choice items. When writing multiple choice answers it is important to keep in mind that proper multiple choice answers need to include only one right answer and multiple wrong answers. The wrong answers need to include enough distractions in order to make it more difficult to guess the right answer. The distractions may have an element of truth on them, this will make a more difficult for the participant to guess the right answers. It is vital to limit the number of alternative answers, because previous research has shown that three-choice items are about as effective as four or five choice items, mainly because it is difficult to come up with plausible distractors. Thus the author uses three alternative answers in addition to the right answer. [87]

Sometimes the respondents are not able or do not want to answer questions as provided by the test. This can occur due to lack of motivation or attention. In order to avoid the "bingo option", where the respondent chooses the answer randomly, the author has added an alternative answer to the test: "Do not know" [88]. The answer is evaluated as wrong answer, but it gives a respondent an alternative choice of answer, if for some reason they cannot choose the right answer. [89]

The answers in multiple choice item questions can vary but they need to be the same amount through the module. In final test, the author used five answers per question: right answer, three wrong answers and do not know answer. Additionally, the final test uses similarly to behavioral questionnaire, the answer sequence randomization, in this way it is harder for the participant to befall the right answer. [90]

5.3.5. Measuring the results

For the final test assessment, the author used TUT unified grading system [132], which is approved by the Estonian Minister of Education, as the basis for the final test assessment. In this grading system the minimum positive answers percentage for passing is 51% (sufficient). Due to the characteristics of the topics covered in Cyber Hygiene e-learning course, the nature and importance of cyber security in workplace and the fact that the course consists of basic cyber security principles and practices the author raised the minimum passing percentage to 71% (good). As the 14 topics in the course are all important and will create a common knowledge core of the basic principles of cyber security behaviors and in order to avoid a situation where the participant will pass the course but totally fail in some specific topic the author added second aspect to the grading scale: the user needs to have at least one right answer for every topic. This will confirm that the user has passed at least 71% of the course and have acquired new knowledge from every topic. The grading scale used for the final test assessment is described in *Table 2*.

Table 2. Test assessment grading scale.

	Percentage	Points	Description
Pass	91-100%	38-42	Proficiency in applying skills and knowledge as well as being able to prevent situations.
	81-90%	34-37	Proficiency in applying skills and knowledge in situations described in the learning context. Some details of knowledge and skills may exhibit errors which are neither substantive nor serious.
	71-80%	30-33	Good proficiency in applying skills and knowledge in situations described in the learning context in a relevant manner. A certain imprecision and lack of confidence are apparent in the depth and detail of knowledge and skills which may exhibit errors.
Fail	61-70%	23-27	Knowledge and skills are superficial and below minimum standard which exhibit errors.
	51-60%	18-22	
	0-50%	0-21	

The test questions contain 5 answers: 1 right answer, 3 wrong answers and a "Do not know" as an answer. Only the right answer will give a point (1), all other answers will give no points (0). Based on this logic, the author will calculate numerical scores per every topic in order to assess the results of the test.

5.4. Questions and answers in general

A question is a linguistic expression, which is used as an effective instrument for conducting different researches, studies and tests. Often, researchers use series of questions and prompts with the goal of gathering information from the participants. Adequate question structure is vital to the success of the research. Although the most important part of the question is the topic it involves, the inappropriate questions, incorrect scaling or bad format can have bad effects on the research or even change the questions utterly useless. [92] In question generation process it is important to take under account different key points. Main key requirements which affect all of the question categories in this thesis are described below.

5.4.1. Form

Through the thesis the author used closed type questions. Closed type questions are appropriate for online questionnaires. The data can be quickly obtained, as closed questions are easy to answer. All respondents are asked exactly the same questions in the same order. This means a questionnaire can be replicated easily. Closed questions structure the answers by allowing only answers which fit into categories that have been decided in advanced. Closed questions provide information which is easily converted to quantitative data and provide reliable measurement.

In general, the questions can be divided into two broad categories: closed-ended questions and open-ended questions. Closed-ended questions' main purpose is to limit the answers of the participant to response options provided by the question. The purpose of the open-ended question is give participant an opportunity to provide their own answers in free form, since there are no predefined options included. The main advantage of the close-ended questions are that the respondent is restricted to a finite set of responses; easy and quick to answer; have response categories that are easy to code and they permit the inclusion of more variables in a research study because the format enables the respondent to answer more questions in the same time required to answer fewer open ended questions. The closed ended questions are questions where is given list of predetermined responses from where the respondent can choose the right answer. The list of answers usually consists of all the variations of answers. This is often used for quantifying answers and to compare the levels or frequency across respondents. The response format for closed questions can range from a simple yes/no response, to an approve/disapprove alternative, to asking the respondent to choose one alternative from 3 or more response options. [93], [94]

All question categories presented in this thesis are close-ended questions, because the course will be conducted over the Internet, which needs automatic assessing and administering methods – will be a lot quicker through predefined questions, also this type of question will not leave much room for unambiguous questions, since it will force the user choose from predefined answers. Close-ended questions distribute into multiple choice questions and data or scale based questions. Multiple choice questions are providing predefined different answer versions which from the respondent needs to

choose from. In scale based questions, respondents are provided with different intensity level questions from where the respondent needs to choose the most suitable answer. Both of these types are presented in this thesis. Behavioral questionnaire uses scale based questions and control questions with final test uses multiple choice questions. [94]

The unambiguous questions have one main possible interpretation of what the question can mean. At the same time ambiguous questions can have more than one possible interpretation, main reasons for ambiguous questions are: Bad structuring of the question, bad choice of vocabulary or the question relies on external content which is absent. In order to develop an unambiguous and clear questions one needs to avoid uncertainty and general and ambiguous words like often, usually, many and general. In order to develop unambiguous questions, it is vital to provide clarity in the them. In order to provide effective clarified questions, it is important to use examples where possible and avoid too specific abbreviations. [39] All the questions in every category in this thesis need to follow similar format through their module. This means that all of the questions for every module need to use their category specific methods for formatting and presenting the questions. For example, if one question is written from third person view and asks the respondent opinion in some situation, then other questions in the same module should be similar if possible. This will provide more unambiguity and intelligibility through the course.

The examples and focus points of the questions need to be in general form. For example, it is bad practice to ask question about “Facebook” under the social media category, because users may use social media, but not exactly Facebook. The questions need to be developed in a general format which contain the main principles and ideas of the field, not specific brands. The general form makes the questions more scalable. For every question in the course, all of the answers need to be with similar length and complexity as possible. Otherwise it is easy for the respondent to figure out the potential right answers. Additionally, the weight of the answer content should also be as similar as possible through different answers, this does not allow to easily guess the right answer.

5.4.2. Content

The course is based on 14 different topics on which the generated questions need to be based on. In the course curriculum only main aspects of every topic are defined, which means that many of them are probably missing. The 14 topics are static and cannot be changed, as defined in chapter *2.3. Defining the limits*, but the subjects for every topic can change, be added or removed. When developing the questions, one may found that there are many important subjects missing from certain topics, then it should be definitely added to the course. The subjects need to be as specific as possible. Need to avoid general problems. One important aspect of the content of the questions are the impact and frequency. The impact on how large amount of people are affected by the problematic situation, action or threat described in the questions. The questions need contain topical situations which have affect on large amount of people and need to be more frequently happening problems.

Although the Cyber Hygiene consists of three different level e-learning courses: regular users, specialists, managers, this thesis focuses on the regular user course as the basic course needs to be finished by all the members of the organization (including specialists and management). Thus the target group of the course is addressed by this thesis is regular users. Regular users are considered as all members of the organization who are using computers and computer systems for their everyday work. The course will give an understanding of a basic cyber security level for the organization users which presumably will deliver a good cyber security level for the organization. Thus all the content of the course needs to contain only basic complexity security principles. The basic complexity security principles comprise of minimum level of identification of the main threat vectors that are major sources of concern, areas of human risk behavior, threat vectors and so on. The complexity level of the multiple choice answers needs to be as similarly structured to avoid too easily predictable right answers.

The course is focusing on improving the basic cyber hygiene level on organizations by educating the employee's. The focus is not so much on regular home user, although it is important to understand that these two worlds are very closely related. From psychological aspect, the behavior patterns and attitude towards security usually transfers from personal life to professional life. Thus all the content in the questions need to be from the organization viewpoint. It needs to influence organization directly or indirectly.

5.4.3. What to avoid

Leading questions are questions which are deliberately designed in a way which will influence the respondent to think certain way. Leading questions can either include the right answer, point the respondent to the right direction or include form to send them into right answer. Leading questions often use linked statements, implication questions, ask for agreement and assumptions. For example: “How much will prices go up next year?” This statement assumes that the prices are going up next year, this is forcing the respondent to think about if the prices will go up. [95]

The properly generated questions should avoid using contractions where possible. The contraction is a shortened form of a phrase, word, syllable which is formed by omitting certain letters or syllables and assembling the first and last elements. Example of a contraction is: “don’t, can’t, won’t”. The contraction should be avoided because there can occur a situation where the respondent does not fully understand either the question or the answer because of the contraction. [94]

It is important to use proper and clear wording when generating questions. One needs to avoid complex wording which can be hard to be followed by the respondent. That is why the questions need to be easy to understand and easy to answer. Questions should contain words that have the same meaning for the general public as the survey specific field. Additionally, this is important to avoid the use of slang and use terms consistently throughout the questionnaire. This means that every word is always used to convey an identical meaning. When using more than one term to refer to specific thing can confuse the respondent and resulting with wrong answers. [96]

It is a phenomenon where the question consists two questions in one. This approach is problematic because it asks the respondent to give one answer for two entirely different questions, although the answers are often only for one question. This can be problematic because the respondent may understand the question ambiguous way and the measurements of the questions may result inaccurate. Example of a double barreled question would be: “How far would you be willing to drive for dinner and movie?” [96]

When developing the answers for the multiple choice questions, it is important that the answers are mutually exclusive and exhaustive. In other words: it is vital that the answers should not overlap and cover all possible answers to the question. It may seem straightforward but this is not always the case. In case of response overlap, it remains unclear for the respondent, on which of the answers is the right one. [97]

Example of response overlap: Question: Approximately how many employees work in your organization?

- 1-100
- 100-200
- 200-300

The answer capacity will determine what one can do with and conclude from the collected data. If the response is merely yes/no, then one may know only of what percent answered yes/no to the question. But if we are interested more specifically, how user understands, what are her user behaviors and so on, then it would be more effective to use full sentence's as answers, which will give a better overview of the answer. [39]

If the answers in the questionnaire are too distinguishable from the other answers, it is very easy to capture the obvious right answer. In multiple choice questions, at least the right answer should have one similar answer, which would make it harder for the respondent to capture right away the right answer. [39]

6. Questions' generation

The author conducted the questions volume raising in three stages: The behavior assessment questionnaire, the control questions and the final test. Together, the author developed 200 unique questions based on developed evaluation method which is used in the Cyber Hygiene course.

Stage 1 – Behavior assessment questionnaire. Based on developed evaluation method, the author created 42 unique questions for measuring the participant's behavior patterns together in 14 different topics with 3 questions per topic.
Stage 2 – Control questions. Based on developed evaluation method, the author created 34 different control questions for the 14 topic in the course. Control questions are used to support the learning process.
Stage 3 – Final test. Based on developed evaluation method, the author has generated 124 unique questions for the final test. The questions are divided into 14 different topics. The final test evaluates the participants acquired information.

Due to the large volume of the developed questions (200) and legal restrictions based in agreements with BHC it is not possible to add entire list of all the questions to this thesis. Therefore, the author has added samples of questions from every topic. The examples of the questions are presented in the appendixes: *Appendix 2 – Behavior assessment questions, Appendix 3 – Control questions, Appendix 4 – Test questions*.

7. Questions' evaluation

When developing materials for any kind of educational materials, it is essential to consider several important aspects: method, goal of the materials, scientific value, quantity of the materials, scalability and so on. As all of these aspects are vital in order to achieve educational objectives, it is a good practice to do pilot testing on different audiences, in order to get indispensable feedback to improve and raise the trustworthiness of the educational materials. Therefore, the raw questions, based on developed method, are validated by cyber security experts and pilot tested on test audience. The goal of the validation and piloting was to verify whether the questions' content is legitimate, whether something needs to be added or removed from the questions, whether the participants understand the questions properly, and whether the method provides expected results through the questions.

The author has conducted the evaluation process in two parts: the cyber security experts' evaluations and the pilot test. The experts evaluated the developed questions legitimacy and gave an overview of the quality of the questions' content. The pilot study of the questions was conducted on undergraduate IT students form TUT, who completed the prototype course with newly developed questionnaire, control questions and test questions. Additionally, the author asked qualitative feedback from the students to assess the course structure and to improve the questions.

7.1. Experts' evaluation

The author asked security experts to assess the quality of the three parts of the questions. The purpose of the questions validation by the security experts was to verify if the questions are relevant to specific topics and if something needs to be added or removed from the questions. The feedback from the security experts was overall positive. Experts suggested some wording improvements and to use more examples where possible. For example, if the question describes situation about social media, then it should provide more examples of social media: Twitter, Instagram, Facebook, etc. Additionally, when talking in general terms, the question should involve specifications. For example, in topic related to Open Wi-Fi and Shoulder surfing, it is important to make difference between Shoulder surfing related threats in places where are lots of people and places where one

may be alone when using Open Wi-Fi, for example hotel room. Experts also pointed out couple of questions which expect previous knowledge about context. For example: “When do you have opened strange attachments from work e-mails? Choose the answer that you think is the most accurate.” - expects a knowledge related to potential threats like phishing and expects that the respondent will evaluate the trustworthiness of the e-mail sender and verify of the contents of the e-mail. Experts confirmed the questions accuracy, connectedness towards topics used in the course and pointed out that from the questions it is clear the target audience: average computer user, who does not have many cyber security related skills. In general, the feedback was positive related to topics and questions used, the questions were well thought-out and related closely to the covered material and fulfill the purpose of assessing the behavior and learning process. The suggested observations were taken under consideration and corresponding changes were made in the questions.

7.2. Pilot

The second part of the evaluation was conducted as a pilot test. The pilot was conducted in collaboration with TUT and BHC. The author provided newly developed 200 questions (based on the evaluation method described in this thesis) to BHC, who replaced the old questions with the new ones and provided a test environment. Author conducted the pilot on a sample group of 69 TUT undergraduate IT students. All three parts of the course (questionnaire, main module with control questions, and final test) were conducted in succession. Due to technical issues, it was not possible to add newly developed control questions to the existing course and it was not possible to use randomization functionality when choosing the test questions, however the behavior assessment questionnaire and final test were successfully added. As the author is not measuring the control question results, because it is used as a study method in the course, then it was not vital for the first pilot to use control questions as the old questions were presented.

The average time to finish the entire course was 112 minutes. In average the behavior assessment questionnaire took 26 minutes to finish, the main module with videos, control questions and learning materials took 44 minutes and the final test took on 41 minutes to finish. As the whole course passing time is almost 2 hours, it would be beneficial to consider a possibility to split the course into two days (day 1 – behavioral assessment

questions; day 2 – main module and test) in order to save time and minimize the respondent burden. It is important to note that the passing time can vary between participants, the shifting factors could be age, language skills, technical understanding and motivation. As expected, main module was the most time consuming to finish, following by test. The behavior assessment questionnaire took about 1/3 less time to pass (see *Figure 1*).

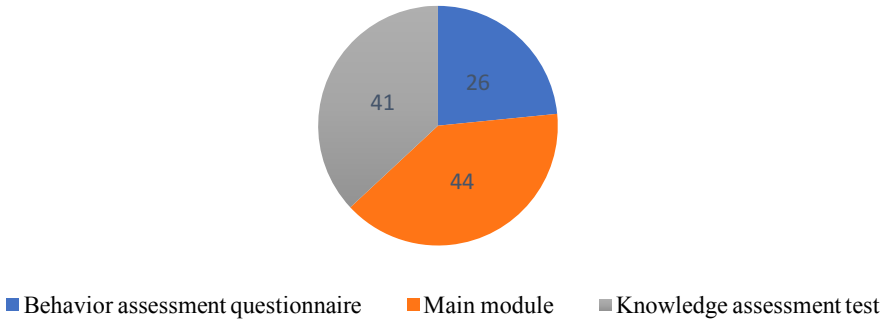

Figure 1. Time distribution (minutes).

7.2.1. Behavior assessment questionnaire results

For the behavior assessment questionnaire results measurement the author created 2 of 4 divisions: Groups based on interval values and groups based on topics.

Groups based on interval values: each question in behavior assessment questionnaire contained four answers (two correct and two incorrect behaviors). Based on previously mentioned values or behavior intervals, the respondents were divided by their responses into four interval groups per every topic on the accuracy of the response. The interval groups were created based on the answer numerical weighs which in turn were divided into two larger interval groups: incorrect behavior and correct behavior. This approach allows to have an overview whether the respondent practices correct or incorrect behaviors. The results were assessed based on 14 topics in the course. As the course involves many different types of topics, the 14 topics were distributed into 4 bigger topic groups in order to provide more general overview of the respondent's behavioral level: Malicious websites and information sharing, access to the information, human aspects, network and physical devices.

Groups based on topics: based on the first pilot, the participants were divided based on their behavioral answers into 4 topic groups (distribution of topics into groups are described more precisely in *Appendix 1 – Topics distribution*): where the group with the most correct answers was "Malicious websites and information sharing". This group contained 91% of respondents with correct self-reported behaviors. The weakest group, i.e. with the least correct answers, was "Network and physical devices" and contained 65% of respondents with correct behaviors. The precise answers distribution between 4 groups are described in *Figure 2*.

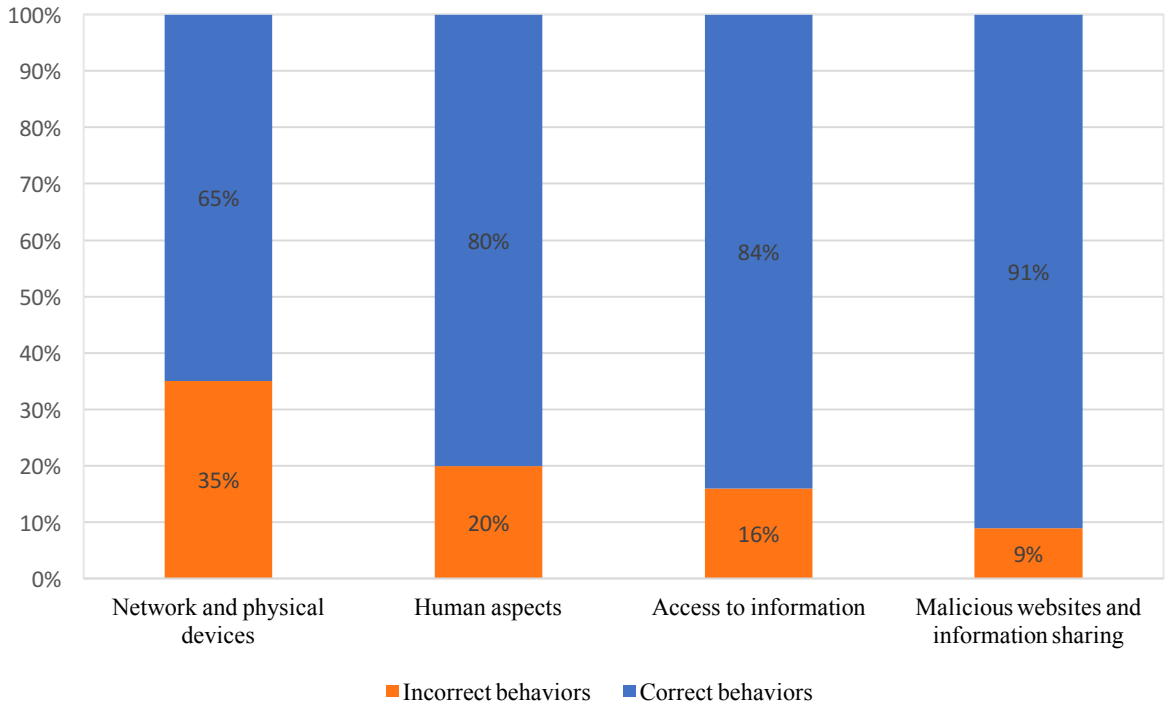

Figure 2. The behavior assessment questionnaire results distribution between 4 groups.

The questionnaire contained 14 specific topics, from the 14, the topics towards which the respondents had the most correct behaviors are: Social networks – 62 respondents (90%) with correct behaviors and one user did not own any social media accounts; E-mail related risks – 63 respondents (91%) with correct behaviors; Harmful websites – 60 respondents (91%) with correct behaviors and two respondents did not own personal computer. The topics towards which the respondents had the most incorrect behaviors are: Bring Your Own Device – 38 respondents (55%) with incorrect behaviors; Open Wi-Fi – 24 respondents (59%) with incorrect behaviors; Password risks – 17 respondents (25%) with

incorrect behaviors; Bad identification culture – 17 respondents (25%) with incorrect behaviors. The precise distribution of results per topic are described in *Figure 3*.

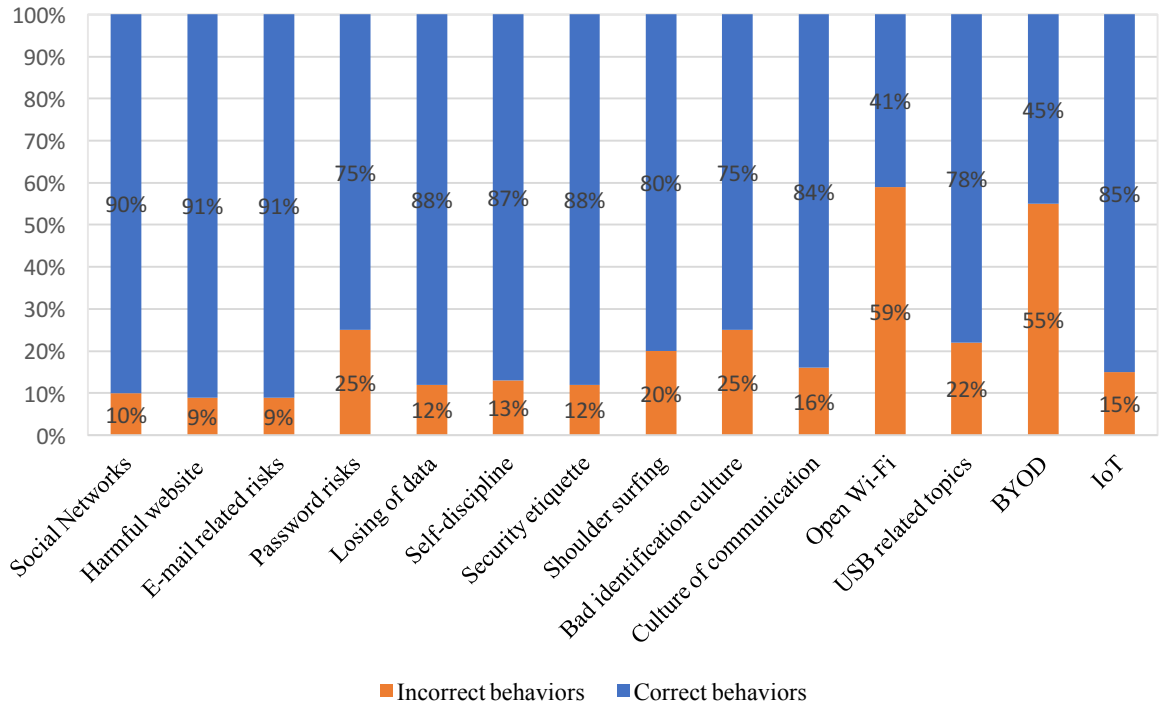

Figure 3. Behavior assessment questionnaire results per topic.

As presented in *Figure 4*, the behavior assessment questionnaire results approved that the "0" option as answer, which meant that either the participant does not have specific device or is not exposed to specific situation, is vital for this questionnaire. For the entire behavior assessment questionnaire, the "0" answer was used 33 times. Mainly, "0" value responses were provided by the users who do not own a social media account or do not own personal smart devices. One of the question got 28 responses with "0" value. The question was related to using public Wi-Fi for work purposes. The results were legitimate, because the participants are undergraduate IT students and not all of them have a job yet.

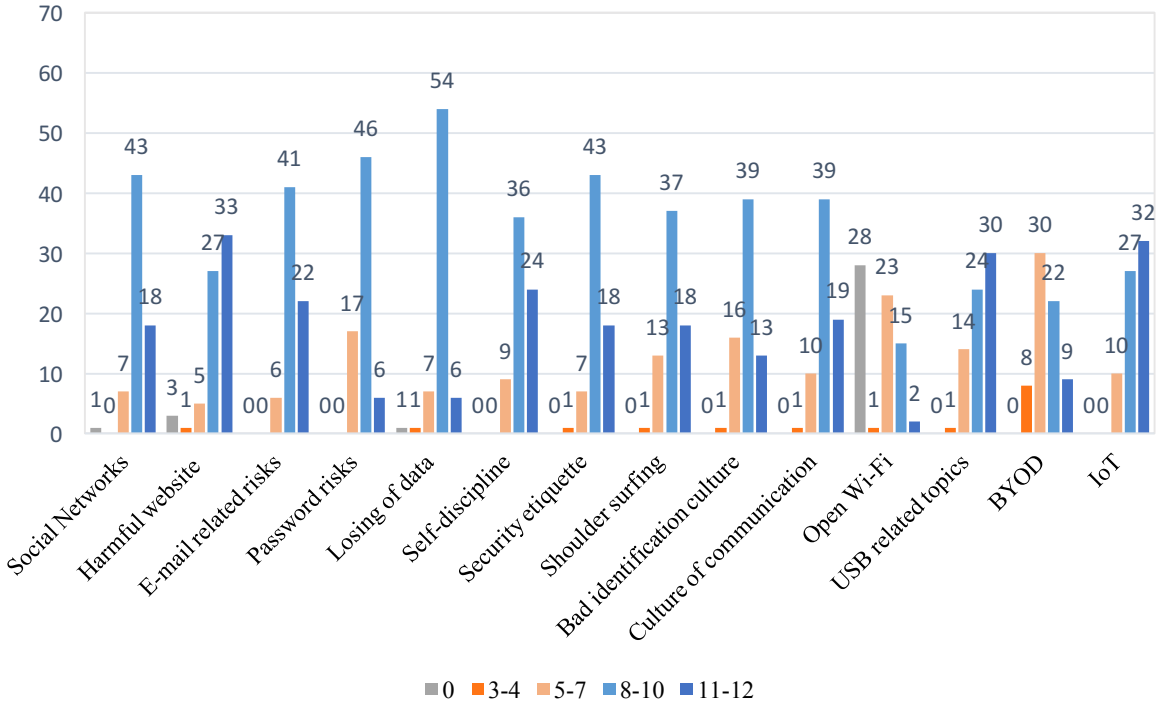

Figure 4. Distribution of answer intervals per topic of respondents.

In general, the behavior assessment questionnaire showed the realistic behavioral patterns of test audience. When taking under consideration that the test audience was more experienced computer users than average people as they are undergraduate IT students, the results were mainly correct as expected. The questionnaire showed (see *Figure 4*) also that some areas still need improvement (e.g. Open Wi-Fi and BYOD).

7.2.2. Test results

As already mentioned in the chapter *5.3.5 Measuring the results*, the author used TUT unified grading system as the basis for the final test assessment. As a result of the pilot, 64 students (93%) from 69 successfully passed the course (based on knowledge assessment test) and 5 students (7%) failed the course. From the 64 students who passed the course, 37 students (54%) were in the highest point range: 38-42 points, 18 students (26%) got score between 34-37 points and 9 students (13%) got score between 30-33 points. As we can see from *Table 3*, over half of the respondents finished the test with maximum points, which implies that over half of the participants who participated in the pilot, have acquired the basic cyber security principles.

Table 3. The knowledge assessment test results distribution in grading scale.

Fail/pass	Points	Respondents	Percentage
Fail	0-29	5	7%
Pass	30-33	9	13%
	34-37	18	26%
	38-42	37	54%

The test contained 42 questions in 14 different topics, with 3 questions per topic ratio. As there are 3 questions per topic, then with 69 respondents there are 207 responses per every topic. The 3 topics which got the most correct answers were: Social networks – 193 correct answers (93%); E-mail related risks – 198 correct answers (97%); Self-discipline – 197 correct answers (95%). The weakest topics with the most incorrect answers were: Shoulder surfing – 30 incorrect answers (15%); Culture of communication – 46 (22%) incorrect answers; Internet of things (IoT) - 40 (19%) incorrect answers. More precise overview is presented in *Figure 5*. This states that the participants had the most trouble with topics related to Shoulder surfing, Culture of communication and Internet of things. The participants understood the most topics related to Social networks, E-mail related risks and Self-discipline.

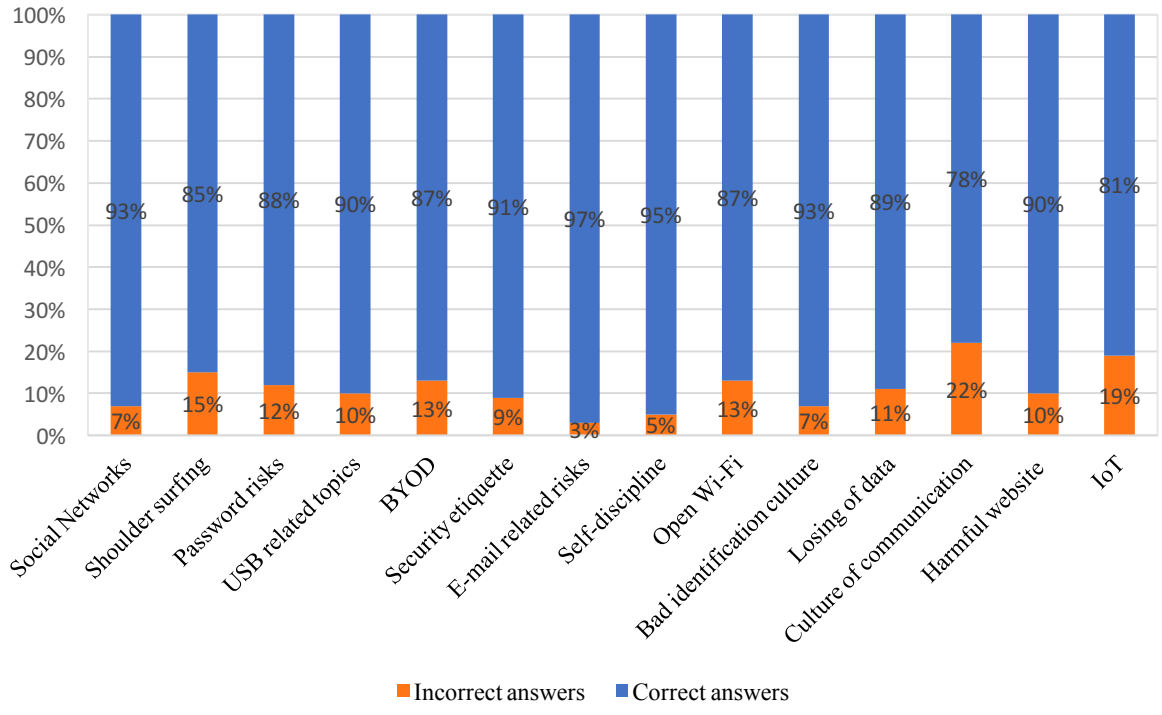

Figure 5. Knowledge assessment test results per topic.

The final test contained “Do not know” answer which was chosen together 7 times: Internet of things – 3 times; Harmful websites – 2 times; Open Wi-Fi – 1 time; Shoulder surfing – 1 time. This confirms the need of the fifth choice among answers.

7.2.3. Pilot feedback

The other part of the pilot was the feedback from the participants. From 69 participants, 38 gave feedback about the course and the questions. The overall feedback from the students was positive. The students liked the course structure with tests, videos and control questions. Feedback implied the effect of control questions as a study method and the content of the questions was related to the video. Several students said that the feedback from the control question helped to understand the topic more deeply and thus had better learning curve. The overall questions structure and content got also positive feedback. The situations reflected in the questions were important and relatable to and fancied by the students. Several students noted that the questions reflected their own experiences in everyday life, thus the course experience is more personal and educational.

From the negative side, the course had some technical issues in conducting the course. The students noted that they would have liked to see a progress bar of the course and questions. Also the course contained some grammatical mistakes. Due to technical issues, it was not possible to use dynamic questions in main part of the course and in final test. Several students noted that the questions should vary and not be static for everyone, also potentially the answers sequence should vary.

As additional suggestions, they also suggested that the course materials should involve more additional materials like links, books, other courses, articles, so the participants can continue learning. Another interesting idea was to ask a wrongly answered control question again later in the final test, to see if the participant has understood the question. Also the feedback mentioned that the final test was too long to finish and should be potentially shorter. This is taken under consideration as future work, which needs to assess the answers trustworthiness if the course test will contain less questions. This feedback is vital for the course in development process and all the suggestions and problems were taken under consideration, in further development process to improve the course more.

7.2.4. Pilot conclusion

In general, the pilot, conducted on TUT undergraduates, was successful. The pilot pointed out some technical issues, shortcomings of the wording and provided additional feedback of the problems and how to improve the questionnaire (corresponding changes are made in the questionnaire). The results of the pilot were as expected or even better (e.g. passing times) taking under consideration the background of the participants (undergraduate IT students). In order to validate the questions even better, it is important to conduct the course again on different audiences. BHC will use the evaluation method, questions and results in order to improve the course and to test the questions on different audiences.

8. Future work

As the Cyber Hygiene suggests, the Cyber Hygiene course needs to be conducted at least once a year. The same pilot test should be tested on the same audience after some time, in order to see if their behavioral practices have changed or not. This way it would be possible to see any correlations between the results and the effectiveness of the course. In the next testing phase the technical issues need to be fixed and the course should contain also control questions and final test questions randomization.

Secondly, as the developed questions were pilot tested on 69 students, the questions need to be tested on different samples, preferably on participants with different background (technical and nontechnical).

Thirdly, future work should explore the possibility to conduct the course in 2 different days: day 1 - the behavior assessment questionnaire; say 2 - the main module together with test. This distribution will be less burdensome for the participants and will save more time. This is because the main module should be conducted in succession and in work environment there may be difficult to find 2 hours of free time for the course. In order to reduce the course time, additionally, future work should explore the possibility to reduce the number of questions in final test in order to minimize the final test passing time, but at the same time to provide the trustworthy results about the course completion.

Additionally, the future work should explore the benefits and losses on effectiveness, time and results' trustworthiness of adding wrongly answered control questions among the final test questions.

9. Conclusion

The purpose of this thesis was to develop an evaluation method for Cyber Hygiene e-learning course, which will improve the questions used in the course modules, evaluate the results and in turn will raise the cyber awareness and readiness of the organizations. The author developed a structural evaluation method which took into account psychological aspects (e.g. respondent bias) in order to measure the participant's behaviors, support the study process and evaluate the acquired information of the participants. This method improves the Cyber Hygiene e-learning course scalability and can be further used to raise the volume of the questions in the course. Additionally, the developed method can be used to develop e-learning course module for the specialist or management target group, which is expressed in more complex content.

Based on that developed method the author created 200 questions for the Cyber Hygiene course to measure participant's behaviors, support the study process and measure the acquired information. The author evaluated the content of the questions with 2 cyber security experts and pilot tested the developed questions on 69 TUT undergraduate IT students. The pilot test showed that the topics with the most incorrect behaviors were: Password risks, Bad communication culture, Open Wi-Fi and Bring your own device (BYOD) and the topics with the most correct behaviors were: Social networks, Harmful websites and E-mail related risks. Secondly, the most problematic topics to understand based on the results in the learning module of the course were: Shoulder surfing, Culture of communication, Internet of things (IoT) and the strongest topics based on the results were: Social networks, E-mail related risks and Self-discipline. The pilot test received positive feedback from the pilot participants, about the vignette usage and relatable situations described by the questions.

The pilot showed that the assessment method fulfilled its purpose and provided desired results. The experts and pilot group provided constructive feedback (e.g. wording, context) about the developed questions based on which the author improved the questions. The purpose of the thesis fulfilled its objectives and will be used by BHC in further improvement and development of the Cyber Hygiene e-learning course, this in turn will reduce the risk related to human factor towards cyber security.

References

[1] Eminagaoglu, M., Ucar, E., Eren, S. *The positive outcomes of information security awareness training in companies - A case study* – Information security technical report, 2009, 14, 223-229. [Online] Science Direct (25.02.2016)
[2] EMC Corporation. *CYBERCRIME 2015: An Inside Look at the Changing Threat Landscape.* 2015. [WWW] (https://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf) (12.02.2016)
[3] Winnefeld, J., Kirchhoff, C., Upton, D. *Cybersecurity's Human Factor: Lessons from the Pentagon.* 2015. [WWW] (https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon) (12.02.2016)
[4] Interpol, Cybercrime. 2015. [WWW] (http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime) (12.02.2016)
[5] Tsiakis, T. *Contribution of corporate social responsibility to information security management* – Information security technical report, 14, 2009, 217-222. [Online] Science Direct (25.02.2016)
[6] Ashenden, D. *Information security management: a human challenge?* Information Security Technical Report, 2008, 13, 195-201. [Online] Cranfield CERES (25.02.2016)
[7] IBM, 2015 *Cyber Security Intelligence Index.* 2015. [WWW] (https://www-03.ibm.com/security/data-breach/2015-cyber-security-index.html) (12.02.2016)
[8] Paganini, P. *Why humans could be the weakest link in cyber security chain?* 2012. [WWW] (http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html) (12.02.2016)
[9] Flink, C. W. *Weakest Link in Information System Security.* 2002. [WWW] (https://www.acsac.org/waepssd/papers/01-flink.pdf) (12.02.2016)
[10] Trendmicro. The human factor. 2015. [WWW] (http://blog.trendmicro.com/trendlabs-security-intelligence/the-weakest-link-in-data-protection-infographic) (15.02.2016)
[11] ISO, 2005. *ISO/IEC 27001:2005* [Online] (http://www.iso.org/iso/catalogue_detail?csnumber=42103) (15.02.2016)
[12] Cyberstreetwise, [WWW] https://www.cyberstreetwise.com/about-us (15.02.2016)
[13] Staysafeonline, [WWW] https://staysafeonline.org/about-us/overview (15.02.2016)
[14] Futurelearn, [WWW] https://www.futurelearn.com/about (15.02.2016)
[15] Symantec, [WWW] https://www.symantec.com/services/education-services/campaigns/security-awareness (15.02.2016)
[16] IT Planeet, [WWW] – Nafta. http://www.nafta.ee/itplaneet/eng (15.02.2016)
[17] Päästa Liisa ID, [WWW] – Andmekaitse inspektsioon. http://www.aki.ee/et/noortele/paasta-liisa-id (15.02.2016)
[18] Netiohud, [WWW] http://www.netiohud.ee/assapauk (15.02.2016)
[19] Bradely, L. 2014. People Say They Care About Cyber Security, but They Don't Act Like It [Online] http://www.slate.com/blogs/future_tense/2014/11/25/byu_study_says_online_behavior_malware_safety_do_not_match_self_reported.html (15.02.2016)
[20] Sang, A. 2015. Eesti käivitas üleeuroopalise küberohtude vähendamise algatuse. [Online] http://www.kmin.ee/et/uudised/eesti-kaivitas-uleeuroopalise-kuberohtude-vahendamise-algatuse (15.02.2016)
[21] The Baltic Course, 2015. Estonia launches pan-European initiative for reducing cyber threats [Online] http://www.baltic-course.com/eng/Technology/?doc=106316 (15.02.2016)
[22] ENISA, 2014. *Estonian Cyber Security Strategy 2014-2017.* [WWW] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf estonia_cyber_security_strategy_2014-2017_public_version.pdf (16.02.2016)
[23] Human Factors and Information Security: Individual,

Culture and Security Environment, 2010. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L. [WWW] http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf (20.02.2016)
[24] Mitnick, D. K., Simon, L. W. The art of deception. Wiley publishing, Inc., Indiana: 2012.
[25] Lacey D. Managing the human factor in information security: how to win over staff and influence business managers. John Wiley & Sons, Inc.: 2009.
[26] McDaniel, P., Smith, W. S., Koppel, R. Circumvention of Security: Good Users Do Bad Things. 2013 [WWW] http://www.cs.dartmouth.edu/~sws/pubs/bks13.pdf (20.02.2016)
[27] Trendmircro. 2015. *How can enterprises reduce the risk of human error in cyber security?* [WWW] http://blog.trendmicro.com/how-can-enterprises-reduce-the-risk-of-human-error-in-cyber-security/ (20.02.2016)
[28] Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene) – The standard document. 2015. BHC Laboratory OÜ.
[29] KÄSKKIRI: Riigihanke läbiviimine. 2015 nr 6. Kaitseministeerium. [WWW] (https://webcache.googleusercontent.com/search?q=cache:obsVsQFuir8J:www.kaitseministeerium.ee/dok-register/DokumendiAndmed.action%3Bjsessionid%3DE1D176446C1A492ADB3DDD99FEF37443%3FopenFile%3D%26dokAndmed.id%3D54E4CFA3199D19FFC2257DC400491534%26manusid%3D36383+&cd=4&hl=et&ct=clnk&gl=ee) (21.02.2016)
[30] SANS Institute. End User Security Awareness Training Program. [WWW] https://securingthehuman.sans.org/security-awareness-training/enduser (21.02.2016)
[31] SANS Institute. Employee security awareness survey. [WWW] https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf (21.02.2016)
[32] Trustwave. Security Awareneness Education. [WWW] https://www.trustwave.com/Services/Compliance-and-Risk/Security-Awareness-Education/ (21.02.2016)
[33] Security Awareness Program Special Interest Group PCI Security Standards Council. 2014. Information Supplement: Best Practices for Implementing a Security Awareness Program [WWW] https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (21.02.2016)
[34] Mäses, S. *Evaluation method for human aspects of information security.* Masters thesis. Tallinn, 2015.
[35] Baker, T.L. Doing Social Research 3rd edition. McGraw Hill, International Editions. 1999, 136.
[36] Hirsjärvi, S., Remes, P., Sajavaara, P. Uuri ja kirjuta. Tallinn: Medicina, 2005.
[37] Furr, M. R. Scale Construction and Psychometrics for Social and Personality Psychology. London: SAGE Publications Ltd, 2011.
[38] LeFebvre, R. 2012. *The Human Element in Cyber Security: A Study on Student Motivation to Act* [WWW] https://dl.acm.org/citation.cfm?doid=2390317.2390318 (01.03.2016)
[39] Fan, W., Yan,Z. 2010. Factors affecting response rates of the web survey: A systematic review. Computers in Human Behavior 26, pp. 132–139.
[43] Deutskens, E., de Ruyter, K.,Wetzels, M.and Oosterveld, P.. (2004). Response Rate and Response Quality of Internet-Based Surveys: An Experimental Study. Marketing Letters 15(1), pp 21–36.
[44] Galesic, M., Bosnjak, M. 2009 Effects of questionnaire length on participation and indicators of response quality in a web survey. Public Opinion Quarterly, Vol. 73, No. 2, pp. 349–360
[45] Cook, C., Heath, F., & Thompson, R. L. 2000. A meta-analysis of response rates in Web- or Internet-based surveys. Educational and Psychological Measurement, 60, 821–836.
[46] Increasing response rates to postal questionnaires: Systematic review. Edwards, P., Roberts, I., Clarke, M., DiGuiseppi, C., Pratap, S., Wentz, R., et al. 2002. British Medical Journal, 324
[47] Sue, V. M., Ritter, L. A. 2012. Conducting Online Surveys 2nd edition. Sage.
[48] Couper, M. P. 2000. Web surveys – A review of issues and approaches. Public Opinion Quarterly, 64, 464–494.

[49] McCarty, C., Killworth, D. P., Rennell, J. Impact of methods for reducing respondent burden on personal network structural measures. C. McCarty et al. / Social Networks 29, 2007, 300–315. [Online] Science Direct (01.03.2016)
[50] Rolstad,S. Adler, J. and Ryden, A. 2011 Response Burden and Questionnaire Length: Is Shorter Better? A Review and Meta-analysis. Value in Health, 14(8), pp. 1101–1108
[51] Effect of questionnaire length, personalisation and reminder type on response rate to a complex postal survey: randomised controlled trial. Shalqvist, S., Song, Y., Bull, F. C., Adams, E. J., Ogilive, D. 2011. [Online] Loughborough University Institutional Repository. (01.03.2016)
[52] Forte, J. 2014. *How To Build Powerful Behavioral-Based Questions.* [WWW] http://www.eremedia.com/ere/how-to-build-powerful-behavioral-based-questions/ (01.03.2016)
[53] Development of a Questionnaire to Assess the Dietary Behavior of Low-Income Populations. Cabili, C., Cohen, R., Briefel, R., Grau, E. [WWW] https://nifa.usda.gov/sites/default/files/resource/Development%20of%20a%20Questionnaire%20Report.pdf (01.03.2016)
[54] Williams, A. 2015. Move Over, Millennials, Here Comes Generation Z. [WWW] http://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html?_r=0 (02.03.2016)
[55] Kane, S. T. 1994. The New Oxford Guide to Writing – Amazon. New York: 1988.
[56] UPENN. 2008. Questions. [WWW] http://www.ling.upenn.edu/~beatrice/syntax-textbook/00/box-questions.html (02.03.2016)
[57] Vocabulary. 2016. Interrogative. [WWW] https://www.vocabulary.com/dictionary/interrogative (02.03.2016)
[58] Calhoun, T. T. 2009. Grammatical person in text and narrative. [WWW] http://search.proquest.com/docview/305008165 (02.03.2016)
[59] Scott, A. G., Sechrest, L. SURVEY RESEARCH AND RESPONSE BIAS. University of Arizonas. [WWW] http://www.amstat.org/sections/srms/Proceedings/papers/1993_036.pdf (02.03.2016)
[60] Black, T. R. 1999 Doing quantitative research in the social sciences. SAGE Publications.
[61] Crocker, L., and Algina, J. 1986. Introduction to Classical and Modern Test Theory. New York: CBS College Publishing.
[62] Dolnicar, S. 2013 Asking Good Survey Questions. Journal of Travel Research 52(5) 551–574
[63] Converse, J. M., Presser, S. 1986. Survey questions: Handcrafting the standardized questionnaire. Beverly Hills: Sage Publications.
[64] Bartram, D. 2007. Increasing Validity with Forced-Choice Criterion Measurement Formats. Wiley Online Library. [WWW] http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2389.2007.00386.x/abstract (03.03.2016)
[65] Gingery, T. 2009. Forced choice survey questions. [WWW] http://survey.cvent.com/blog/market-research-design-tips-2/forced-choice-survey-questions (03.03.2016)
[66] Ritter, L. A. 2012. Conducting Online Surveys. SAGE Publications.
[67] Bowling, A. 1997. Research Methods in Health. Buckingham: Open University Press. [WWW] https://www.statmodel.com/download/irt%20of%20forced%20choice%20questionnaires%20epm11.pdf (03.03.2016)
[68] Messick S. J. 1967. The psychology of acquiescence: An interpretation of research evidence. In: Berg, I.A. (editor). Response set in personality assessment. Chicago: Aldine;. pp. 115–145.
[69] Göritz, A. S. 2005. Incentives in Web-based Studies: What to Consider and How to Decide (WebSM Guide No 0) Web Survey Methodology Site http://websm.org
[70] Couper, M. P. 2000. Web Surveys: A review of issues and approaches. Public Opinion Quarterly Vol. 64:464–494
[72] Krithikadatta J., Conserv, D. 2014 Normal Distribution. 17:96-7 [WWW] http://www.jcd.org.in/article.asp?issn=0972-0707;year=2014;volume=17;issue=1;spage=96;epage=97;aulast=Krithikadatta (03.03.2016)

[73] About. 2015. Question – About. [WWW] http://grammar.about.com/od/pq/g/questionterm.htm (05.03.2016)
[74] Tofade, T., Elsner, J., Haines, S. T. 2013. REVIEWS: Best Practice Strategies for Effective Use of Questions as a Teaching Tool. American Journal of Pharmaceutical Education 2013; 77 (7) Article 155. [WWW] http://www.ajpe.org/doi/pdf/10.5688/ajpe777155 (05.03.2016)
[75] Higher Education Comission, Pakistan. [WWW] http://www.hec.gov.pk/InsideHEC/Divisions/LearningInnovation/Documents/Learning%20Portal/NCES/NCES%20Presentations/TEST%20AND%20TYPES%20OF%20TEST.pdf (05.03.2016)
[76] Khan, M. S. 2007. School Evaluation. A.P.H. Publishing Corp.
[77] CITL. Completion Test Items. [WWW] https://citl.illinois.edu/teaching-resources/evaluating-student-performance/writing-good-test-questions/completion-test-items (10.03.2016)
[78] CITL. Matching Test Items. [WWW] https://citl.illinois.edu/teaching-resources/evaluating-student-performance/writing-good-test-questions/matching-test-items (10.03.2016)
[79] University of Waterloo. Centre for teaching excellence: Designing multiple-choice questions. [WWW] https://uwaterloo.ca/centre-for-teaching-excellence/teaching-resources/teaching-tips/developing-assignments/assignment-design/designing-multiple-choice-questions (10.03.2016)
[80] Beck, J. On the Usefulness of Pretesting Vignettes in Exploratory Research. [WWW] https://www.amstat.org/sections/srms/proceedings/y2010/Files/400125.pdf (10.03.2016)
[81] Martin, E. 2006. Vignettes and Respondent Debriefings for Questionnaire Design and Evaluation. [WWW] https://www.census.gov/srd/papers/pdf/rsm2006-08.pdf (10.03.2016)
[82] Using vignettes in qualitative research to explore barriers and facilitating factors to the uptake of prevention of mother-to-child transmission services in rural Tanzania: a critical analysis. Gourlay, A., Mshana, G., Birdthistle, I., Bulugu, G., Zaba, B., Urassa, M. [WWW] http://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-14-21 (10.03.2016)
[83] Barter, C., Renold, E. 1999. The Use of Vignettes in Qualitative Research [WWW] http://sru.soc.surrey.ac.uk/SRU25.html (10.03.2016)
[84] Hughes, R., Huby, M. 2004. The construction and interpretation of vignettes in social research. Social Work & Social Sciences Review 11(1), pp.36-51
[85] Ajzen, I. 2002. Constructing a TpB Questionnaire: Conceptual and Methodological Considerations. [WWW] http://chuang.epage.au.edu.tw/ezfiles/168/1168/attach/20/pta_41176_7688352_57138.pdf (13.03.2016)
[86] English For Everyone. Grammatical Person - 1st , 2nd and 3rd Person. [WWW] http://englishforeveryone.org/PDFs/Grammatical%20Person.pdf (13.03.2016)
[87] University of Waterloo. Designing multiple-choice questions. [WWW] https://uwaterloo.ca/centre-for-teaching-excellence/teaching-resources/teaching-tips/developing-assignments/assignment-design/designing-multiple-choice-questions (13.03.2016)
[88] Murata, T., Gwartney, P., "Question Salience, Question Difficulty and Item Nonresponse in Survey Research", Paper presented at the International Conference on Survey Non-response, Portland, Oregon, October 28-31, 1999.
[89] Sue, V. M., Ritter, L. A. 2012. Conducting Online Surveys SAGE Publications, Inc.
[90] Brigham Young University. 2001. 14 RULES FOR WRITING MULTIPLE-CHOICE QUESTIONS. [WWW] https://testing.byu.edu/handbooks/14%20Rules%20for%20Writing%20Multiple-Choice%20Questions.pdf (13.03.2016)
[91] Tallinna Tehnikaülikool. Tallinna Tehnikaülikooli õppetegevuse eeskiri. [WWW] https://www.ttu.ee/public/m/majandusteaduskond/Tudengile/Doktoriope/_ppetegevuse_eeskiri.doc (20.03.2016)
[92] Carston, R. Linguistic Communication and the Semantics/Pragmatics Distinction*. [WWW] https://www.ucl.ac.uk/pals/research/linguistics/publications/wpl/06papers/carston (20.03.2016)

[93] University of Minnesota. Survey Design: Item Writing. [WWW] http://surveys.umn.edu/best-practices/survey-design-item-writing (20.03.2016)
[94] Ross, K. N. 2005. Questionnaire Design. [WWW] http://www.unesco.org/iiep/PDF/TR_Mods/Qu_Mod8.pdf (20.03.2016)
[95] Changing Minds. Leading questions. [WWW] http://changingminds.org/techniques/questioning/leading_questions.htm (20.03.2016) [96] Statistics New Zealand. Methodological standard for writing and constructing a questionnaire. [WWW] http://www.stats.govt.nz/methods/survey-design-data-collection/writing-questionnaire/wording.aspx (20.03.2016)
[97] Halterman, E. 2012. Get Better Survey Data By Avoiding Overlapping Ranges. [WWW] https://www.surveygizmo.com/survey-blog/a-note-about-overlapping-ranges/ (20.03.2016)

Appendix 1 – Topics distribution

Malicious websites and information sharing

- Social Networks
- Harmful website
- E-mail related risks

Access to the information

- Password risks
- Losing of data
- Self-discipline
- Security etiquette

Human aspects

- Shoulder surfing
- Bad identification culture
- Culture of communication

Network and physical devices

- Open Wi-Fi
- USB related topics
- Bring your own device (BYOD)
- Internet of things (IoT)

Appendix 2 – Examples of behavior assessment questions

Social networks

Have you discussed confidential work information over social networks (example Facebook)? Choose the answer that you think is the most accurate.

- Actively, whenever there is need to discuss these topics, either through public profile or chat.
- Only in emergencies and in private chat, never through public profile.
- Only what I believe to be public work information and suggest to move to more secure channels (example work e-mail).
- I discuss these type of topics over work e-mail or phone.
- I do not use social media.

Shoulder surfing

How often do you discuss work topics over the phone in a public place (example diner or bank), where you probably have less personal space? Choose the answer that you think is the most accurate.

- Only when it is emergency.
- Occasionally but never confidential information.
- I never discuss work topics over the phone in public places.
- I discuss it daily, whenever there is need.

Culture of communication

Have third parties (example friends, family) helped you to fix issues (example e-mail related issues) with your work devices? Choose the answer that you think is the most accurate.

- I have asked help couple of times from friends or family.
- I have always asked help from IT support.
- I have tried to manage by myself, without anyone's help.
- I have often asked help from friends or family.

Bring your own device (BYOD)

How often do you use third party services (example Dropbox, Trello, Google Docs) for storing or processing work documents? Choose the answer that you think is the most accurate.

- I use actively different third party services for work purposes.
- I use time to time some of them for work purposes.
- I use third party services for work purposes because I have permission to use.
- I do not use any third party services for work purposes.

Self-discipline

In your opinion, is it realistic that someone will abuse your computer when left unattended? Choose the answer that you think is the most accurate.

- No, because I do not have anything confidential in my computer nor money to steal.
- Yes, only when I have left open some sensitive service (example Internet bank, social media account).
- No, no one will care about my devices, more less abuse my computer.
- Yes, one can do many things in there (example place a keylogger, send fake email, invite other colleagues for a free cake) and most probably will do it.

Appendix 3 – Examples of control questions

Social networks

Situation description: Coworker Adam calls to Eva and informs her, that the meeting is moved to earlier time. Eva posts meeting topics, time and location to social media, for other colleagues. She did not notice, that she accidentally posted the information to her public profile.

If Eva deletes certain information from social media, is the information deleted completely from the social media? Choose one of the following answers:

- Information will be deleted completely and will not be accessible by anyone anymore.
- Information is still accessible by third parties, even after one has deleted information from one's profile.
- The information will be deleted after the social media managers have reviewed the request of information deletion.
- The information is deleted as long the information is in image format.
- Do not know.

USB related topics

Situation description: Adam needs a USB drive for upcoming meeting, but he hasn't any, he has left it at home. Eventually he founds one drive which was a present from guest delegation, with marketing materials.

Is it safe to use borrowed USB devices from a friend for work purposes? Choose one of the following answers:

- It is safe as long as the computer has updated antivirus software installed.
- It is not safe, if the borrowed USB drive is not encrypted.
- Yes, because the owner of the device is not stranger, and most probably have no intentions to infect the USB device deliberately.
- It is not safe, because the strange USB device can still be infected with malware, despite that the owner is a friend.
- Do not know.

Culture of Communication

Situation description: Just before Eva starts going home from work, she wanted to check over some e-mails but there were some technical difficulties with her computer. Restart did not fix the problem and she could not fix the issue by herself. It is after hours but she still calls to IT helpdesk. Fortunately, her colleague picked up the phone and fixed her problem.

If Eva had not been able to contact the IT helpdesk, how she should have proceeded with her problem? Choose one of the following answers:

- She should have just ignored the problem.
- She should have asked help from her neighbor IT specialist.
- She should have waited to the next morning and then contact the IT helpdesk again.
- She should have asked help from ex colleague who was IT specialist in that firm.
- Do not know.

Security Etiquette

Situation description: Paul continues with the next meeting in the same room, when others are gone, because there is some urgent situation and needs to be dealt with immediately. Meeting is remote so audience will take part remotely, over webcam. What he does not notice is the whiteboard from last meeting with sensitive information behind his back (now everybody knows what was discussed in the previous meeting).

How Paul should act, when he would discover confidential work documents from the trashcan? Choose one of the following answers:

- He should ignore the documents in the trash because if they are in there, then probably they are not necessary anymore
- He should withdraw the documents out of the trashcan and put them into paper shredder.
- He should take the documents out of the trashcan and bring them to his superior.
- He should ignore the documents because it is not his responsibility to validate the contents of the trashcan.
- Do not know.

Appendix 4 – Examples of test questions

Social media

Julia is travelling to Paris. She posts a picture of herself in the airport to the social media (example Facebook) public profile. The title of the picture says: "Flying to Paris, see you all in a month!". Which of the following is true:

- It is necessary to post this information to social media public profile, otherwise her friends do not know that she will be away.
- Posting this to her public profile makes her vulnerable to various potential attacks by third parties.
- By posting this to her public profile, she is safe from all of the potential threats because social media companies are protecting their users.
- By posting this to her public profile, she is safe from all of the potential threats because strangers do not care whether she travels or not.
- Do not know.

Carmen and Julia did a selfie *(picture of themselves)* at the office. They posted it to social media *(example Facebook)*. The picture was from an angle which exposed a list of phone numbers of all the employee's from the computer screen. Which of the following is true:

- It is safe to post this to social media, because the headline of the picture does not involve the name of the company and no one will be able to associate the information with the organization.
- It is safe to post this because many of their colleagues have posted same kind of pictures to social media and nothing has happened, thus it is safe to post these kind of pictures to social media.
- By posting pictures to social media private profile, the organization sensitive information is safe because it is protected by social media company.
- By posting pictures to social media, they would have to check that the pictures would not contain sensitive information about the organization. Otherwise it will make the organization vulnerable to various potential attacks by third parties.
- Do not know.

Internet of things (IOT)

Adriana works in a large software development company. She loves to improve their company's office, so that everyone will feel more homely there. She received a gift from associate firm, for a good partnership. The gift was a smart light bulb, which can be adjusted through smartphone using Wi-Fi connection. She inserted the bulb to the socket and connected to corporate Wi-Fi. Which of the following is true:

- She acted correctly, because it was a practical and innovative gift. Now they can very conveniently manage one light bulb.
- She did not act correctly, because she inserted unverified third party device to corporate network. She should have contacted the security officer first.
- The new smart light bulb cannot cause any threat to a company.
- She did not act correctly, because it is impossible to secure smart devices, thus they should be never used in corporate nor personal environment.
- Do not know.

Culture of communication

Joe is a cyber aware employee. He can detect all the social engineering attacks and phishing mails without any issue. As he works in a bank, he sees them often, but he ignores them. He deletes the e-mails or ends the calls. He does not tell anyone about them, a full three months already. There have been around 30 incidents. Which of the following is true:

- He acted correctly, by detecting them and not falling for malicious e-mails or phone calls. It is not his job to notify IT personnel about the incidents.
- In addition to detecting, he should also start investigating to identify who is responsible of the malicious e-mails and phone calls.
- In addition to detecting, he should also inform the responsible department for every incident.
- He acted correctly, because he should ignore the first 45 incidents, after what it is reasonable to inform about the incidents.
- Do not know.

Open Wi-Fi

Marina is waiting her flight to Kamchatka. While waiting she decides to log into social media (example Facebook) using airport free Wi-Fi. When she opens the site, she notices that the website is not using "*https*" protocol like it has always used and the domain name is odd. The domain name looks like: "*http://facebook.socia1media.com*". Which of the following is true:

- She should not log in, because the domain name is not legitimate domain name for that service. This is probably *"Man In The Middle Attack"* which is using a phishing site.
- She should not log in, if she does not use antivirus program and her device is not encrypted using *"RSA"* encryption algorithm with 256-bit key.
- She may log in, if she can verify that all the necessary visual elements of the social media web page are presented.
- She may log in, if she should could verify with someone from the airport, that they are also seeing the same domain name.
- Do not know.

E-mail related risks

Donna receives an email claiming that she won 100 000€ on an online lottery. In order to claim the prize, she needs to send small amount of money to specific bank account for the government taxes and bank fees. Which of the following is true:

- She may transfer the money if the e-mail also states that the company of the lottery is Europe gaming commission.
- She may transfer the money, because it is very common that people have won with online lottery. Although Donna does not remember that she has participated in any online lotteries before.
- She should never transfer the money, because it is probably a scam e-mail which is trying to lure the recipient to transfer money.
- She should never transfer the money, because it is unethical to gamble online.
- Do not know.