TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science

Heleri Aitsam 178126

TEACHING CYBERETHICS AND MEASURING CYBERETHICAL BEHAVIOR IN A CLASSROOM SETTING

Master's thesis

Supervisor: Sten Mäses
MSc

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Tarkvarateaduse instituut

Heleri Aitsam 178126

KÜBEREETIKA ÕPETAMINE JA KÜBEREETILISE KÄITUMISE MÕÕTMINE ÕPPETÖÖS

Magistritöö

Juhendaja: Sten Mäses
MSc

Tallinn 2019

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: Heleri Aitsam

13.05.2019

Abstract

The aim of this research was first, to give an overview of topics in cyberethics that could be taught to students with one lecture. Second, to develop a method with what students' cyberethical behavior could be measured and third, to measure, how much students' cyberethical behavior, attitude and ethical views would be influenced with one lecture.

To reach these goals, an overview of important issues of cyberethics was given based on the literature review. The experiment was conducted to see, if the developed method could be used for measuring cyberethical behavior and to measure, the influence of one lecture to cyberethical behavior. Also, a questionnaire was used to measure cybersecurity attitude and ethical views of students.

The results from the experiment indicate that the developed method could be used for measuring cyberethical behavior. The cybersecurity attitude and ethical views questionnaires were not found to be good for predicting cyberethical behavior, but it revealed that some change had occurred after the cyberethics lecture. Also, the lab for measuring cyberethical behavior indicated that some students started to behave more ethically after the lecture.

The research offers insights into cyberethics and measuring it. It could be used as a guidance for creating effective cyberethics education programs.

This thesis is written in English and is 80 pages long, including 7 chapters, 14 figures, and 7 tables.

Annotatsioon

Kübereetika õpetamine ja kübereetilise käitumise mõõtmine õppetöös

Antud magistritöö üheks eesmärgiks oli anda ülevaade olulisetest teemadest kübereetikas, mida oleks võimalik õpetada üliõpilastele ühe loenguga. Teiseks eesmärgiks oli välja arendada meetod, millega oleks võimalik mõõta üliõpilaste kübereetilist käitumist. Kolmandaks sooviti näha, kas ja kui palju on võimalik mõjutada ühe loenguga üliõpilaste kübereetilist käitumist, suhtumist ja eetilisi vaateid.

Töös püstitatud eesmärkide täitmiseks anti erialase kirjanduse põhjal ülevaade kübereetikast ja sellega seonduvatest probleemidest. Loodud ülevaate põhjal koostati ka loengu materjalid. Magistritöö käigus arendati välja meetod üliõpilaste kübereetilise käitumise mõõtmiseks. Antud meetodi toimivuse hindamiseks ja selgitamaks, kui palju on võimalik üliõpilaste kübereetilist käitumist, suhtumist ja eetilisi vaateid ühe loenguga mõjutada, viidi läbi ekperiment.

Eksperimendi käigus kogutud andmete põhjal võib järeldada, et magistritöös arendatud meetodit saab kasutada üliõpilaste kübereetilise käitumise mõõtmiseks. Tulemusi analüüsides ei leitud kinnitust, et küberkaitse suhtumise ja eetiliste vaadete küsimustikku saaks kasutada üliõpilaste kübereetilise käitumise ennustajana. Küll aga selgus eel- ja järelküsimustiku tulemusi võrreldes, et pärast loengu kuulamist oli üliõpilaste kübereetilises käitumises toimunud muutus. Muutusi kübereetilises käitumises kinnitas ka labori tulemuste analüüs. Pärast loengu kuulamist käitus osa üliõppilasi eetilisemalt kui varem. Selgus, et pärast loengu kuulamist käitus osa üliõpilasi eetilisemalt kui varem.

Antud magistritöö annab olulise ülevaate kübereetikast ja selle mõõtmise võimalustest.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 80 leheküljel, 7 peatükki, 14 joonist, 7 tabelit.

List of abbreviations and terms

ACM	Association for Computing Machinery
CAPTCHA	Completely Automated Public Turing test to Tell Computers and Humans Apart [1]
CAS	Cybersecurity Attitude Scale
CERT	Computer Emergency Response Team
GDPR	General Data Protection Regulation
HAIS-Q	Human Aspects of Information Security Questionnaire
IB	Impartial Beneficence
IEEE	Institute of Electrical and Electronics Engineers
IH	Instrumental Harm
IT	Information Technology
OSINT	Open-Source Intelligence
OUS	Oxford Utilitarianism Scale
PA	Policy Adherence
PV	Perceived Vulnerability
SQL	Structured Query Language
TalTech	Tallinn University of Technology

Table of contents

1 Introduction 11
2 Background of Ethics 13
2.1 Definition of Ethics 13
2.2 Ethical Theories 14
2.2.1 Utilitarianism 15
2.2.2 Deontology 16
2.2.3 Contract-based and Character-based Ethical Theories 18
3 Background of Cyberethics 19
3.1 Definition of Cyberethics 19
3.2 Cyberethics as Field of Applied Ethics 20
3.3 Uniqueness of Cyberethics 21
3.4 Important Issues in Cyberethics 23
3.4.1 Professional Ethics 23
3.4.2 Security 24
3.4.3 Privacy 25
3.4.4 Cybercrime 26
3.4.5 Intellectual Property 26
4 Related work 27
4.1 Measuring the Impact of Teaching Cyberethics 27
4.2 Cyberethical Behavior Measurement 28
5 Methodology 30
5.1 Phase One: Designing the Experiment 31
5.1.1 Virtual Hands-on lab 33
5.1.2 Attitude and Ethical Views Questionnaire 35
5.1.3 Cyberethics Lecture 38
5.1.4 The Environment of the Experiment 40
5.1.5 Expert Interview 40
5.2 Phase Two: Pilot Study 41
5.3 Phase Three: Main Experiment 42

5.4 Results 43
5.4.1 Cronbach Alpha of Pre- and Post-questionnaire 45
5.4.2 Spearman's Rank-order Correlation of Pre- and Post-Questionnaire 46
5.4.3 Behavior in the Virtual Hands-on Labs Before the Lecture 48
5.4.4 Lecture 50
5.4.5 Behavior in the Virtual Hands-on Labs After the Lecture 51
5.4.6 Answer Type and Time Waited for Permission in the Lab 52
5.4.7 Chi-square Tests on Lab Results 53
5.4.8 Apriori Algorithm Results 55
6 Discussion 60
6.1 Limitations of the Experiment 66
6.2 Future Work 67
7 Summary 70
References 72
Appendix 1 – Questionnaire 77
Appendix 2 – Time Labels for Apriori Algorithm 80

List of figures

Figure 1. Acts vs. Rules and Consequences vs. Duties [17]. 17
Figure 2. Phases of the research. 30
Figure 3. Design of the experiment..... 31
Figure 4. Example answers to student's email in one lab. 34
Figure 5. Example model of the answer types to students. 35
Figure 6. Design of the experiment – in more detail. 39
Figure 7. Percentage of students in groups GX and GY, who gave permission and participated in the lecture. 43
Figure 8. Students divided by gender in percentage. 44
Figure 9. Distribution of men and women in groups GX and GY in percentage. 44
Figure 10. Diagram describing the results in the labs. 49
Figure 11. Feedback from students on the lecture. 51
Figure 12. The number of students based on answer type and behavior in the lab in percentage. 52
Figure 13. The average waiting time in labs with standard deviation. 53
Figure 14. The average waiting time in labs with standard deviation and answer type. 53

List of tables

Table 1. Cronbach alphas of pre-questionnaire. 46
Table 2. Cronbach alphas of post-questionnaire..... 46
Table 3. Spearman's rank-order correlation between pre-questionnaire scales. 47
Table 4. Spearman's rank-order correlation between post-questionnaire scales..... 47
Table 5. Chi-square test results between lab results. 55
Table 6. Apriori results on pre- and post-questionnaire and labs. 58
Table 7. Apriori results containing time. 59

1 Introduction

Ethics and ethical behavior have been a topic of discussion for thousands of years and is tightly connected to various parts of our lives. With the development of computers, the term “computer ethics” was taken into usage in the 1970s [2]. The field itself existed already back in the end of 1940s, but it was then not considered as “separate field of research” [2]. The term “cyber ethics” was taken into use later to describe mainly the same field of ethics as was explained with computer ethics. With the growth of accessibility of computers, cybersecurity is gaining more importance. A large and growing body of literature has investigated different aspects of cyberethics. Whether this domain of ethics has unique issues or not is an ongoing discussion among philosophers that are discussed in chapter 3.3. Nevertheless, it certainly influences people and organizations as a whole.

Current IT students are going to face cyberethical problems in their future work and need to be educated on how these issues are affecting them and how to react to it. Otherwise, the lack of awareness might cause misunderstandings. For example, situations like in article [3] might happen, where in 2017 River City Media (RCM) filed a lawsuit against security researcher, who claimed he had found evidence that RCM was operating a massive and illegal spamming operation and published his findings online [3]. The researcher claimed that the data had been left exposed to online by RCM and was accessible to everyone [3]. RCM, on the other hand, claimed that this had been a targeted attack against them by the researcher [3]. This example raises another reason, why cyberethics is important. Differentiating between “white hat”, “grey hat” and “black hat” hackers is difficult – what is white to one might be gray to another [4]. Also attacking the system is nowadays often used to raise security or awareness and find vulnerabilities, deciding what is an ethical way to behave and what is not is a challenging task [5], [6]. The importance of teaching cyberethics is also evident from Amorim et al. article [7], where it is mentioned, that when training for cyber defense typical cybersecurity skills, like cybersecurity strategy skills, IT base skills, communication skills and also cyberethics skills are needed [7]. IEEE has launched its separate IEEE TechEthics

program, with the purpose to make sure that ethics becomes an important part of the development process [8]. When putting ethical behavior into monetary values article [9] brings out that unethical and criminal behavior through the use of computers brings approximately billions of dollars of loss per year [9].

The gap in this field of research is that students' cyberethical behavior and attitude change is usually not being measured. Currently, the main way to measure change is through questionnaires and interviews, but one thing is what the student puts on the paper and another how (s)he behaves. With this research, the gap in how one lecture on cyberethics influences students cyberethical behavior and attitude and how to measure it is addressed. To fill this gap following research questions were formed:

RQ 1. What topics should be taught in cyberethics?

RQ 2. How can students' cyberethical behavior be measured?

RQ 3. How much can one lecture influence students' cyberethical behavior?

To answer the 1st research question (RQ 1) background on cyberethics is given based on literature review in chapters 2 and 3. To have a cleared understanding of cyberethics, first a basic overview of ethics is given. Two ethical theories – utilitarianism and deontology – will be given a closer look and some important issues in cyberethics are brought out and introduced.

The thesis continuous with giving a literature review of related work on the field of measuring cyberethical behavior in chapter 4.

To see, how cyberethics can be measured, the experiment is created. The description of the experiment and the results of it are brought out in chapter 5. In chapter 6 the results gathered from the experiment are discussed, and the limitations of the experiment are brought out. Finally, the impact of one lecture to the students' cyberethical behavior is analyzed and discussed.

2 Background of Ethics

In this and the following section basic topics, that would be good to teach, of ethics and cyberethics are discussed. To have a better understanding of cyberethics some basic concepts of ethics are brought out. In this chapter, an overview is given about the definition of ethics, three types of ethical inquiry and two well-known ethical theories – utilitarianism and deontology.

2.1 Definition of Ethics

In this chapter, an overview is given about the different definitions that exist to describe the term ethics. Also, a common way to categorize ethics is shortly outlined.

Different wordings exist in literature to describe ethics. Pojman et al. bring out in book [10] that "ethics is that branch of philosophy that deals with how we ought to live, with the idea of the Good, and with concepts such as "right" and "wrong"" [10]. A similar explanation is given in article [11], where it said that "ethics in the broadest sense refers to the concern that humans have always had for figuring out how best to live" [11]. Rich writes in [12] that "as a philosophical discipline of study, ethics is a systematic approach to understanding, analyzing, and distinguishing matters if right and wrong, good and bad, and admirable and deplorable as they relate to the well-being of and the relationships among sentient beings" [12]. Though there is not a single definition for ethics the main idea of the different wordings stays the same – figuring out what is good life [11]. Ethics is put in action through different methods like codes of conduct, formal theories and other approaches [12].

In different writings, a common way to categorize ethics is based on three types of inquiry or study: normative ethics, meta-ethics and applied ethics [13], [14], [15]. Followingly each of these terms is shortly explained.

- Normative ethics: Normative ethics deals with the evaluation of moral rules and principles by asking "what ought to be the case" according to morally right and wrong behavior [16]. Descriptive ethics is seen as the basis of normative

ethics [14]. Descriptive ethics tries to describe and understand ethical principles and behavior [12], [14], [16]. Normative ethics has developed some widely used ethical theories including utilitarianism, deontology and virtue ethics [14].

- Meta-ethics: Meta-ethics tries to understand the meaning of morality by analyzing the ethical concepts and theories [12]. For example, analyzing concepts like good and happiness [12].
- Applied ethics: Applied ethics deals with practical moral issues [16]. Applied ethics is also known by the name of practical ethics. Applied ethics deals mainly with controversial issues [10], [13]. When solving the applied ethical issue, several normative principles should be consulted to determine its morality [13]. Applied ethics examines moral issues through ethical theories like utilitarianism and deontology [17].

Even though it is possible to define the inquiries mentioned above, we cannot separate them, for example, when solving a difficult ethical problem [10], [18]. For instance, applied ethics and normative ethics are tightly connected [10]. Pojman et al. have said that: "theory without application is sterile and useless, but action without a theoretical perspective is blind" [10].

Ethics is closely connected to law. Ethics often influences, which laws are created and laws, on the other hand, may give a stronger foundation for ethical positions [19]. For example, the General Data Protection Regulation (GDPR) is strongly influenced by ethical values (e.g., privacy).

2.2 Ethical Theories

In the previous chapter, short overview of the definition and different categories of ethics was given. In this chapter, the explanation of ethical theory is given, and two ethical theories are introduced.

Tavani has said in his book [17] that "ethical theory, like scientific theory, provides us with a framework for analyzing moral issues via a scheme that is internally coherent and consistent as well as comprehensive and systematic" [17]. It helps to understand concepts that are relevant and teaches how to live [10]. There are a lot of different theories, often opposing each other [10]. Two types of ethical theories that have gained much attention

in the literature are duty and consequence based [20]. Consequentialism states that it is the consequences of an action, where the ethical value can be found [14], meaning that the consequences of actions are measured. The well-known consequentialist theory is usually considered to be utilitarianism [12], [20]. Duty-based ethical theory, on the other hand, states that it is the duty, a commitment between people, that matters, and never about the consequences [17]. The widely known duty-based theory is deontology [20]. These two theories – utilitarianism and deontology - will be discussed next.

2.2.1 Utilitarianism

Utilitarianism is a type of consequentialist ethics that follows the principle of "greatest good" [10], [11], [20], [17]. In the book [10] is given the following definition: utilitarianism "calls for the maximization of goodness in society - that is, the greatest goodness for the greatest number - and not merely the good of the agent" [10]. Happiness and pleasure, also in some cases the absence of pain, are used to measure the "good" [11]. For utilitarians, happiness is an intrinsic good – "that is, something that is good in and of itself, for its own sake, and not merely a means to some further end or ends" [16]. For example, if we have a choice between actions A and B, then the utilitarian way to act would be the one which produces the most happiness for the greatest number of individuals [16]. Jeremy Bentham and John Stuart Mill were two most influential philosophers, who promoted classical utilitarianism in the 18th and 19th century and who are still quoted [10], [16], [14].

Utilitarianism can be divided into two subdivisions: rule and act utilitarianism [10], [12], [17]. Act utilitarianism says that "an act, X, is morally permissible if the consequences produced by doing X results in the greatest good for the greatest number of people affected by X" [17]. One of the problems with act utilitarianism is that often we cannot make calculations to figure out which action is better one in each situation [10].

Rule utilitarianism states that "an act, X, is morally permissible if the consequences of following the general rule Y, of which act X is an instance, would bring about the greatest good for the greatest number" [17]. The consequences of following the rules matter compared to act utilitarianism, where the consequences of individual actions matter [17]. Rules like "do not kill" and "do not lie" [12]. For example, if as a consequence of a promise-breaking more good is produced then according to act utilitarianism it is allowed,

but based on rule utilitarianism promise has to be kept, because in most cases, it produces more happiness [12].

2.2.2 Deontology

Deontological theories are based on duty and rules where the obligation is the foundation of morality [17]. It is not the consequences that matter for deontologists but the features of the act itself [10], [21]. Deontologist use the argument that as being part of society we have duties to each other because of our rational nature [17]. When deciding on the morality of an action comparison with universal rules has to be made [21]. Article [17] states that if our main purpose is to seek happiness, as utilitarians suggest, then we would be, in a moral point of view, similar to other creatures and animals. However, humans can make rational decisions. This refutes utilitarianism in the eyes of deontologists [17]. The only thing that deontologists consider good is a good will [10]. Everything else, like success and happiness, are not good in themselves, because they can produce evil [10]. For example, if utilitarians believe that happiness should be distributed equally then, deontologists believe it should be distributed proportionally based on peoples morality [10]. Deontology, as well as utilitarianism, can be divided into two: rule and act deontology [17]. Followingly these two will be shortly discussed.

In rule deontology, the ethicality is based on complying with rules [22]. Most well-known rule deontologist is Immanuel Kant [12], [17]. Kant believed that the only way to lead a person to moral actions is through rules and duty but not through emotions [12]. Kant supported the concept of *categorical imperative* – the principle that should be followed to determine the basics of our morality according to Tavani's book [17]. It states that the ethicality of an action are based on the application of "goodwill" [23]. This imperative has several variations, two of them are following:

1. "act always on that maxim or principle (or rule) that ensures that all individuals will be treated as ends-in-themselves and never merely as a means to an end" [17],

2. "act always on that maxim or principle (or rule) that can be universally binding, without exception, for all human beings" [17].

This favors equality among people. Making an exception to these rules would mean the violation of principle [17].

David Ross, 19th - 20th-century philosopher and act deontology follower, believed that Kant's version of deontology is flawed [17]. Act deontologists believe that if two or more moral duties collide then, individual situations have to be taken into consideration to make decisions [17], [24]. Rules are taken only as guidelines; exceptions may be done [22], [25]. In act deontology like in rule deontology the ultimate notion is duty, but unlike believed in rule deontology act deontologists think it might not be enough in all situations [17]. According to Ross [26], there are *prima facie duties* or conditional duties that must be followed. These kind of duties are for example gratitude and justice [26]. If in a certain situation there are no conflicts between prima facie duties, then this duty will become an *actual duty* [17]. However, if two duties conflict a process called "rational intuitionism" is used to figure out the actual duty [17].

Article [27] brings out that rule deontology and rule utilitarianism are similar because the moral way to behave in both cases is to follow the rules. However, the difference between these two is about the impact of the consequences – it matters to rule utilitarians but is not important to rule deontologists [27]. In book [17] is said that act utilitarians, as well as act deontologists, believe that individual situations must be analyzed to figure out what is the morally correct way. The difference stays in the concept of considering the consequences of one's actions. Utilitarians believe that the consequences of an act have to be considered, but to deontologists, it is all about the duty [17]. A Figure 1, taken from Tavani's book [17], describes the differences and similarities between rule and act deontology and rule and act utilitarianism.

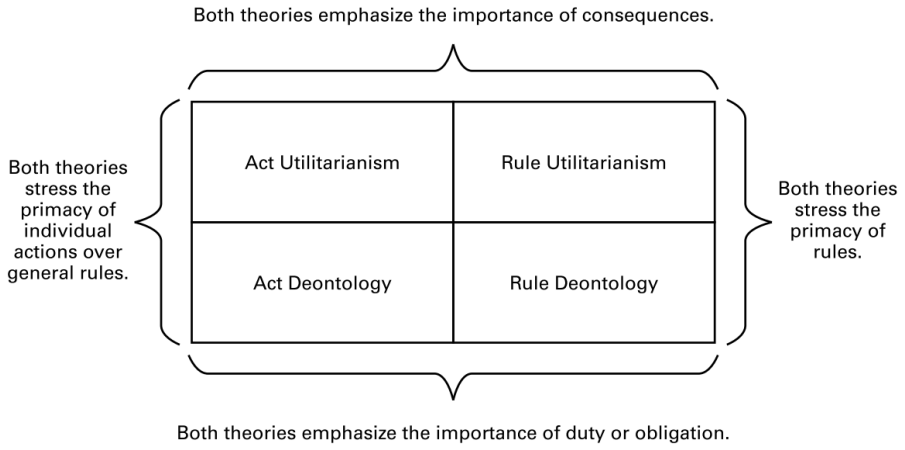

Figure 1. Acts vs. Rules and Consequences vs. Duties [17].

In the previous sections, two common ethical theories were introduced – utilitarianism and deontology – and their distinction into two subdivisions was mentioned.

2.2.3 Contract-based and Character-based Ethical Theories

Additionally to utilitarianism and deontology, many other ethical theories exist, but these stay out of the scope of this paper. Still, two of them - contract-based and character-based ethical theories – are briefly mentioned here [17].

One example of the contract-based theory is the social-contract theory. In this theory, contracts between individuals are what set the base for the moral system [17]. Pojman et al. give the following definition to social contract theory: "the moral and political theory that people collectively agree to behave morally as a way to reduce social chaos and create peace" [10]. One of the strengths of social-contract theory is that it motivates humans to act morally because it is in everybody's best favor to come-up with rules [17].

Virtue ethics is one type of character-based theory [17]. Pojman et al. gives the following definition: virtue ethics is "the view that morality involves producing excellent persons who act well out of spontaneous goodness and serve as examples to inspire others" [10]. In focus is the development of one's character, having proper motivation and emotions [10], [17]. It tells us to go after an ideal person. Virtues can be divided into two: moral and nonmoral virtues [10].

To sum up, chapter 2 discussed the definition of ethical theory and described two ethical theories – utilitarianism and deontology. Additionally, a short introduction about contract-based and character-based theories was given.

3 Background of Cyberethics

In the previous chapter basics of ethics were given. In this chapter, a closer look is taken on cyberethics and computer related issues. Definitions introduced in different literature are brought out to describe cyberethics. Also, three perspectives to cyberethics as a field of applied ethics are introduced. Whether cyberethics is a unique kind of ethics is still an ongoing discussion, and basic views from both sides are brought out later in this chapter.

3.1 Definition of Cyberethics

In literature, there are different definitions describing what is cyberethics and often the term "computer ethics" is used instead to describe the same thing [28]. This is the reason why the term computer ethics is used interchangeably with cyberethics in this paper. Followingly few of the definitions introduced in the literature are brought out.

Article [2] brings out that the foundation to cyberethics (or computer ethics) was laid down by Norbert Wiener on 1940s and 1950s. Although he did not use the term computer ethics nor defined it, he raised questions that are also concerns in today's cyberethics. Questions like what will be the social and ethical consequences of cybertechnology or what are the social and ethical responsibilities for professionals using such technology [2]. The term computer ethics came into usage in the 1970s [2], [29] when Walter Maner started to use it in his papers, presentations and lectures in the university [2]. Maner gave it the following definition: computer ethics studies "ethical problems aggravated, transformed or created by computer technology" [30].

In 1985 James Moor gave the following definition to computer ethics, which is considered wider than Maner's [29]: "computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology" [31]. For many computer and cybersecurity professionals in cyberethics field, this definition has become the "standard" [28].

Still, Tavani argues that Moor's definition and the term computer ethics does not cover wide enough area and uses the term cyberethics instead, by giving the following

definition: “cyberethics can be defined as the study of moral, legal, and social issues involving cybertechnology. Cyberethics examines the impact of cybertechnology on our social, legal, and moral systems, and it evaluates the social policies and laws that have been framed in response to issues generated by its development and use” [17], [28]. Cybertechnology refers to different computing and communication devices [17].

Pruitt-Mentle also uses in her article the term cyberethics and gives the following definition: “cyberethics is the discipline exploring appropriate and ethical behaviors, and the moral duties and obligations pertaining to online environments and digital media. It refers to choices about what is right and wrong in spite of the ability to do something. It includes plagiarism, bullying, and hacking to name a few” [32].

Discussion about which term to use is still ongoing among scientists. To decide which term to use is not a simple task. Still, Onyancha, O. B., compared in his article [33] the usage and meaning of three terms: cyberethics, computer ethics, and internet ethics. At the end of the article, he concluded that there are signs that cyberethics will become the main concept that covers all aspects of both - internet ethics and computer ethics [33].

In this chapter, different definitions of cyberethics used in the literature were introduced. Next, cyberethics as a field of applied ethics is given a closer look.

3.2 Cyberethics as Field of Applied Ethics

In the following chapter cyberethics as a field of applied ethics is examined. Three perspectives of this field are introduced.

Cyberethics is seen as a field of applied ethics [34], [14], [28], [35]. Applied ethics deals with practical ethical issues as mentioned before in chapter 2.1. For example, is it ethical to hack somebody back? Cyberethics investigates moral issues that are relevant to cybertechnology [16]. The range of issues with what cyberethics deals with is wide. The professionals of the field have given three perspectives to this topic [17], [35]:

- Professional ethics perspective: articles [17], [28] state that this perspective includes mainly the analysis of ethical responsibility that computer professionals have. An example of this kind of issue is when a computer professional is asked to design or develop a controversial product [17], [28]. Writings [17], [35] bring

out that parallels are mostly drawn with other professional areas like law and medicine. In these fields, the main concern is the moral responsibility of the professionals. The same analogy is used in cyberethics as a field of professional ethics [17], [35].

- Philosophical ethics perspective: writings [17], [28] mention that compared to professional ethics, where the main issues are usually around responsibility, philosophical ethics covers a wider area of topics. These topics include social policies and individual behavior that affects the general public [17], [28]. For example, issues with privacy, surveillance, and security. These issues do not only influence computer and cybersecurity professionals but everybody in society [14], [17], [28]. In contrast with professional ethics, philosophical ethics does not have an analogy to take from other fields of technologies [17]. In other words, we do not have areas of ethics called, for example "airplane ethics" or "train ethics" [17]. Cybertechnology is so different because it is "logically malleable, its uses often generate policy vacuums and conceptual muddles" [17].
- Descriptive ethics perspective: various moral systems, groups, and cultures have different views on moral issues [17]. Descriptive ethics tries to describe, how different aspects are viewed in these systems [17]. Quite often, when some moral issue is under attention, its sociological aspect is described [17], [35]. Descriptive ethics helps to understand better some normative ethical issues [17], [35]. It gives us a better understanding of how practical ethical issues influence systems policies and laws [17]. Also, it might help computer professionals to design computer systems so that they would refrain social and ethical issues that were made with previous computer system [17].

In this chapter, three perspectives of cyberethics as a field of applied ethics were introduced – professional, philosophical and descriptive ethics. In the following chapter, discussion on the topic whether cyberethics is a unique type of ethics is given.

3.3 Uniqueness of Cyberethics

There is an ongoing discussion among philosophers and experts of its field whether cyberethics is a unique type of ethics or not. Two schools of thought have formed on the subject of this question [17].

One school of thought found that nothing new or unique is in cyberethics issues. For example, Deborah Johnson argues that even though computers make new things possible they still rather adjust old ethical problems by giving them a new point of view [29], [36]. Computers can be replaced with cybertechnology in the context of this paper. She justifies her views with the idea that many of the cyberethics issues are "social value and policy issues", meaning they influence everybody not only computer professionals [36]. Johnson also, argues that majority of the issues that computer professionals face are similar to problems that other groups face or quite often are common issues of business ethics instead [36]. Article [33] brings out that many researchers also do not consider cyberethics as a unique type of ethics [33]. For example, Onyancha brings out that Wong argues in her article [37] that computer or cyberethics does not clearly differ from other ethics, capabilities of computers rather just give a unique character to computer related ethical issues [37].

The second school of thought, on the other hand, argues that forms of behavior, scope, and scale made possible by cybertechnology have raised new ethical problems [17]. For example, Tavani concludes in his book [17] chapter, that talks about the uniqueness of cyberethics, that indeed cyberethics as an independent field of applied ethics is a unique type of ethics. To reason his opinion he uses in Moor's article [38] brought out argument, based on what Tavani states that cyberethics is a unique type of ethics because of the essence of cybertechnology, which differs greatly from similar technologies by the high number of policy vacuums cybertechnology produces [17]. He says that even though the issues might not be completely unique the pressure that it puts on "conceptual frameworks and normative reasoning" is significantly bigger than in other areas of applied ethics [17]. Tavani's idea of the uniqueness of cyberethics issues is also supported by Maner, who argues that some of the ethical issues would not have existed if there were no computer technology. Also, the lack of satisfying analogy from non-computer areas proves in his eyes the uniqueness of computer ethics or in the context of this paper, uniqueness of cyberethics [30]. Moor reasons in his later work, that "no other technology, as revolutionary as it may be for a given area, has and will have the scope, depth, and novelty of impact that computing technology has and will have" making cyberethics a unique kind of ethics [39].

In conclusion, it can be said, that even though the uniqueness of cyberethics is debatable, it has many sides, that can be considered unique.

3.4 Important Issues in Cyberethics

Cyberethics covers a wide area of topics and articles and books bring out different problems. Johnson explains that with the development of computer technology some basic issues stay – "issues of privacy, property rights, accountability, and social values" [36]. Wilk, on the other hand, mentions that currently, the debates are about "surveillance, Big Data, intellectual property of digital content and shaming in social media" [19]. To Vallor et al. important ethical issues in cybersecurity are "harms to privacy", "harms to property", "cybersecurity resource allocation", "transparency and disclosure" and "cybersecurity roles, duties and interests" [11]. However, in this paper, some cyberethics issues that are brought out and shortly discussed are based on Tavani's book [16]. The following chapters give a non-conclusive overview of important issues in cyberethics.

3.4.1 Professional Ethics

One of the major issues according to Tavani's book [16] is professional ethics. More precisely to what extent computer professionals should be considered as responsible if the computer systems fail [16]. Professional ethics perspective was also shortly discussed in chapter 3.2. Under this issue belong, for example, questions like, who is considered liable, when a computer produces an error [16]. These kinds of errors, in some cases, can cause little harm, but for example, if it would be military equipment, errors in a computer system can cost unintended lives [16], [40]. Hence, cybersecurity and computer professionals have a "responsibility to assure the correctness, reliability, availability, safety, and security of all aspects of information and information systems" [40]. Codes of conduct often regulate professional ethics.

Code of ethics – or in other words code of conduct – is defined as "the collection of norms and/or values, that supports solving moral issues in some domain and on the selection of behavior" [41]. Johnson has said that codes of conduct have been developed to describe, what is and what is not expected from computer professionals [36]. Many institutions and organizations have developed their codes of conduct to reflect moral responsibilities that cybersecurity professionals have [29], [40]. Two widely recognized codes of ethics are created by ACM and IEEE Computer Society (IEEE-CS) [19], [42]. ACM and IEEE-CS also have a joint code of ethics ACM/IEEE-CS for software engineers [19], [42]. The

weakness of these codes is that, if a rule has not been added to the code of ethics it might be interpreted as ethically accepted [19].

3.4.2 Security

Kizza [43] defines security as a "means to prevent unauthorized access, use, alteration, and theft or physical damage to property" [43]. Tavani separates security in the context of cybertechnology into three big categories: data security, system security, and network security [16]. Data security is concerned with the confidentiality, integrity, and availability of information [16]. Epstein says that confidentiality, integrity, and availability are views through what security related issues should be analyzed [44]. System security, on the other hand, deals with attacks on system resources and network security with attacks on computer networks [16]. One of the ethical questions in this area is for example, whether it is ethical to use a certain tool or method to defend oneself or organization against an attack or what is the ethical way to behave in case of a situation. When talking about security in cyberethics context, the hacker ethics needs also mentioning.

Usually, the term "hacker" is understood as "a person who accesses computers and information stored on computers without obtaining permission" [5]. These days, hackers with illegal activity, are called "black hat hackers" [45]. However, there are also many cases where hacking is done legally to discover potential threats. This is called ethical hacking [46]. The goal of ethical hacking is to detect threats to avoid future attacks [46]. This kind of ethical hackers, who use their skills for protective goals, are called "white hat hackers" [45], [5]. Also, the third type of hacker exist - "gray hat" hacker [5], [6]. Usually, this kind of hackers do not have permission, but their goal is to enhance the security of a system [6].

Falk analyzes in his paper [6] three types of hackers from the perspective of different ethical theories – utilitarianism, Kant's deontology, and virtue theory. As in the current paper, the main focus has been on deontology and utilitarianism, then these two are described followingly based on opinions brought out in Falk's article [6]. Falk says that from utilitarianism point of view white hat hacker actions are considered ethical because the pain is lightened for the entire group when the weak system crashes. Black hat hacker actions are considered unethical because they violate the greatest happiness principle. He explains his opinion with a thought, that compared to the personal gain that the black hat

hacker gets, causes more pain to the people who are affected by the hacker actions. Determining whether gray hat hackers are ethical or unethical is more complicated because the consequences are unknown [6].

Falk believes that from the perspective of rule deontology, white hat hackers are acting ethically because they must keep the system safe and that is what they are trying to do. Black hat hacker actions are considered unethical because they violate Kant's categorical imperative variation one, mentioned in chapter 2.2.2. To explain his view, Falk brings and example, that black hat hackers abuse the work of system administrators – these administrators are used as means to an end to gain pleasure or some other type of personal gain by the hackers [6]. Still, there may be exceptions to this. For example, if black hat hacker weakens illegal channels [45]. As before, classifying gray hat hackers is more challenging, because the first variation of categorical imperative is followed, but the second variation causes problems, when trying to universalize gray hat hacker actions – it would mean, that everybody is allowed to break into other person's computers without their permission, with the purpose to strengthen it [6].

3.4.3 Privacy

Privacy is considered to be an important subtopic of security. Privacy has received a lot of attention and is especially important in the context of ethics [16], [47]. Book [16] brings out that privacy concerns often emerge because individuals are afraid of losing control over their data. Security concerns, on the other hand, usually rise because people worry that their data may be stolen or changed by unauthorized people. Still, these two quite often overlap [16]. The importance of privacy issues is also evident from the mentioning in different articles about cyberethics. For example, articles [11], [34], [36] bring privacy out as an important ethical issue. For example, data about our healthcare or work. Privacy affects even these people, who have never used a computer in their life [16]. Privacy raises questions like who can have access to data and who controls it or what kind of data can be collected [16]. Privacy violation can also be a situation, where permission to do something, has not been asked. For example, is it ethical to gather information about someone or investigate someone's belongings without their knowing? Usually, it depends on the context in what certain cyberethics issue is investigated. Helen Nissenbaum created a model called 'contextual integrity' [47]. The basic idea of this is

that everything we do happens in a certain context and the context is taken into consideration when examining an issue [47].

3.4.4 Cybercrime

Tavani proposes the following definition to cybercrime: cybercrime is a crime in which "the criminal act can be carried out only through the use of cybertechnology and can take place only in the cyberrealm" [16]. Issues of crime and security often overlap [16]. For example, is hacking somebody back after being a victim of a cybercrime ethical or not? Would it be ethical to commit a cybercrime to avoid greater problems? From the consequentialist point of view, this kind of activity would be ethical because the greater good is produced, but on the other hand, deontologist believe it to be unethical because the act of cybercrime is illegal by definition [16].

3.4.5 Intellectual Property

Tavani says that "the debate over intellectual property rights in cyberspace has become one of the defining ethical issues of the digital era" [16]. This is evident also from the fact, that next to privacy intellectual property is mentioned as an important cyberethics issue in different articles. For example in articles [2], [11], [16], [19], [35], [36], [48], [49], [34]. Intellectual property in cyberethics deals with issues such as "what exactly is it that I own when I own something?" [30]. In other words, who should have the ownership rights, for example deciding who owns the software or digital content [14], [16]. Intellectual property issues do not end, with the question "who owns what" but also, for example, is it ethical to damage someone's property. In most cases, unauthorized damage to property is considered unethical, even if it is not directly regulated by law [11]. However, for example, some consider it to be ethical in case of national security like happened with Stuxnet worm in Iran [11].

To sum up, chapter 3 discussed and described the topics of professional ethics, privacy, security, cybercrime, and intellectual property. Often these issues overlap and are viewed together.

4 Related work

In the previous chapter's basic ideas of cyberethics were given. In this chapter, an overview is given about related work in the field of measuring students' cyberethical behavior and the change in it.

4.1 Measuring the Impact of Teaching Cyberethics

Different articles and books exist that emphasize the importance of teaching cyberethics. Variety of methods and measurements are used to prove the improvement caused by teaching. For example, Lester et al. wrote an article [50] about a full semester course "Professionalism and Ethics", where the emphasis was on teaching cyberethics while using a case-study approach, to computer science students. To measure students' improvement, Critical-thinking Assessment test (CAT) was used before and after the course. The instrument evaluated student's improvement in "individual learning growth in critical thinking skills" [50].

Hirabayashi et al. introduced in their article an instructional method of how to integrate cyberethics thinking into the teaching of "informatic and systematic thinking." [51]. The game, with what cyberethics problem solving was taught, was five days long. It consisted of several steps and presumed, that students were preparing presentation slides. To validate, that the method was changing students attitudes, pre- and posttest were conducted [51].

Some researchers combine cyberethics topic with some other cybersecurity course. For example, as described by Bell et al. in their article [52]. They hold a whole semester lasting introductory cybersecurity course, where one area presented was ethics in cybersecurity. To measure the improvement three sets of interviews were conducted with the students throughout the semester. Teaching methods varied; for example, lecture-based teaching was used for one class and laboratory-based for another. This kind of assessment of improvement is not suitable for current research, because of time limitations [52].

As seen, students' cyberethical behavior and the change in it is not being measured often. Change in behavior indicates that theoretical knowledge learned is also applied in a realistic situation by the student. This is also supported by Leutner and Plass, who found in their research that some shortcomings of the questionnaire can be overcome by using behavioral observations [53]. Often, the improvement in cyberethics knowledge is measured using questionnaires [53] and interviews instead.

4.2 Cyberethical Behavior Measurement

Even though measuring cyberethical behavior is not often used to determine students' improvement, it is used individually, to see students' cyberethical behavior and what it is influenced by.

Majority of the researches use questionnaires to measure students' and others' cyberethical behavior. For example, Chiang et al. analyzed ethical behavior and attitude regarding computer use in Taiwan. The questionnaire, based on the theory of planned behavior (TPB), was developed "to reflect Internet user concerns about the contents of information ethics" [54]. The results indicated that attitude influences behavior positively considering computer ethics [54].

A study conducted by Leonard et al. validated the IT ethical model on students. They found that personal normative beliefs, scenario, "attitude toward ethical behavior, ego strength, relative preference for principled reasoning over conventional and pre-conventional reasoning, and gender" are indicators of ethical behavior intention [55]. To measure these variables also a questionnaire was used [55].

Research written by Mohamed et al. investigated how individual characteristics influence a person's attitude. The research was conducted on academic staff and students in Malasia. The results of these indicated whether a person is inclined towards ethical or unethical behavior while using computers [56].

Gattiker et al. used vignettes to see how people felt about computer-related behavior. Vignettes were about ethical dilemmas concerning computer-related behavior [57].

Athey surveyed IT students to determine their ethical beliefs. Combination of scenarios and ethical problems was used. All the scenarios were formed so that computer-related

issues that IT professionals face were taken into account. The main goal was to compare students and experts' ethical beliefs on this topic. The difference between the two groups was evident from the results [58].

Howard, David developed a Cybersecurity Attitude Scale (CAS) to "measure workers' cybersecurity attitudes", more precisely "cyber policy adherence attitudes and perceived vulnerability to a cyberattack" [59]. Theory of planned behavior was used to model the relationship between cybersecurity attitude and other characteristics [59].

As described before, questionnaires and surveys are widely used to measure behavior and different characteristics that influence it. However, the issue with only using survey is that student's real behavior cannot be fully seen. Shwarz brings out that behavior surveys are strongly influenced by different attributes [60] which often leads to various response biases [61]. It might be two different things, how students think they are behaving and another how they are behaving [61]. Another gap in the literature is that usually, the characteristics that are measured do not include persons ethical views or beliefs.

There is very little literature regarding the actual measurement of cyberethical behavior. Parsons et al. demonstrated convergent validity of questionnaire – The Human Aspects of Information Security Questionnaire (HAIS-Q) - with an empirical phishing study [62]. HAIS-Q measures behavior, attitude, and knowledge. Phishing email studies are usually used to assess students susceptibility or security awareness [62]. In this research, this kind of approach (phishing email study) would not be suitable because the virtual hands-on lab had to be flexible enough to fit with different homework's.

To sum up chapter 4 related work on the topics of how the cyberethical behavior and the impact of teaching cyberethics is measured was given.

5 Methodology

As described in previous chapters cyberethics is an important topic in the current world of cybersecurity. To reduce the likelihood that current IT students will behave unethically in their future work and personal life, we need to educate them about this field of ethics. The content of previous chapters could be used for educating students on those topics. The problem with teaching cyberethics is that it is difficult to assess the student's improvement. One step towards solving this problem would be to develop a method of how to measure students change in their cyberethical behavior. Taking that into consideration one of the goals of this research was to measure the change in students' cyberethical behavior. To achieve this goal following research questions were formed:

RQ 2. How can students' cyberethical behavior be measured?

RQ 3. How much can one lecture influence students' cyberethical behavior?

In this research, a method was decided to develop to assess the behavior of students' in a realistic cyberethics situation. Majority of the researches use interviews and questionnaires to measure cyberethical behavior, for example, researches [9], [52] and [63], but there is a lack of research that would measure how students really would behave if they are fronting a cyberethical dilemma. It is one thing that students' say on paper and another how they behave. To see whether the virtual hands-on lab can be used to measure students cyberethical behavior and how much students' cyberethical behavior can be influenced by one lecture an experiment was created.

The research consisted of 3 phases. In the first phase, preparation was done for the experiment. In the second phase pilot study was conducted and in the third phase, the main study was carried through. Figure 2 depicts the process of research.

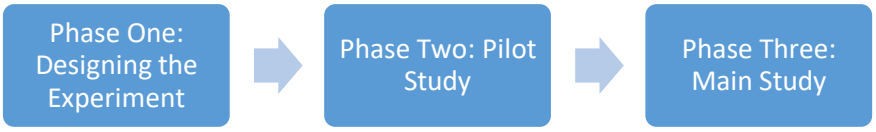

Figure 2. Phases of the research.

In following sections, each of these phases will be given a closer look.

5.1 Phase One: Designing the Experiment

In this chapter, the design of the planned experiment is introduced. First, the overall structure is given, and then each item of the experiment will be given a closer look.

The experiment was designed so that the virtual hands-on lab suitability for measuring students' cyberethical behavior could be tested. Also, a questionnaire was used to measure cybersecurity attitude and ethical views of the students. The questionnaire was created from existing scales – Oxford Utilitarianism Scale, Cybersecurity Attitude Scale, and Human Aspects of Information Security Questionnaire. Ethical views were chosen to be measured, to see how student's personal ethical beliefs are influencing their behavior. According to [34] ethics regulates human behavior. Attitude is found to be in a strong relationship with ethical behavior [9], [63], [64], and for this reason, is measured in this research. Similar design – questionnaire and lab – was, for example, used in research, written by Parsons et al., where convergent validity of the questionnaire was demonstrated with an empirical phishing study [62]. To see whether this same method – virtual hands-on lab - can be used to measure change caused by one lecture about cyberethics pretest-posttest approach was taken as suggested by Fraenekel et al. [65] and Cohen et al. [66].

At the beginning of the experiment twenty-six-question questionnaire (marked as "QUEST." in Figure 3 and Figure 6) was given to students to get a preliminary overview of the current situation, students ethical views, and cybersecurity attitude. Chapter 5.1.2 gives a more detailed look at the questionnaire. Students had 5 days to answer to the questionnaire. This timeframe for the questionnaire and following parts of the experiment were set by the course, where the experiment was tested. The design of the experiment can be seen in Figure 3. The boxes with the same color represent the same treatment in the experiment. For example, blue color on GX-L1 and GY-L1 mean that both of the groups did the same lab.

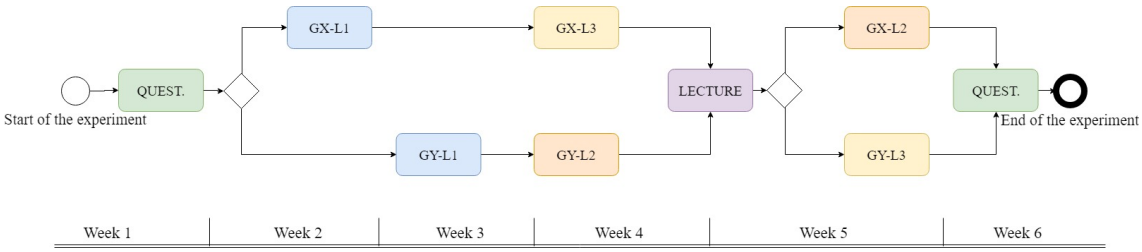

Figure 3. Design of the experiment.

To see whether the lab content and the time of conducting the labs have any impact on the results, students were randomly divided into two subgroups – group X (GX) and group Y (GY). Equivalency of groups can be assumed because of the randomization [65]. Fraenkel et al. say that randomization ensures that extraneous variables are controlled [65]. This is also supported by Cohen et al. [66].

After filling in the questionnaire first virtual hands-on lab (marked as "GX-L1" in Figure 3 and Figure 6) was given to group GX. The virtual hands-on lab is described in more detail in chapter 5.1.1. Students had 5 days to do the lab. As before, the time limit was set by the course, where the experiment was conducted. After group GX had finished group GY started the same lab (marked as "GY-L1" in Figure 3 and Figure 6). Lab 1 was given on different weeks to see how the time gap between the labs influences the results. When lab 1 (L1) was done by both of the groups (GX and GY) the second phase of pre-test labs started. In this step subgroups, GX and GY received different labs. GX started with lab 3 (L3)(marked as "GX-L3" in Figure 3 and Figure 6) and GY with lab 2 (L2)(marked as "GY-L2" in Figure 3 and Figure 6).

Right after the end of the pre-tests – questionnaire and labs – lecture (marked as "LECTURE" in Figure 3 and Figure 6) about cyberethics was given to students. The description of the lecture is given in chapter 5.1.3. Both groups received the lecture at the same time. When the lecture ended, new labs were opened. This time group GX received lab 2 (L2)(marked as "GX-L2" in Figure 3 and Figure 6) and group GY lab 3 (L3)(marked as "GY-L3" in Figure 3 and Figure 6). Crossover design was decided to take into usage because of the advantage of serving individuals in all of the behavior labs. Crossover design allows to measure the impact of individual behavior and also to look at the cumulative of an individual participating in both conditions [67]. Also, it shows whether the content of the lab influences the outcome. After all the labs were done the same questionnaire that was given at the beginning of the experiment was given again to compare them with the results received at the beginning.

In the following chapters, each of these components of the experiment is taken under a closer look.

5.1.1 Virtual Hands-on lab

Many of the topics in cybersecurity are connected to asking permission. Quite often the ethicality and legality of actions are dependent on having permission or not. For this reason, in current research, the approach of asking permission in a virtual hands-on lab was taken. A virtual hands-on lab is a virtual machine running on the IT platform, where students can carry out various tasks [68]. The content of these labs was not created by the author of this paper.

The hands-on labs were created in a virtualized environment so that the actions of students could be monitored. Asking permission was added to three labs – lab 1 (L1), lab 2 (L2) and lab 3 (L3) - with different tasks (reverse engineering (L1), SQL injection (L2), OSINT (L3)). Students were given a role of a worker and were told, that before they can start with the task, they have to ask for written permission from the company. However, as the co-worker, who was supposed to answer them, was on a holiday, then the reply to the letter might come in 72 hours. Actually, the reply was given in no more than 24 hours. Students had 5 days to complete the assignment. If the student chose not to ask permission, then there was a small risk of losing points. The probability of losing points depended from the lab also. In L1 the chance of losing points, when not asking permission, was 1 from 10000, but in L2 and L3 1 from 100. The aim of this was to see, if the chance of losing points was higher, whether students are more likely to ask permission or not. Extra points to students who asked permission were not given.

The answer to the student's first email was given within a timeframe of three hours to twenty-four hours. Minimum time was set to three hours so that students had to wait a bit of time before getting permission. Maximum time, twenty-four hours, was chosen so that the researcher would have time to answer everybody and so that the waiting time would not be too long. The exact time of waiting differed for each student because answers were written manually to each student.

Both subgroups – GX and GY – were again randomly divided into two. GX was divided into subgroups GX-1 and GX-2. GY was divided into subgroups GY-1 and GY-2. There were two options for answers based on the subgroup – answer 1 (A1) or 2 (A2). Answer 1 (A1) was a simple reply with the message "OK". Answer 2 (A2) gave them an additional (very simple) task. For example, students were asked to confirm, whether they are from the company's CERT department ("Hi, just to confirm - are you part of our CERT

department?") or, if they already mentioned their work position, to solve an easy CAPTCHA ("Hi, just to be sure - please solve this CAPTCHA: how much is 1234 plus 103?"). After receiving a reply answer with a confirmation or correct CAPTCHA answer, a message containing the permission to start the lab was sent ("OK, you have permission"). The language of an answer – Estonian or English - depended on the student's email. Two different answers were given to see whether the type of reply has any impact on the results of the lab. Students, who received answer 2 (A2) were in the position, where they had to wait longer and put more effort to get the permission.

Example answers to one of the labs can be seen in Figure 4. The color yellow represents the actions made by the student. The color blue represents the message content sent back to the student by the researcher. In parallel students' actions in the virtual lab are monitored to compare the time when they start the lab in real and when they receive an email with permission. The waiting time is measured as the difference between the time the researcher receives an email and the time student receives a reply message with permission. In both groups the researcher answers within 24 hours, but in this group, where student receives A2 answer, the time it takes for a student to reply is also added to the measurement. Hence, for students who receive A2 answer, this waiting time might be longer than 24 hours, because student has to reply to researchers' email before receiving permission.

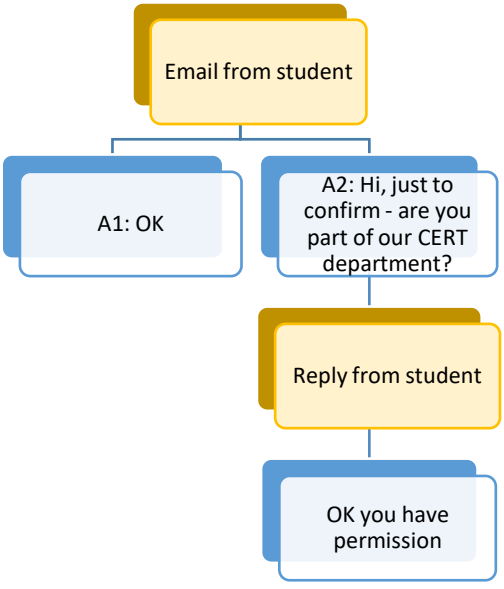

Figure 4. Example answers to student's email in one lab.

In lab 1 (GX-L1 and GY-L1) answer 1 (A1) was received by groups GX-1 and GY-1 and answer 2 (A2) by groups GX-2 and GY-2. In the second part of labs (GX-L3 and GY-

L2), the types of answers were converted between the groups. Group GX-2 and GY-2 received answer 1 (A1) and groups GX-1 and GY-1 answer 2 (A2). This was done to understand, what influences the results – whether students' results change, depending on the type of answer they receive. Each student received both types of answers, A1 and A2. This allows comparing results of the answer types without the influence of the intervention of the lecture. In the third part of the labs (GX-2 and GY-3), after the lecture, groups GX and GY were both divided randomly into two subgroups. Group GX was randomly divided into two subgroups – GX-3 and GX-4 – and same with group GY – GY-3 and GY-4. This was done so that students from both of the pre-test subgroup would receive answers A1 and A2 without the bias from the previous group allocation. Example of the lab subgroups and the answer they received can be seen in Figure 5. On the figure can be seen that in lab GX-L1 students, who were in subgroup GX-1 received answer A1 and students, who were in group GX-2, received answer A2.

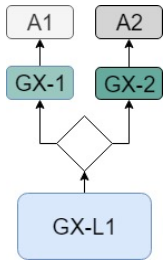

Figure 5. Example model of the answer types to students.

The goal of these labs was to see whether students would ask for permission before starting their task or not. The actions students take during this exercise show their cyberethical behavior. Though it does not give a full picture of students' behavior in real-life, it gives an idea, how they probably will act in a similar situation.

5.1.2 Attitude and Ethical Views Questionnaire

According to [62] behavior and attitude are in a strong positive relationship [62]. On the other hand, ethical behavior relates to ethical beliefs. Whether it is consequences of one's actions that matter or the act itself might influence people's behavior [34]. Article [34] says that people's behavior is regulated by ethics [34]. To measure attitude and ethical views a questionnaire was developed. The questionnaire was added to the experiment to compare the results from virtual hands-on labs with the values that were self-reported in the questionnaire.

Many theories have been developed to explain the influencers of behavior. Theories like Theory of Planned Behavior [69], Protection Motivation Theory [70] and Knowledge-Attitude-Behavior model [71]. However, these theories are only assessing, according to Parsons et al., "the variables in the theory under investigation, other potentially important variables are not considered" [72]. For this reason, no specific one model is being followed in this research and only attitude and ethical views are taken under a closer look.

As described in the previous chapter (chapter 2.2) two main ethical theories that are compared the most are deontology and utilitarianism [20]. For this reason, in this research, deontological and utilitarianism views are measured. Trolley-type dilemmas have been a common way to study people's ethical views between utilitarianism and deontology [73]. Lately, some have started to argue, that these kinds of problems do not give a full overview, because they only focus on the instrumental harm, meaning only the willingness to sacrifice someone is measured [73]. Kahane et al. bring out in [73] that also positive side or in other words impartial beneficence should be measured. To address this issue, Kahane et al developed a new scale called The Oxford Utilitarianism Scale (OUS) [73]. According to [73] OUS consists of 9 questions, from what first five measure impartial beneficence (IB) and last four instrumental harm (IH). 7-point Likert scale is used to measure, how much person agrees to the given statement. People who score higher on the scale are considered with utilitarianism views and people who score lower with deontological views. This scale does not strictly categorize people into deontologist or utilitarians; it rather gives a matter of degree [73].

The subscale of instrumental harm shows the negative side of utilitarianism, how willing is a person to harm someone for greater good [73]. Impartial beneficence measures more of the positive side, the concern for others, greater good and future generations [73]. This dimension shows how much is cared for the "well-being of all sentient beings on the planet" [73].

Because of the better coverage of both positive and negative side of utilitarianism this scale was decided to take into usage in current research. Even though in the original questionnaire a 7-point Likert scale was used, in this research 6-point Likert scale was used instead to avoid the answer "Neither Agree or Disagree". Also, article [74] concluded that the 6-point Likert scale has a higher level of reliability and discrimination

in psychology tests [74]. Likert scales are often used in the researches to measure attitude and student views [75].

As said before, attitude is found to be in a strong relationship with intentions to behave ethically or not [9]. Leonard et al. have said that through attitude it is judged whether the act is good or not [63]. They found in their study that the consequences of behavior have an influence on people's attitude to behave ethically [63]. Ajzen concludes in his article that attitude measurement is an essential tool to understand behavior [64]. Research [76], conducted by Hadlington that investigated the correlation between employees' attitudes towards cybersecurity and risky online behavior in the United Kingdom found that there is an interplay between these two. Lack of knowledge, skills, and awareness were found to be the key problems, why employees do not practice actively safe cybersecurity behavior [76].

To measure attitude towards cybersecurity Howard developed The Cybersecurity Attitude Scale (CAS) [59]. According to [59] CAS gives a better understanding, why people behave the way they do. This scale measures the following: "cyber policy adherence attitudes and perceived vulnerability to a cyberattack" [59]. [59] brings out that CAS consists out of 10 items. First five measure policy adherence (PA) and the last five perceived vulnerability (PV). 5-point Likert scale is used to measure, how much people agree to each statement [59]. Policy adherence subscale shows how an individual feels about following rules and policies. Perceived vulnerability, on the other hand, measures what kind of attitude a person has towards vulnerabilities and how does (s)he perceives it [59]. As both following policies and being aware of threats and vulnerabilities is an important part of cyberethics this scale was decided to be used in this research. For the same reasons, why OUS was modified from 7-point to 6-point Likert scale, CAS items are measured in this research also on a 6-point Likert scale.

Additionally, to the 10-item attitude scale, seven questions from The Human Aspects of Information Security (HAIS-Q) were decided to use to add a third dimension – own responsibility - to the attitude scale. HAIS-Q is a questionnaire developed by Parsons, et al. to measure information security awareness (ISA) [62]. According to [62] with HAIS-Q it is possible to predict information security behavior. HAIS-Q consists of 63 items and has seven focus areas: "Password management, Email use, Internet use, Social media use, Mobile devices, Information handling and Incident reporting" [62]. Each of these areas

is additionally divided into three sub-areas – knowledge, attitude and behavior [62]. The items were selected from the behavior area so that each of the seven sub-areas would be covered – one item from each of the sub-areas. These seven questions were chosen to see how students feel about taking their own responsibility to behave in a secure way. Like previously 6-point Likert scale was used to measure the answers.

As these scales – CAS and HAIS-Q - are aimed at organization employees and the items are developed from the perspective of the organization, an introductory description was given to students. This description was formed based on the web pages of IT companies. Based on this description a control question was asked to make sure students had read through the introduction given to them.

As a result of combining OUS, CAS and HAIS-Q 26 item questionnaire (marked as "QUEST." in Figure 3 and Figure 6) with additional control question formed. The questions can be seen in Appendix 1 – Questionnaire.

5.1.3 Cyberethics Lecture

The experiment measured the effect of the impact of a lecture about cyberethics (marked as "LECTURE" in Figure 3 and Figure 6). The topics covered in this lecture are brought out in chapters 2 and 3 of this thesis. Additionally, some theoretical background situations, that have happened recently and have been talked about in media, are brought out, and students' opinion about the ethicality of them is asked using Kahoot!. Kahoot! (https://kahoot.com/) is a free online tool to create quizzes and present them in the classroom [77]. Using game-based learning is seen as good practice to engage students to the class activity and review the content presented [78]. Kahoot! also motivates students to listen and participate actively in the lecture [77]. The problems mentioned in the lecture include, for example, Twitter bug, that resulted in some of the private tweets to be seen by the public [79]. The cyberethical aspect that can be discussed around it, for example, is whether it is ethical to notify the publicity before the bug is fixed or not. Also, topic, how would it have been correct to behave in the labs, was touched. The lecture was presented by a third party so that it would be possible to observe it from the side.

Figure 6 illustrates the above-described process of the experiment in more detail with the subgroups and the types of answers they received in each step. Boxes that are colored with the same tone suggest that the treatment given is the same.

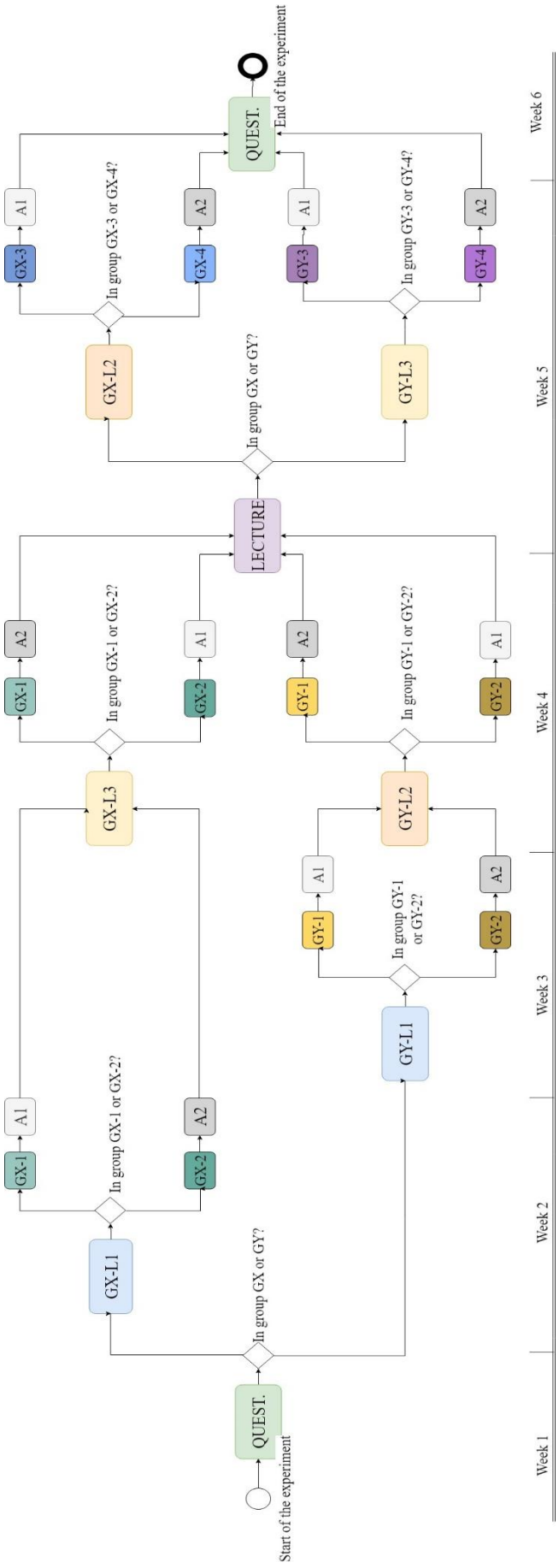

Figure 6. Design of the experiment – in more detail.

5.1.4 The Environment of the Experiment

In this chapter, an overview is given of the environment in which the experiment was created.

The questionnaire was given to students through Tallinn University of Technology (TalTech) IT courses Moodle (https://ained.ttu.ee/). Moodle is an online environment, where teachers can give assignments, and other materials to students and students can upload their work and check grades. Behavior lab assignment descriptions were also given through this environment.

The email account on what students had to send an email was created with ProtonMail (https://protonmail.com). ProtonMail is an email service that provides end-to-end encryption.

Labs into what the behavior part was added were created with TalTech i-Tee (elab.cs.ttu.ee). i-Tee is a "fully automated Cyber Defense Competition platform", where students can also solve hands-on labs in a virtualized environment [68]. The timestamp, when the students started their lab, was received from this environment's logs.

5.1.5 Expert Interview

Before the pilot study, a semi-structured expert interview was made with the expert in the field of psychology, to improve the validity of the questionnaire, behavior labs and the overall design of the experiment. Having an expert interview is also suggested by Creswell to identify the validity of questions [80]. The expert interview offers a useful way how to get good results quickly [81]. Harvey-Jordan et al. bring out that the advantage of the semi-structured interview is the "richness of data they yield" [82]. The interviewee can speak openly, and this helps to get the most important issues to be brought out [82].

During the interview questionnaire, behavior labs and the structure of the experiment were discussed. Based on the feedback some changes were made, for example, one of the recommendations made by the expert was to add additional questions to cybersecurity attitude scale, that would give a better understanding of students' attitudes towards taking responsibility of keeping themselves safe. Seven HAIS-Q questions, like described in chapter 5.1.2, were decided to take into usage, to address this issue.

5.2 Phase Two: Pilot Study

In the previous chapter, an overview was given about the overall structure of the experiment and each component separately. In this chapter, the conducted pilot study will be introduced.

A pilot study was conducted before the start of the actual experiment to see the flaws and improve the experiment where needed. The questionnaire, behavior labs, and lecture were tested on three students using the think-aloud method. Cotton and Gresty state that think-aloud method is a useful method to evaluate someone's decision and thought process when performing a task [83]. Students participating in the pilot study were asked to verbalize their thoughts to get a better understanding of their thinking process. Notes were taken in parallel, with the study.

Based on the notes collected, some lecture wordings were taken under closer look to improve their understandability. Questionnaire items got overall good feedback; no changes were made on them based on the pilot study. When testing the behavior labs, it came out that one of the students would not ask permission and would start solving the lab right away to save time. The other two students noted that they would ask permission first. The comments made were taken into consideration when starting the actual experiment.

Even though the parts of the experiment were tested individually the whole experiment was not tested altogether. This is a limitation in this work because the real outcome cannot be fully predicted.

5.3 Phase Three: Main Experiment

In this chapter, an overview of the actual experiment will be given. Before the start of the experiment a written permission was asked from the students.

The experiment started at the end of February 2019 and continued throughout March. Participants of the experiment were from Tallinn University of Technology. The method was tested on course Foundations of Cyber Security (course code: ITI0103) students. This course is aimed at IT bachelor first-year students. There were altogether 99 students, who participated in the course in the spring semester of 2019.

To ensure anonymity of students, they were asked to select an alias for themselves and use it instead of their name when solving the labs and questionnaires.

The sample size consisted of 86 students. The size of the sample was chosen because of the accessibility to this group of people. Because the target group is mostly first-year IT bachelor students and research was conducted on them, then the results should not be generalized. The limitation of this sample size was the lack of possibility to generalize the results. Cohen et al. suggest in their book [84] (Box 4.1 Sample size, confidence levels and confidence intervals for random samples, page 104) that the sample size for the population of 100 students with confidence level of 95% should be 86 students and with a population of 75 students it should be 67 [84]. The population for this experiment is 86 students, the number of students, who participated, fits between these limits to gain 95% confidence level.

To analyze the data, Microsoft Excel 2016 and R were used.

5.4 Results

In the following chapter, the results gathered from the experiment and analyzing the methods used will be introduced.

From 99 students participating in this course, 86 gave permission, that their results may be used in the experiment. 13 students' results, who did not agree, were removed from the analysis. All the students, who gave permission, answered the pre-questionnaire and 81 students answered the post-questionnaire. 45 students were in group X (GX) and 41 students in group Y (GY). The small gap between the number of students came because all of the (99) students were randomly distributed into two groups. There were more students in group GY, who did not give permission for their data to be used in the experiment. From 86 students, who gave permission to use their data in the research, 73 participated in the lecture, from whom 39 (53%) were in group GX and 34 (47%) in group GY. Figure 7 depicts the distribution of students in percentage who participated in the lecture and also gave permission, that their data may be used in the research, from the point of view of subgroups GX and GY. Students, who did not participate in the lecture were removed from the later analysis.

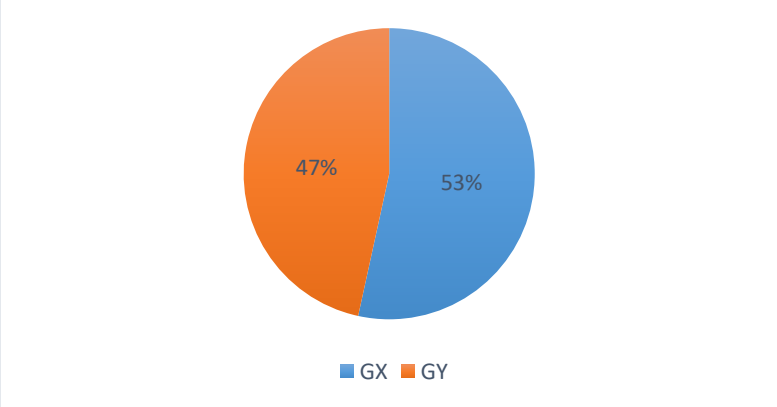

Figure 7. Percentage of students in groups GX and GY, who gave permission and participated in the lecture.

In group GY-1 were 17 (23%) students and in GY-2 17 (23%). In group GY-3 18 (25%) students were distributed and into group GY-4 16 (22%) students. Group GX-1 consisted out of 18 (25%) students and group GX-2 out of 21 (29%) students. In group GX-3 were 18 (25%) students and in group GX-4 were 21 (29%) students. From 73 students 12 (16%) were women, and 61 (84%) were men. Figure 8 illustrates the proportion of women and men participating in the experiment in percentage. Figure 9 illustrates the distribution of

men and women in the groups in percentage. In group GX were 5 women (13%) and in group GY 7 (21%) women.

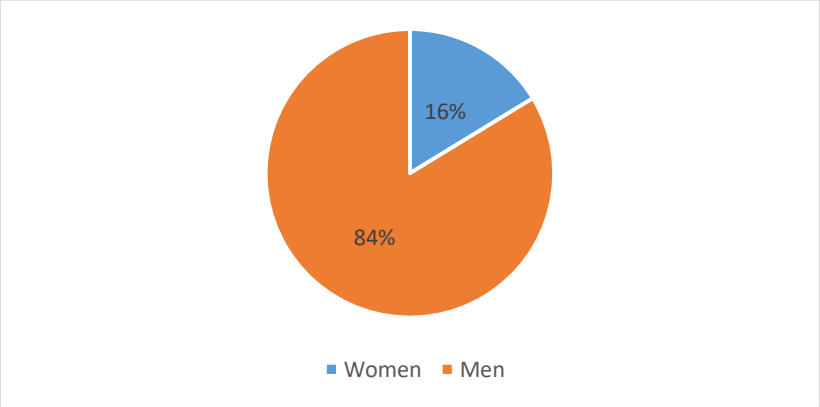

Figure 8. Students divided by gender in percentage.

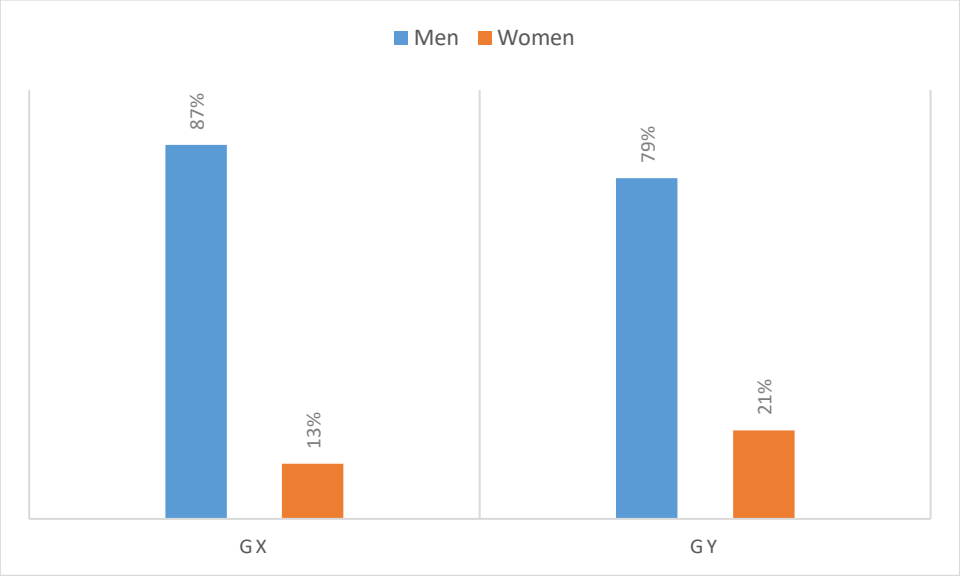

Figure 9. Distribution of men and women in groups GX and GY in percentage.

The experiment started with conducting the questionnaire. 86 students gave responses. 8 students failed in the attention check (a simple question that is easy to answer wrong if the question text is not read properly). These students' results were also removed from the pre-questionnaire analysis. Also, students, who did not participate in the lecture were removed from the analysis. In the end, 65 students' pre-questionnaire results were analyzed. 21 students (32%) were with utilitarianism views and 44 (68%) deontological views, based on the OUS. In group GX 25% and in group GY 41% of the students were classified as with utilitarianism views. Over half of the students (63%, 41 students) scored

low on the impartial beneficence scale and also on the instrumental harm scale (65%, 42 students).

All the students felt that following policies and rules is important. Perceived vulnerability shows somewhat different results. 9 students (14%) did not discern their vulnerability very highly. On HAIS-Q 1 (2%) student does not value own responsibility highly.

The experiment ended with conducting the same questionnaire as at the beginning. 81 students gave responses. 8 students failed in the attention check. These students' results were removed from the post-questionnaire analysis to improve the validity of the experiment. Results of the students, who did not participate in the lecture were removed. In the end, 66 students' post-questionnaire results were analyzed. 21 students (32%) were with utilitarianism views and 45 (68%) deontological views, based on the OUS. Over half of the students (65%, 43 students) scored low on the impartial beneficence scale and also low on the instrumental harm scale (64%, 42 students).

8 students (12%) scored low on perceived vulnerability (PV). On HAIS-Q 4 students scored low (4%), 2 students in both groups.

5.4.1 Cronbach Alpha of Pre- and Post-questionnaire

To check the internal consistency of pre-questionnaire Cronbach alpha (α) was calculated on the questionnaire each subscale separately. Results in OUS are minimally reliable, according to [84]. Only subscale of instrumental harm (IH) can be considered as reliable. Cronbach alpha calculated for cybersecurity attitude scale (CAS) shows highly reliable results, according to Cohen et al. [84] and also for both of the subscales – perceived vulnerability (PV) and policy adherence (PA). Cronbach alpha for overall the attitude scales – HAIS-Q and CAS – shows also reliability, but HAIS-Q individually cannot be considered as reliable because of the alpha value α = 0.48. Cohen et al. consider alpha value lower than 0.60 as unreliable [84]. Results can be seen in Table 1.

Table 1. Cronbach alphas of pre-questionnaire.

	OUS (IB+IH)	**IB**	**IH**	**CAS (PA+PV)**	**PA**	**PV**	**HAIS-Q**	**CAS+HAIS-Q**
Cronbach alpha	0.66	0.68	0.75	0.81	0.77	0.86	0.48	0.74

To compare the internal consistency of pre-questionnaire with post-questionnaire Cronbach alpha (α) was calculated again on the on questionnaire (post-questionnaire) each subscale separately. Results indicate that the internal consistency is reliable for all the scales ($\alpha > 0.70$). Results can be seen in Table 2.

Table 2. Cronbach alphas of post-questionnaire.

	OUS (IB+IH)	**IB**	**IH**	**CAS (PA+PV)**	**PA**	**PV**	**HAIS-Q**	**CAS+HAIS-Q**
Cronbach alpha	0.76	0.72	0.74	0.89	0.89	0.90	0.75	0.82

5.4.2 Spearman's Rank-order Correlation of Pre- and Post-Questionnaire

For analyzing ordinal data, article [75] suggests using Spearman's rank-order correlation [75]. Spearman's rank-order correlation (r_s) was calculated to see the correlation between questionnaire items. First, Spearman's rank-order correlation was calculated on pre-questionnaire. Oxford Utilitarianism Scale (OUS) two subscales IB and IH do not show any correlation between them ($r_s = -0.01$, $p = 0.98$). Also, the subscales (PA and PV) of Cybersecurity Attitude Scale (CAS) do not show strong correlation ($r_s = 0.28$, $p = 0.03$) between each other, but the correlation between perceived vulnerability (PA) and HAIS-Q items is evident ($r_s = 0.40$, $p < 0.001$). Interestingly, the correlation ($r_s = 0.25$, $p < 0.05$) between CAS overall results and HAIS-Q items results is not as strong as was between PA and HAIS-Q. The calculated Spearman's correlations can be seen in Table 3.

Table 3. Spearman's rank-order correlation between pre-questionnaire scales.

	1	**2**	**3**	**4**	**5**	**6**	**7**
1. OUS (IB+IH)	1						
2. IB	0.76	1					
3. IH	0.58	-0.00	1				
4. Attitude (CAS+HAIS-Q)	-0.05	-0.08	-0.05	1			
5. CAS (PA+PV)	0.03	-0.01	0.01	0.86	1		
6. PA	-0.02	-0.02	-0.07	0.67	0.68	1	
7. PV	-0.01	-0.07	0.03	0.69	0.88	0.28	1
8. HAIS-Q	-0.26	-0.24	-0.17	0.67	0.25	0.40	0.08

Spearman's correlation (r_s) was also calculated on post-questionnaire to see the correlation between questionnaire items and compare them to pre-questionnaire. Oxford Utilitarianism Scale (OUS) two subscales IB and IH do not show a correlation between them ($r_s = 0.21$, $p = 0.11$). Also, the subscales (PA and PV) of Cybersecurity Attitude Scale (CAS) do show a weak correlation ($r_s = 0.44$, $p < 0.001$) between each other. A moderate correlation ($r_s = 0.60$, $p < 0.001$) between HAIS-Q items and CAS is seen and also between CAS subscales (PA: $r_s = 0.60$, $p < 0.001$ and PV: $r_s = 0.46$, $p < 0.001$) and HAIS-Q. The calculated Spearman's correlations can be seen in Table 4.

Table 4. Spearman's rank-order correlation between post-questionnaire scales.

	1	**2**	**3**	**4**	**5**	**6**	**7**
1. OUS (IB+IH)	1						
2. IB	0.80	1					
3. IH	0.70	0.21	1				
4. Attitude (CAS+HAIS-Q)	-0.06	-0.12	0.12	1			
5. CAS (PA+PV)	-0.09	-0.16	0.15	0.91	1		
6. PA	0.07	-0.00	0.21	0.76	0.75	1	
7. PV	-0.12	-0.19	0.09	0.80	0.90	0.44	1
8. HAIS-Q	-0.04	-0.07	0.06	0.86	0.60	0.60	0.46

Spearman's rank-order correlation was also calculated between questionnaires and behavior in the labs. No significant correlation was observed.

5.4.3 Behavior in the Virtual Hands-on Labs Before the Lecture

To measure students' activity in the virtual hands-on labs, they were classified, based on their actions, into six groups:

T1. Students, who asked permission and did not start the lab before receiving one.
T2. Students, who asked permission but started the lab before they received it.
T3. Students, who asked permission, but after receiving answer type A2 did not reply and hence did not receive permission to start the lab but nevertheless did so.
T4. Students, who asked permission and received permission, but did not start the lab (did not get results).
T5. Students, who did not ask permission but started the lab.
T6. Students, who did not ask permission nor started the lab.

As a lab starting time was used the timestamp of the submission of the first correct flag. It was chosen because this way it was made sure that the student had done something in the virtual lab and not just opened it. Also, the timestamp of finding first correct flag was a common nominator in all the labs.

In lab GX-L1 9 students (23%) waited for permission before starting the lab (T1); 15 students (38%) asked permission but started the lab before receiving it (T2); 5 students (13%) did not ask permission but started the lab (T5); 2 students (5%) asked permission but did not start the lab (T4); 7 students (18%) did not ask nor completed the lab (T6); 1 student (3%) did not respond (T3) when received answer type A2. Overall 27 students asked permission (69%) and 26 students (67%) got permission. The average time spent on waiting (time difference between the letter sent by the student, to ask permission, and reply message with permission sent back to student; see chapter 5.1.1 for description of waiting) was 10 hours and 42 minutes, minimal time waited by a student was 3 hours and 4 minutes and maximum time waited by a student was 36 hours and 31 minutes.

Figure 10 depicts the behavior in lab GX-L1 and in following labs (GX-L2, GX-L3, GY-L1, GY-L2, GY-L3) in percentages. The red line indicates the lecture. Items that stay before (left from) the red line are labs that were given before the lecture and labs after the red line were given after the lecture.

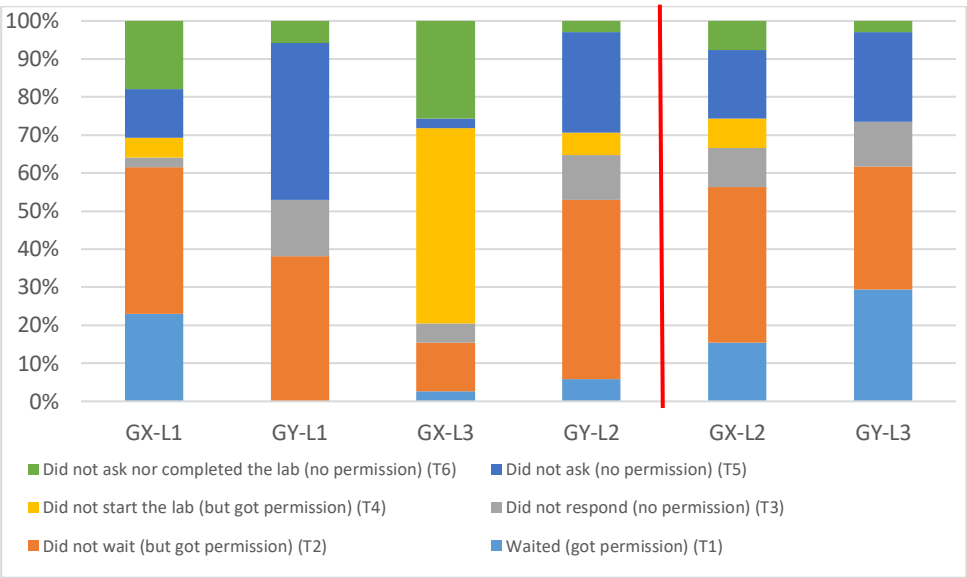

Figure 10. Diagram describing the results in the labs.

In lab GY-L1 (see Figure 10) not a single student waited for the permission letter before starting the lab (T1). 13 students (38%) sent a letter to ask permission but did not wait for reply (T2); 14 students (41%) did not ask permission at all (T5); 5 students (15%) sent a letter to ask permission, but did not respond, when they received answer 2 (A2) – so they did not receive permission (T3). 2 students (6%) did not ask for permission nor completed the lab (T6). Overall 18 students asked permission (53%) and 13 students (38%) got permission. The average time spent on waiting (see chapter 5.1.1 for description of waiting) was 12 hours and 40 minutes, minimal time waited by a student was 3 hours and maximum time waited by a student was 38 hours and 54 minutes.

In lab GX-L3 (see Figure 10) only 1 student (3%) waited before starting the lab until receiving permission (T1). 5 students (13%) sent a letter but did not wait for a reply (T2). 1 student (3%) did not ask for a permission (T5); 20 students (51%) did not start the lab but asked for permission (T4); 2 students (5%) who got answer type A2 did not reply so they did not get a permission (T3); 10 students (26%) did not ask for permission, and neither completed the lab (T6). Overall 28 students asked permission (72%) and 26 students (67%) got permission. The average time spent on waiting (see chapter 5.1.1 for description of waiting) was 17 hours and 43 minutes, minimal time waited by a student was 3 hours and 36 minutes, maximum time waited by a student was 105 hours and 42 minutes

In lab GY-L2 (see Figure 10) 2 students (6%) waited with starting the lab before receiving permission (T1); 16 students (47%) asked permission but did not wait (T2); 9 students

(26%) did not ask permission at all (T5); 2 students (6%) asked permission but did not start the lab (T4); 4 students (12%) asked permission, but when receiving answer type A2 they did not respond so they did not have permission (T3); 1 student (3%) did not ask permission nor completed the lab (T6). Overall 24 students asked permission (71%) and 20 students (59%) got permission. The average time spent on waiting (see chapter 5.1.1 for description of waiting) was 9 hours and 48 minutes, minimal time waited by a student was 3 hours and 5 minutes, the maximum time waited by a student was 45 hours and 49 minutes.

5.4.4 Lecture

The lecture was observed from the side by the researcher. This was done to get a better overview of the strengths and weaknesses of the lecture. In the lecture, 73 students, who gave permission to use their data, participated. Kahoot! questions proved to be a useful way of keeping students interested and listening to the lecture. Students were given feedback, how would it have been ethical to behave in the labs, but it could have been emphasized more to make sure students heard and remembered it. Feedback collected after the lecture was mainly positive. Students assessed the interestingness and usefulness of the lecture on 6-point Likert scale, starting from 0 (Strongly disagree) and ending with 5 (Strongly agree), additional option of not giving comments was also given to students. Results indicate that students found the lecture both interesting and useful. 93% of students scored 3 or higher on the interestingness scale and 89% on the usefulness scale. Figure 11 describes the feedback distribution among answers on Likert scale. On vertical axis can be seen the percentage of students and on horizontal axis the answer options from Likert scale. Both, interestingness and usefulness, were brought out in the figure. Some comments brought out by students were following (the comments have been translated from Estonian):

1. “This time the lecture was really interesting and with Kahoot! tests also interactive.”
2. “The best lecture till now, the topic was very interesting, presented almost perfectly, entangled to be active and listening throughout the lecture.”
3. “In my opinion, it was good that Kahoot! tests were used throughout the lecture; it made things more interesting, forced to pay more attention with a sleepy head. I think it was awesome.”

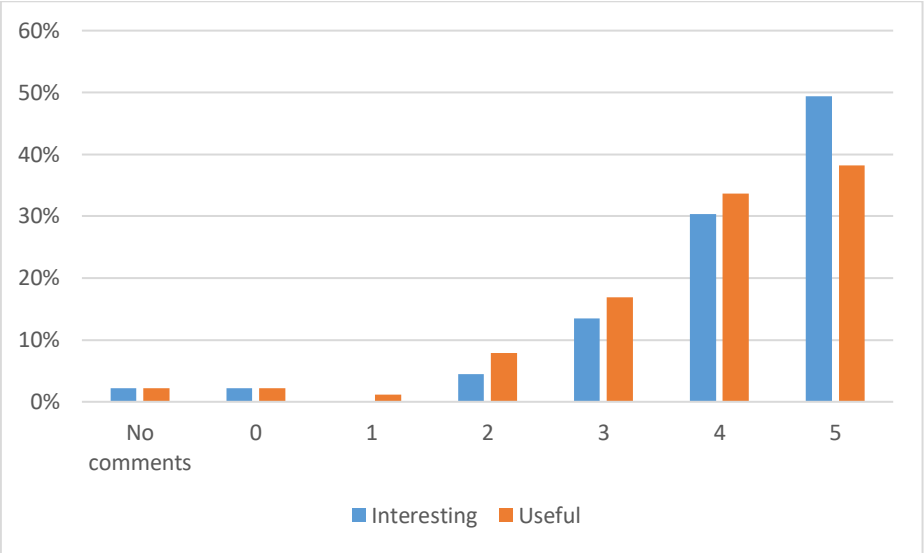

Figure 11. Feedback from students on the lecture.

5.4.5 Behavior in the Virtual Hands-on Labs After the Lecture

After the lecture was conducted, labs GY-3 and GX-L2 were presented to students. In lab GY-L3 (see Figure 10) 10 students (29%) waited before starting the lab for permission (T1). 11 students (32%) sent a letter but did not wait for a reply (T2). 8 students (24%) did not ask for permission but started the lab (T5). 4 students (12%) sent a letter, but as they got an answer type A2, they did not reply and hence did not receive permission (T3). 1 student (3%) did not ask for permission nor completed the lab (T6). Overall 25 students asked permission (74%) and 21 students (62%) got permission. The average time spent on waiting (see chapter 5.1.1 for description of waiting) was 8 hours and 55 minutes, minimal time waited by a student was 3 hours, maximum time waited by a student was 20 hours and 1 minute.

In lab GX-L2 (see Figure 10) 6 students (15%) waited before starting the lab for permission (T1). 16 students (41%) sent a letter but did not wait for a reply (T2). 7 students (18%) did not ask for permission but started the lab (T5). 4 students (10%) sent a letter but as they got an answer type A2 they did not reply and hence did not receive a permission (T3). 3 students did not ask for permission nor completed the lab (8%) (T6). 3 students (8%) asked permission but did not start the lab (T4). Overall 29 students asked permission (74%) and 25 students (64%) got permission. The average time spent on waiting (see chapter 5.1.1 for description of waiting) was 10 hours and 55 minutes, minimal time waited by a student was 3 hours, maximum time waited by a student was 67 hours and 5 minutes.

5.4.6 Answer Type and Time Waited for Permission in the Lab

The type of answer that students received, A1 or A2, played a small role in the results of labs, though it can be seen that the percentage of students who waited before starting the lab (T1) was almost always higher, where A1 answer was received. Only exceptions are in groups GX-L3 and GY-L1. Figure 12 illustrates the distribution of students in percentage based on the answer type and their behavior. On the vertical axis can be seen the number of students in each category and on the horizontal axis the lab type and the answer type. Students, who did not ask permission were excluded from this diagram.

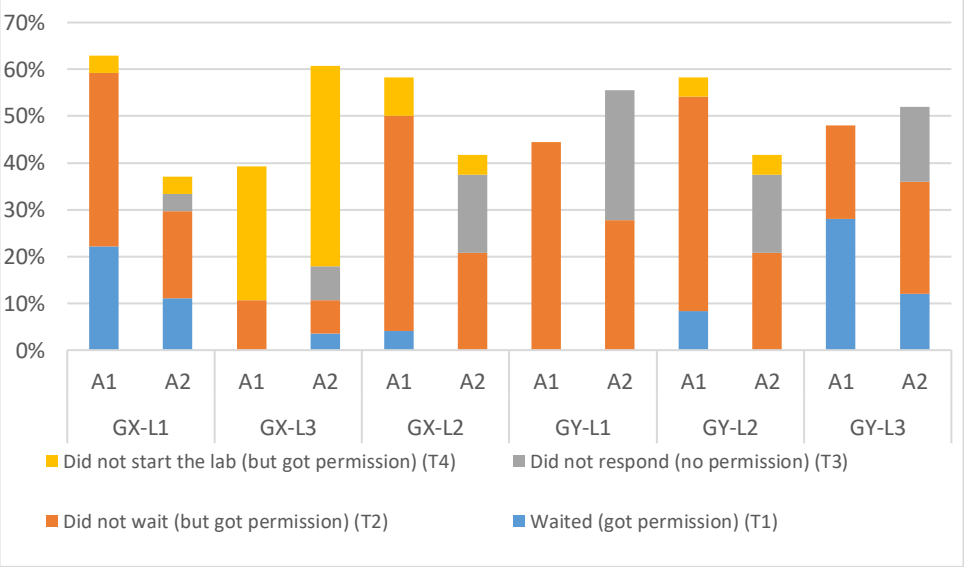

Figure 12. The number of students based on answer type and behavior in the lab in percentage.

The average time waited for permission in each lab was calculated, and also the standard deviation was added. A visible difference was seen in lab GX-L3, where the average time waited was 17 hours and 43 minutes. This relatively big difference was caused by one observation, where student waited for 105 hours and 42 minutes for permission. The long time waited by a student was caused by the student itself, who waited relatively long time before replying to A2 answer. The time waited by a researcher to reply stayed less than 24 hours. The standard deviations reveal that the time waited varied a lot. Figure 13 shows the average time waited in each lab and the standard deviations. On Figure 14 can be seen the average time waited in a lab based on the answer type students received. Standard deviation was also added to the diagram. The average time waited was higher for the students, who received A2 answer in all of the labs. The same reasoning, why the standard deviation was bigger for GX-L3 A2 than for other labs, can be made – a student took a long time to answer. The standard deviations varied throughout the labs.

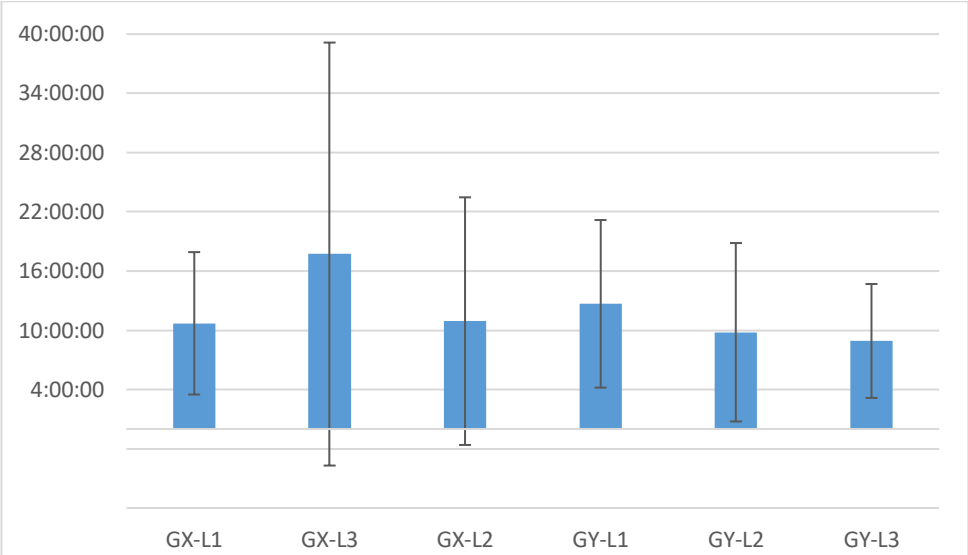

Figure 13. The average waiting time in labs with standard deviation.

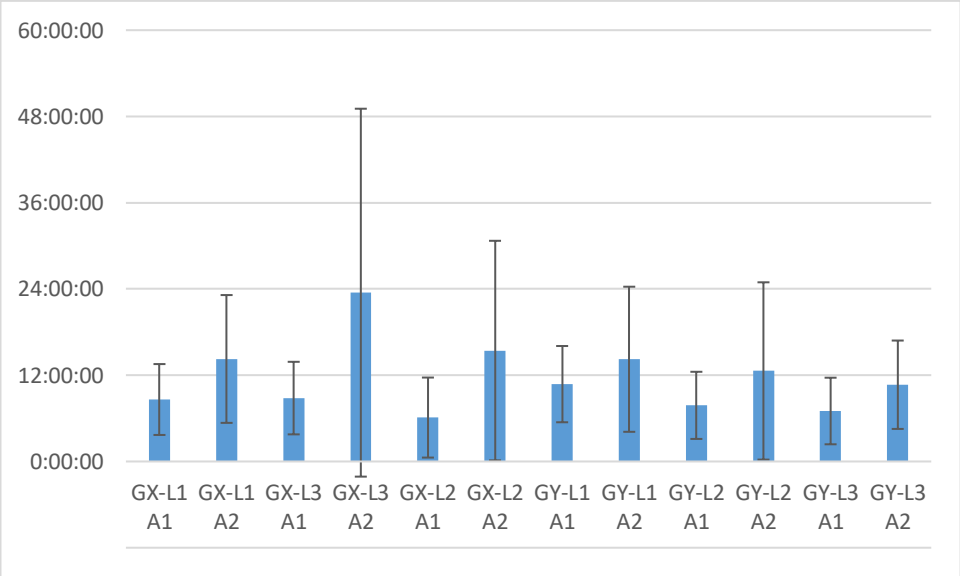

Figure 14. The average waiting time in labs with standard deviation and answer type.

5.4.7 Chi-square Tests on Lab Results

Chi-square (χ^2) test is used for testing a hypothesis using ordinal values [75]. It provides information about the significance of the difference [85]. The expected results in the labs were calculated to perform a Chi-square test.

Hypotheses were set to conduct this test. The first hypothesis was the null hypothesis, which was tried to be rejected. The second hypothesis was the alternative. The hypotheses that were predicted are given in **bold**.

It was assumed that the first lab done by both of the groups but on different weeks has similar results.

$H1_0$: Results of GX-L1 are not related to results of GY-L1.

$H1_1$: Results of GX-L1 are related to results of GY-L1.

As between labs, GX-L1 and GX-L3 have been no intervention; it was hypothesized that the virtual hands-on lab results are independent.

$H2_0$: Results of GX-L1 are not related to results of GX-L3.

$H2_1$: Results of GX-L1 are related to results of GX-L3.

Similarly, as there was no intervention between lab GY-L1 and GY-L2 it was hypothesized that there is no relation between the lab results.

$H3_0$: Results of GY-L1 are not related to results of GY-L2.

$H3_1$: Results of GY-L1 are related to results of GY-L2.

As the experiment holds that between labs GX-L3 and GX-L2 intervention in terms of the lecture are given to students, it was hypothesized that the dependency exists.

$H4_0$: Results of GX-L3 are not related to results of GX-L2.

$H4_1$: Results of GX-L3 are related to results of GX-L2.

Similarly, to group GX group GY has a lecture between the two labs. Hence it was hypothesized that there is a relation between two lab results.

$H5_0$: Results of GY-L2 are not related to results of GY-L3.

$H5_1$: Results of GY-L2 are related to results of GY-L3.

It was also hypothesized, that there should be no relation between labs GX-L3 and GY-L2 as they were hold on the same week, there has been no intervention and the two groups should be equal, because of randomization.

$H6_0$: Results of GX-L3 are not related to results of GY-L2.

$H6_1$: Results of GX-L3 are related to results of GY-L2.

Intervention should have a similar effect on both of the groups, and hence it was hypothesized that there is no relation between GX-L2 and GY-L3.

$H7_0$: Results of GX-L2 are not related to results of GY-L3.

$H7_1$: Results of GX-L2 are related to results of GY-L3.

Chi-square test was conducted on lab results, based on the behavior into what students were classified, and compared with calculated expected results, to find the answers to hypotheses. The results of students, who did not participate in the lecture, were removed from the analysis. Significance level 0.05 was chosen because it is a common way in the research [85]. Chi-squared test results that stayed below the chosen significance level indicate that the lab results are different, as suggested by McHugh [85]. The results reveal that Chi-squared test found a connection between lab GX-L1 and GX-L3 ($p = 0.001$), GX-L1 and GY-L1 ($p = 0.001$), GX-L2 and GX-L3 ($p = 0.001$), GX-L3 and GY-L2 ($p = 0.001$).The results can be seen in Table 5. In grey cells are results, that were not used in the hypotheses.

Table 5. Chi-square test results between lab results.

	GX-L1	**GX-L2**	**GX-L3**	**GY-L1**	**GY-L2**
GX-L1	1				
GX-L2	0.47	1			
GX-L3	0.001	0.001	1		
GY-L1	0.001	0.04	0.001	1	
GY-L2	0.04	0.68	0.001	0.32	1
GY-L3	0.10	0.34	0.001	0.02	0.14

5.4.8 Apriori Algorithm Results

To see the patterns between virtual hands-on lab results and questionnaire questions Apriori algorithm was used. Apriori is used to mine frequent itemsets in a database [86] and finding association rules to discover wisdom [87]. Frequent pattern mining has also been found successful in the educational environment [88]. The parameters measured with Apriori are support, confidence lift and count. Support, confidence, and lift are common and widely used criteria's in association rule mining [89]. Shweta et al. define support for a rule to be "an indication of item how frequently it occurs in database" [90].

Database, in the context of this paper, means the collection of pre- and post-questionnaire and virtual hands-on labs results. Confidence measures the strength of the rule [86]. Lift measures the interestingness of a rule [89]. The count shows how many rows were found with this rule in the dataset.

To use the algorithm students were classified, based on their pre-and post-questionnaire results, accordingly:

1. Deontology – if the sum of the Oxford Utilitarianism Scale (OUS) items was lower than 31.5 (mean from the possible results) or equal. This indicated that the student was more likely with deontology views.
2. Utilitarianism - if the sum of the OUS scale items was greater than 31.5. This indicated that the student was more likely with utilitarianism views.
3. PA-High - if the sum of the policy adherence (PA) scale items was greater than 18.5 (mean from the possible results).
4. PA-Low - if the sum of the PA scale items was lower than 18.5 or equal.
5. PV-High - if the sum of the perceived vulnerability (PV) scale items was greater than 18.5 (mean from the possible results).
6. PV-Low - if the sum of the PV scale items was lower than 18.5 or equal.
7. H-High - if the sum of the HAIS-Q scale items was greater than 24.5 (mean from the possible results).
8. H-Low - if the sum of the HAIS-Q scale items was lower than 24.5 or equal.

Also, the 6-point classification that described students' behavior in the virtual hands-on labs was used, and answer types (A1 and A2) were added to the analysis. Groups GX and GY virtual-hands on lab results were looked together in the analysis, because the group, into what the student belonged to, was not found to form patterns with other criteria. To explain these results better, code names were given. W1 combines in itself GX-L1 and GY-L1 lab results. W2 combines GX-L3 and GY-L2 lab results, and W3 combines GX-L2 and GY-L3 lab results.

Some rules were determined from the results of pre- and post-questionnaire and virtual hands-on labs. Each rule has been given a number so that it would be better to differentiate between them. It can be seen that students, who decided not to ask permission, T5 behavior, in the first lab (W1-T5), decided to do the same in the last lab (W3-T5). The

confidence of this rule (rule nr 8) was 0.58 and support 0.13; this rule encountered 7 times in the dataset. Also, if student acted based on T5 in the first lab (W1-T5) and also in the second lab (W2-T5), a pattern (rule nr 12) was found – these students also behaved the same way in the third lab (W3-T5) (support = 0.09, confidence = 1.00, lift=5.40, count=6). Similarly, a rule between acting according to T2 behavior in the first lab (W1-T2) and the third lab (W3-T2) was found. This rule (rule nr 2) emerged 11 times, support level was 0.20 and confidence 0.65. Rule nr 3 reveals that also students, who behaved according to T2 in the second lab (W2-T2) behaved the same way in the third lab (W3-T2). This pattern was found 11 times in the dataset. Students, who behaved based on type T2 in first (W1-T2) and second (W2-T2) lab tended to behave the same way in the third lab (W3-T2). This patter (rule nr 11) was found 6 times from the dataset.

Apriori revealed a pattern between pre-questionnaire policy adherence items, first lab, and OUS scale. Students, who scored higher on perceived vulnerability subscale (PV-High) in pre-questionnaire and behaved according to type T2 in the first lab, were classified as deontologists in pre-questionnaire (Deontology). Likewise, students, who scored higher on PV (PV-High) and behaved according to type T5 in the first lab (W1-T5) were classified as deontologists in pre-questionnaire OUS subscale (Deontology). These rules (rule nr 4 and 9) were determined 11 and 6 times from the dataset respectively.

Similar results to pre-questionnaire and first lab were also determined from post-questionnaire and third lab - students, who scored higher in post-questionnaire perceived vulnerability scale (POST-PV-High) and behaved according to type T5 in the third lab (W3-T5) were classified as with deontology views in post-questionnaire (POST-Deontology) (rule nr 6, support=0.15, confidence = 0.80, lift = 1.17 and count = 8). Similarly, students, who scored higher on post-questionnaire PV scale (POST-PV-High) and behaved in the third lab according to type T2 (W3-T2), were classified as with deontology views in post-questionnaire (POST-Deontology). This rule (rule nr 1) has support = 0.26, confidence = 0.64, lift = 0.93 and count = 14.

Another pattern was found, students who were classified as with utilitarianism views in pre-questionnaire (Utilitarianism) and post-questionnaire (POST-Utilitarianism) behaved according to type T2 in first (W1-T2, rule nr 5) and last (W3-T1, rule nr 7) lab respectively. Rule 5 emerged 9 times and rule 7 eight times.

A rule was formed from students, who received A2 answer in the first lab (W1-A2) and were classified as with utilitarianism views in pre-questionnaire (Utilitarianism), these students behaved in the second lab according to type T2 behavior (W2-T2). This rule (rule nr 10) was found 6 times in the dataset.

Another interesting trend was visible from experiment results. Students who scored higher on the PV scale in post-questionnaire (POST-PV-High) and behaved ethically (T1) in the third lab (W3-T1) were classified as with utilitarianism views in post questionnaire (POST-Utilitarianism). This rule (rule nr 13) was evident in the dataset 4 times. While it is an interesting trend, it is not strong enough result to make good conclusions out of it.

The results of the Apriori algorithm can be seen in Table 6.

Table 6. Apriori results on pre- and post-questionnaire and labs.

Rule nr.	**Antecedent**	**Consequence**	**Support**	**Confidence**	**Lift**	**Count**
1	POST-PV-High, W3-T2	POST-Deontology	0.26	0.64	0.93	14
2	W1-T2	W3-T2	0.20	0.65	1.45	11
3	W2-T2	W3-T2	0.13	0.52	1.57	11
4	W1-T2, PV-High	Deontology	0.20	0.58	0.89	11
5	Utilitarianism	W1-T2	0.17	0.50	1.29	9
6	POST-PV-High, W3-T5	POST-Deontology	0.15	0.80	1.17	8
7	POST-Utilitarianism	W3-T2	0.15	0.50	1.13	8
8	W1-T5	W3-T5	0.13	0.58	3.15	7
9	W1-T5, PV-High	Deontology	0.11	0.60	0.93	6
10	W1-A2, Utilitarianism	W2-T2	0.11	0.67	2.12	6
11	W1-T2, W2-T2	W3-T2	0.07	0.50	1.50	6
12	W1-T5, W2-T5	W3-T5	0.09	1.00	5.40	5
13	POST-PV-High, W3-T1	POST-Utilitarianism	0.07	0.50	1.53	4

To see, if the time, that students waited for permission, formed any patterns with other characteristics, it was added to the Apriori algorithm. As time differs greatly between students, it was categorized to have clearer results. The comprehensive list of labels are brought out in Appendix 2 – Time Labels for Apriori Algorithm, but example of three first labels are brought out followingly:

- 1t: 3:00:00 – 6:59:59
- 2t: 7:00:00 – 10:59:59
- 3t: 11:00:00 – 14:59:59
- …

Clear pattern was formed - students, who received answer type A1 answer in the labs also waited the least of time to get permission (rules 1, 3 and 4), for example, students who received answer A1 in the third lab (W3-A1) had to wait between 3 to 7 hours (W3-1t) to get permission. Another set of patterns formed (rules 2, 5 and 7), students, who had to wait for the least time (1t) behaved according to type T2 in labs. For example, students who waited between 3 to 7 hours in the third lab (W3-1t) behaved according to type T2 in the same lab (W3-T2). Another trend (rules nr 6 and 8), though not a strong one, was that students, who waited between 7 and 11 hours for reply in labs (W1-2t or W2-2t), also behaved based on type T2 in the same lab (W1-T2 or W2-T2). This rule was found respectively 5 and 4 times in the dataset. The results can be seen in Table 7.

Table 7. Apriori results containing time.

Rule nr.	**Antecedent**	**Consequence**	**Support**	**Confidence**	**Lift**	**Count**
1	W3-A1	W3-1t	0.30	0.53	1.44	16
2	W3-1t	W3-T2	0.24	0.65	1.46	13
3	W2-A1	W2-1t	0.17	0.35	1.34	9
4	W1-A1	W1-1t	0.16	0.33	2.00	9
5	W2-1t	W2-T2	0.13	0.50	1.58	7
6	W1-2t	W1-T2	0.09	0.83	2.14	5
7	W1-1t	W1-T2	0.09	0.56	1.43	5
8	W2-2t	W2-T2	0.07	0.57	1.81	4

6 Discussion

In the previous chapter, the gathered results from the experiment were introduced and analyzed with Cronbach alpha, Spearman's rank-order correlation, Chi-square, Apriori, and the overall percentage of results in the labs. In this chapter, these results will be discussed.

The goal of this research was to develop a method, with what students cyberethical behavior can be measured. As the common way to measure cyberethical behavior is through questionnaires in this research, a different approach was taken. A decision was made to put students into a realistic situation and then measure, how they would behave. The second goal was to see, whether students cyberethical behavior could be influenced by one lecture. To test the method and see the change, experiment was conducted. The experiment consisted of pre-questionnaire, to measure students' attitudes and ethical views, virtual hands-on labs developed in this research to measure cyberethical behavior, the lecture was given to students, to see if students cyberethical behavior can be influenced and post-questionnaire to see the change.

To see the internal validity of the questionnaire Cronbach alphas were calculated on each subscale separately. The results indicate that the questionnaire was a good fit to measure ethical views and cybersecurity attitude. Overall the Cronbach alphas calculated on the pre-questionnaire subscales show improvement in post-questionnaire. When comparing to other subscales the improvement in HAIS-Q items subscale show unexpectedly big change from α = 0.48 in pre-questionnaire to α = 0.75 in the post-questionnaire. This indicates a likely change in the mindset of students. It might be caused by the increase in the understanding of questions or students thinking more carefully, when answering.

Spearman's rank-order correlations were calculated on pre- and post-questionnaire subscale results to see, how each subscale is correlated with each other. Similarly to an article [73], where the OUS scale was developed, no correlation between the OUS subscales (IB and IH) was also found in this research. These two subscales are considered as totally independent factors [73]. The correlation found in the article was $r_s = 0.14$, $p <$

0.01. In this research the correlation in the pre-questionnaire was found to be $r_s = -0.00$ ($p = 0.97$) and in post-questionnaire $r_s = 0.21$ ($p = 0.10$). The increase in the correlation indicates that students' views shifted a bit, but it is still a weak correlation between IH and IB to consider it significant.

Similarly, to OUS no correlation was found between policy adherence (PA) and perceived vulnerability (PV). In pre-questionnaire the correlation found was $r_s = 0.28$ ($p = 0.03$) and in post-questionnaire $r_s = 0.44$ ($p < 0.001$). The correlation found between the two subscales in [59] was $r_s = 0.28$, $p < 0.01$, which is similar to the results found in this research.

Interestingly the correlation between PA subscale and HAIS-Q items ($r_s = 0.41$, $p < 0.001$) was much stronger than between PV and HAIS-Q ($r_s = 0.08$, $p = 0.51$) in the pre-questionnaire. On the other hand, in post-questionnaire, the gap was smaller because the correlation found between HAIS-Q and PA was $r_s = 0.60$ ($p < 0.001$) and between HAIS-Q and PV $r_s = 0.46$ ($p < 0.001$). This indicates that HAIS-Q questions were helpful addition to measure students' attitudes and to understand better, how they think about their own responsibility. The results indicate that a relationship exists between the subscales. Increase in PV and HAIS-Q correlation shows that there was a change in the attitudes of students between the pre- and post-questionnaire. On the other hand, when comparing results in percentage from pre- and post-questionnaire no significant difference was observed.

To see the results from the virtual hands-on lab's students' results were classified into six classes. For group GY it is visible that the results improved with each lab. When in the first lab only 38% of students got permission, then in the final lab, the number had increased to 62%. Also, the number of students, who waited before starting the lab for permission (T1) increased. In the first lab (L1) not a single student waited before receiving permission (T2), in the second lab (L2) 6% waited and in the third lab (L3) after the cyberethics lecture was held, 29% of the students waited before starting the lab. This gives some indication that cyberethics lecture had a positive effect on the cyberethical behavior of students. When in the first lab 53% of students asked permission, then in the second lab this number increased to 71%. This change can be caused by the probability of losing points. When in the first lab it was one from 10000 then in the second the probability of losing points was higher one from 100.

Interestingly the results for group GX were different. The number of students, who got permission, in the first lab (L1) was 67%, in the second lab (L3) this percentage stayed the same and then decreased to 64% in the third lab (L2). The reason for this might be, that in group GX were more students, who already knew at the beginning of the experiment about cyberethics behavior, but this is not very likely, because the difference between first lab results is big, but in pre-questionnaire, the group difference is not so evident. The gap between the groups GX and GY comes clearly out from the results of the first lab. When in group GX 67% of the students got permission in the first lab then in group GY 38% of the students got permission. Another reason for this might be the timing. Group GX did the first lab right after the pre-questionnaire, compared to group GY, who did the first lab a week later, and it might have affected the result of the lab. There was also observed a slight change in the percentage of students who asked permission in the first lab and in the last, but it is not as considerable as in group GY.

The percentage of students in group GX, who got permission in the experiment stayed almost the same. Hence it is concluded, that the lecture did not have an impact on behavior of group GX. However, as it was found to have an impact on behavior of group GY, further research must be conducted to clarify the matter. To see the significance of the difference between lab results Chi-square tests were used to calculate p-values.

Students', who did not participate in the lecture but did the pre- and posttest and the labs, results were analyzed separately. From 13 students, who did not participate in the lecture, 7 were analyzed, forming a small control group. Though there were not enough results to make any strong conclusions out if it, these students continued to behave mainly the same way throughout the experiment - students started the virtual hands-on lab without asking permission (T5). Not a single student asked permission and waited for it (T1). Some of the students, who participated in the lecture, started to behave more ethically after they listened it. Hence, it was presumed, that lecture had impact on the students' cyberethical behavior.

With Chi-square test answers to hypotheses were also found. The $H1_0$ was rejected because a significant difference between GX-L1 and GY-L1 was found ($p < 0.001$). The reason behind it might be the timing of the labs. Group GX received lab L1 right after the pre-questionnaire, hence it is assumed that it had an impact on the lab results. Where on the other hand group GY received lab L1 a week later and the influence of pre-

questionnaire was lessened through that. The same conclusion was reached before when analyzing the performance in the virtual hands-on labs.

Hypothesis $H2_0$ was also rejected because of a significant difference ($p < 0.001$) was found between GX-L1 and GX-L3. However, hypothesis $H3_0$, on the other hand, was confirmed because no difference was found between GY-L1 and GY-L2. The reason behind it might be again the timing. There was a week between labs GX-L1 and GX-L3 but for group GY the second lab came right after the first one. Hence, the influence of the first lab might have lessened on group GX students and cause a change in the results. The same reasoning might be the reason, why $H6_0$ was rejected. GX-L3 and GY-L2 results were found to be significantly different ($p < 0.001$).

The hypothesis $H4_0$ was rejected because a significant difference ($p < 0.001$) was found between GX-L3 and GX-L2. These results indicated that something had changed after the lecture. On the other hand, hypothesis $H5_0$ was supported with a Chi-square test ($p = 0.14$). Though the Chi-square calculated on the GY-L2 and GY-L3 indicate that the change was not significant, the percentage of students, who waited for permission after the lecture, increased considerably in group GY. This allows to assume that the lecture indeed affected the cyberethical behavior of students though not very significantly.

Hypothesis $H7_0$ found support as no significant difference was found between GX-L2 and GY-L3 results. When comparing the results before the lecture, where two groups – GX and GY – results were found to be different, and after the lecture, where they were found to be similar, it was assumed that it was the lecture that affected students cyberethical behavior and not the type of the lab.

The design of the experiment that group GY received proved to work better as the results in the labs improved continuously throughout the experiment compared to group GX, where the results stayed relatively the same. At least one week should be left between the pre-questionnaire and first lab so that the influence of the questionnaire could be lessened. The following labs should be presented right after the end of the previous one so that no gap is left for students to forget.

The type of the answer, A1 or A2, was found to have a small influence on the results. In percentage, there were more students, who received A1 answer and waited for permission (T1) than students, who got A2 answer and waited for permission. For example, in lab

GX-L1 22% of students, who got answer A1 waited (T1), but only 11%, who got answer A2 behaved the same way. Difference can also be seen in lab GY-L3, where 28% of students, who got answer A1, waited for permission, the number for the same behavior for A2 was 12%. The difference comes out almost in all of the labs, except labs GX-L3 and GY-L1. A1 answer was shorter, and permission was given with the first reply, answer A2 on the other hand, persuaded students to put more effort into getting permission and it also took longer time to receive an answer. From this can be concluded that the type of answer has an impact on the behavior. From the analysis of time waited for permission in average, it can be seen that the time waited for A2 is always higher than for A1. That was also logical because for answer A2 student had to reply to a email.

Apriori was used on the virtual hands-on labs and questionnaire results to see if any frequent items emerge from the dataset. To see the patterns, students were classified based on their answers in the questionnaire and behavior in the labs. Some interesting rules were found. First, the patterns found indicate that students, who behaved according to type T2 or T5 in the first labs and on fewer cases also in the second labs were also behaving the same way in the last lab. Confidences for these rules were 0.58 (W1-T5 => W3-T5), 0.65 (W1-T2=>W3-T2), 0.52 (W2-T2 => W3-T2), 1.00 (W1-T5, W2-T5 => W3-T5) and 0.50 (W1-T2, W2-T2 => W3-T2). This indicates that one lecture did not have a significant effect on students' behavior patterns.

The second rule observed, was that when students, who scored high on perceived vulnerability scale, in either post or pre-questionnaire, and behaved either based on type T2 or T5 in the lab, were with deontological views. Rules that support it are: POST-PV-High, W3-T2 => POST-Deontology (confidence = 0.64); POST-PV-High, W3-T5 => POST-Deontology (confidence = 0.80); W1-T2, PV-High => Deontology (confidence = 0.58); W1-T5, PV-High => Deontology (confidence = 0.60). The common nominator for type T2 and T5 behavior is that virtual hands-on lab was started without permission. Deontology holds that it is the actions that matter and following rules are important to them. Hence it is somewhat interesting that students overstepped the company rules, which expected them to ask permission and not start with the lab without it. According to these patterns students also perceived their vulnerability highly. This might indicate that fixing the problem as quickly as possible, even without permission, is the right action for them. Next to rules that imply to deontology, an interesting trend was observed. Namely, students who scored higher on perceived vulnerability scale and behaved according to

type T1 in the lab, were classified as with utilitarianism views in the questionnaire. However, this rule is not strong enough to make any certain conclusions out of it.

Another type of pattern was noticed in the results of Apriori. Students, who got answer type A2 in the first lab and were classified as with utilitarianism views in the pre-questionnaire, behaved according to type T2 in the second lab. The confidence level for this rule was 0.67. According to this pattern, students received A2 answer in the first lab, meaning they had to put more effort into getting the permission and in the second lab decided to start solving the lab before receiving permission because they knew that they would get the permission in the end. To utilitarian's the greater good is important; in the context of this experiment, this might mean, that students started solving the task, without previous permission, to avoid greater problems, that the delay on solving the task may cause, and they knew that the permission would be given, meaning the bad consequences were lessened. Even though utilitarianism was revealed from this pattern it is more likely, that the experience from first lab was what influenced students' behavior in the second lab.

A similar rule was observed between questionnaire and lab behavior. Students, who were classified as with utilitarianism views in the questionnaire behaved according to type T2 in the lab. Two rules like this were found: Utilitarianism => W1-T2 (confidence = 0.50) and POST-Utilitarianism => W3-T2 (confidence 0.50). The reason behind this might be the same as discussed above – to serve the greater good might mean in the context of this experiment, the greater good for a student is to get the task done as fast as possible and waiting for permission does not serve this purpose.

One type of pattern that formed with time was that students, who received A1 answer waited the least time for the permission. Though the confidence for these rules is low (<0.50) it is still logical because A1 answer did not expect students to write a second letter, saving like this time. The rules observed: W3-A1 => W3-1t (confidence = 0.30), W2-A1 => W2-1t (confidence = 0.35), W1-A1 => W1-1t (confidence = 0.33). Another interesting pattern formed. Students, who waited 3 to 11 hours asked permission but did not wait for permission, before starting the lab. This was somewhat unexpected because these students had to wait the least of the time to receive an answer. This might be caused by small sample size and should be investigated more thoroughly.

6.1 Limitations of the Experiment

In this chapter, the limitations of the experiment are brought out.

One of the limitations of this experiment to validity is the number of students, who participated in the experiment. There were 86 students, who gave permission, that their data can be used in the experiment from whom 73 participated in the lecture. Also, all the students were studying in TalTech. This did not give a wide overview of the entire population and lessened the chance to generalize the results.

Another limitation to the validity of the experiment was the loss of some participants during the experiment. Even though different methods were taken into use to motivate students to participate in the experiment, some students, who filled the pre-questionnaire did not fill-in the post-questionnaire.

Based on the course where the experiment was conducted, students had a lecture and no exercise classes. This meant that the labs and questionnaires were done as homework, leaving the possibility for contamination of results. To reduce the likelihood randomization was used and a time limit was set for solving the labs and questionnaires. Contamination of the results may have also been caused by the concurrent event, and the change in results can be "mistakenly attributed to the intervention" [91]. Meaning, the other knowledge students gathered during the time of the experiment, was not under the control of the researcher and the effect of them cannot be measured.

Some of the students intentionally did not answer the questions truthfully. These results were removed from the analysis. To reduce the likelihood of it happening students did not receive points based on their answers, because there were no correct or wrong answers, and they were emphasized to answer like they really think. Also, as students knew, that they were part of a research experiment, they might not have behaved the way they would in real life.

One of the limitations of the virtual hands-on lab was that it was time-consuming to keep an eye on the emails, mark the data down and respond. To reduce the time spent by the researcher auto-replies could be used in future work.

The experiment had a gap; no control group was used to see if it was the lecture that caused the change. This was because of the constraints of the course, where the

experiment was conducted. All of the students were expected to receive a lecture. Still, the experiment was constructed so that between the first two labs no intervention was given to students and between second and third lab lecture was hold. This allows to assume whether it is the lecture that influences the results or not. Also, an automatic control group formed from students, who did not participate in the lecture but did the labs and pre- and posttest. Though, the number of these students was not high it gave some indication of the influence of the lecture.

In article ”Pretest-posttest designs and measurement of change” notes that the pretest might have an influence on the results - students might have behaved differently if they would not had a pretest [92]. To see, whether it was the pre-questionnaire that influenced the lab results, the experiment was constructed so, that for group GX first lab followed right after the pre-questionnaire and for group GY the first lab was given a week later.

Another limitation was that only the cyberethical side was looked in the experiment, other factors like educational and gamification theories were left unnoticed. These were also not in the scope of this paper. With this thesis a starting point was given from what future work can be conducted.

6.2 Future Work

In this experiment 86 students mostly from TalTech participated. From 86 students 73 participated in the lecture. In the analysis, these students’ results were removed, who did not attend the lecture. It is a relatively small sample size and lacks the possibility for generalization. Also, the majority of the students participating were men. Further research should be conducted with bigger sample size and more women to get more accurate results and improve the method. Having an equal amount of men and women in the sample allows to compare the results between them and see if women behave differently in a similar situation.

In this experiment, the scope of the sample was limited to mostly IT first-year bachelor students. It would be interesting to see, how the results differ for other major and older students.

With this research long-term influences of the lecture cannot be seen. To see, whether there was a persistent change in students' behaviors and attitudes long term study should be conducted.

The field of research, discussed in current research, is interdisciplinary. This thesis concentrated on the cyberethical part and other influencing factors, like the gamification and educational theories were not covered in detail. Future work should be done to get a better understanding of these factors.

The validity of the experiment in this research was supported with the expert interview. To improve the validity, even more further validation should be done. For example, additional interviews with experts in the field could be conducted. Also, interviews with students to get a better understanding of students' attitudes and behavior. The appropriateness and validity of the lecture could also be further improved with expert interviews.

In order to improve the validity and avoid contamination of the results, the experiment should be conducted again in a controlled environment. Control group should be used to get a better understanding, how much intervention changed the results. Additionally, different interventions could be tested to see, what is the best way to teach cyberethics to students and what method has the greatest impact.

The limitation of this experiment was that answering to all of the students is time-consuming and mistakes can be easily made. To improve the method presented in this research automated answers could be designed to reply to students' emails.

Even though students were tried to put into as realistic situation as possible, the problem still stays that students know that they are part of an experiment and might behave in a way that they think is expected from them or not take the storyline of the experiment as seriously as they would in real life. To address this issue, the experiment should be conducted in a real word environment without previous notification of students. On the other hand, this raises a lot of privacy and law questions that should be dealt with.

To analyze the results of the experiment classification of the data was used. This was done because nominal and ordinal data were collected during the questionnaires and labs. In this experiment labels introduced in chapters 5.4.3 and 5.4.8 were used. The analysis

of the results could also be done with different classification. Because of the small sample size, the scores on questionnaire subscales were divided into two. For example, policy adherence low and policy adherence high. With a bigger sample size, more classes could be used to label questionnaire results. This way more accurate results could be determined.

7 Summary

Cyberethics is an important topic that should be taught to our current IT students. With this work, background on cyberethics was given based on the academic literature. These basic ideas of cyberethics were also introduced to students as part of the lecture. Feedback from the students after the lecture was positive. To measure impact of the lecture, a method was created. With this method students' cyberethical behavior was measured. Before starting with the virtual hands-on lab, students were given a scenario. As part of that scenario, students were expected to ask permission before starting with the lab. Currently, the majority of the researches have used questionnaires to assess students' cybersecurity behavior. Ethical aspects of the measured behavior are often left unnoticed. Also using only questionnaires does not give a full picture of student's behavior. This research was trying to address this gap. The experiment was created to see if the student's cyberethical behavior, attitude and ethical views can be measured and also influenced with one lecture. The experiment consisted of attitude and ethical views questionnaire, that was given to students in the beginning and end of the experiment and three virtual hands-on labs, that expected the student to ask permission before starting with the task. Lecture about cyberethics was given between the second and the third lab.

The results indicate that cybersecurity attitude questionnaire is not necessarily a good predictor for cyberethical behavior. Still, students, who scored higher in perceived vulnerability scale and were classified as deontologists on Oxford Utilitarianism Scale (OUS) tended to behave in two following ways. One group of students, who asked permission, but did not wait for the reply letter with permission and started the virtual hands-on lab without it (T2). The second group of students, who did not ask for permission at all and started the lab without it (T5). This rule had a weakness - some patterns were also found between utilitarianism and T2 behavior. Hence, whether a student is with deontological or utilitarianism views is not a strong indicator of behavior.

Results from the Spearman's rank-order correlation conducted on pre- and post-questionnaire that there was a change in students cybersecurity attitudes after the lecture was held. The correlation coefficients got stronger in the post-questionnaire. Students'

cyberethical behavior was also compared before and after the lecture was given. The analysis revealed that the number of students, who waited for permission after the lecture increased. These results indicate that the lecture had some positive effect on students cyberethical behavior.

The proposed method for measuring students cyberethical behavior could be a valuable resource for educators, who want to teach cyberethics or conduct further research.

References

[1] G. Mori and J. Malik, “Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA,” in *2003 IEEE Computer Society Conference on Computer and Pattern Recognition (CVPR’03)*, 2003, pp. 1–8.

[2] T. W. Bynum, “The Foundation of Computer Ethics,” *SIGCAS Comput. Soc.*, vol. 30, no. 2, pp. 6–13, 2000.

[3] C. Cimpanu, “Security Researcher and Alleged Spam Operator to Square Off in Court in Ugly Lawsuit,” *BleepingComputer*. May-2017.

[4] S. M. Furnell, “The Problem of Categorising Cybercrime and Cybercriminals,” in *Survival in the e-conomy: 2nd Australian information warfare & security conference 2001*, 2001, pp. 29–36.

[5] S. Tulasi Prasad, “Ethical Hacking and Types of Hackers,” *Int. J. Emerg. Technol. Comput. Sci. Electron.*, vol. 11, no. 2, pp. 24–27, 2014.

[6] C. Falk, “CERIAS Tech Report 2004-20. Gray Hat Hacking: Morally Black and White,” 2004.

[7] J. A. Amorim, M. Hendrix, S. F. Andler, and P. M. Gustavsson, “Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment,” in *NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111), 2013*, 2013, pp. 1–12.

[8] IEEE, “About - IEEE TechEthics™,” *IEEE TechEthics*, 2019. [Online]. Available: https://techethics.ieee.org/about. [Accessed: 12-Mar-2019].

[9] L. N. K. Leonard and T. P. Cronan, “Attitude toward ethical behavior in computer use: a shifting model,” *Ind. Manag. Data Syst.*, vol. 105, no. 9, pp. 1150–1171, 2005.

[10] L. P. Pojman and J. Fieser, *Discovering Right and Wrong*, 7th ed. Boston, MA, USA: Wadsworth, Cengage Learning, 2011.

[11] S. Vallor, J. William, and S. J. Rewak, “An Introduction to Cybersecurity Ethics,” Santa Clara, 2018.

[12] K. L. Rich, “Introduction to Ethics,” in *Nursing ethics: Across the curriculum and into practice*, Jones & Bartlett Learning Burlington, MA, 2016, pp. 3–30.

[13] J. Fieser, “Ethics,” *Internet Encyclopedia of Philosophy: A Peer-Reviewed Academic Resource*, 2019. [Online]. Available: https://www.iep.utm.edu/ethics/#H1. [Accessed: 04-Mar-2019].

[14] B. C. Stahl, J. Timmermans, and B. D. Mittelstadt, “The Ethics of Computing: A Survey of the Computing-Oriented Literature,” *ACM Comput. Surv.*, vol. 48, no. 4, p. 55:1--55:38, 2016.

[15] P. Singer, *Applied ethics - (Oxford readings in philosophy)*. New York, USA: Oxford University Press, 1986.

[16] H. T. Tavani, *Ethics & Technology: Controversies, Questions, and Strategies for Ethical Computing*, 4th ed. Wiley, 2013.

[17] H. T. Tavani, *Ethics & Technology: Ethical Issues in an Age of Information and Communication Technology*, 1st ed. Hoboken: John Wiley & Sons, 2004.

[18] “Eetika ja moraal,” *Eetikaveeb*, 2019. [Online]. Available: https://www.eetika.ee/et/eetika/eetika-moraal. [Accessed: 04-Mar-2019].

[19] A. Wilk, “Cyber Security Education and Law,” in *2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE)*, 2016, pp. 94–103.
[20] R. A. Spinello and H. T. Tavani, “The Internet, Ethical Values, and Conceptual Frameworks: An Introduction to CyberEthics,” *ACM SIGCAS Comput. Soc.*, vol. 31, no. 2, pp. 5–7, 2001.
[21] B. R. Schlenkerand, D. R. Forsyth, N. H. Mcginnis, H. Goldman, and R. Schlenker, “On the Ethics of Psychological Research,” *J. Exp. Soc. Psychol.*, vol. 13, pp. 369–372, 1977.
[22] J. Fraedrich and O. C. Ferrell, “Cognitive Consistency of Marketing Managers in Ethical Situations,” *J. Acad. Mark. Sci.*, vol. 20, no. 3, pp. 245–252, 1992.
[23] R. S. Upchurch and S. K. Ruhland, “The Organizational Bases of Ethical Work Climates in Lodging Operations as Perceived by General Managers.,” *J. Bus. Ethics*, vol. 15, no. 10, pp. 1083–1093, 1996.
[24] J. P. Fraedrich, “The Ethical Behavior of Retail Managers.,” *J. Bus. Ethics*, vol. 12, no. 3, pp. 207–218, 1993.
[25] E. Aronson, “Integrating Leadership Styles and Ethical Perspectives,” *Can. J. Adm. Sci.*, vol. 18, no. 4, pp. 244–256, 2001.
[26] W. . Ross, *THE RIGHT AND THE GOOD*. New York, United States: Oxford University Press, 1930.
[27] B. L. Adams, F. L. Malone, and W. James, “Confidentiality Decisions: The Reasoning Process of CPAS in Resolving Ethical Dilemmas.,” *J. Bus. Ethics*, vol. 14, no. 12, pp. 1015–1020, 1995.
[28] R. A. Spinello and H. T. Tavani, *Readings in cyberethics*, 2nd ed. Sudbury, Massachusetts: Jones & Bartlett Learning, 2004.
[29] J. Iqbal and M. B. Bilal, “Computer Ethics from Obscure to Ubiquitous,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, pp. 982–990, 2017.
[30] W. Maner, “Unique ethical problems in information technology,” *Sci. Eng. Ethics*, vol. 2, no. 2, pp. 137–154, 1996.
[31] J. H. Moor, “WHAT IS COMPUTER ETHICS?,” *METAPHILOSOPHY*, vol. 16, no. 4, pp. 266–275, 1985.
[32] D. Pruitt-Mentle, “C3 Framework Cyberethics, Cybersafety and Cybersecurity Promoting Responsible Use,” *Educ. Technol. Policy, Res. Outreach*, vol. 13, pp. 1–6, 2000.
[33] O. B. Onyancha, “An informetrics view of the relationship between internet ethics, computer ethics and cyberethics,” *Libr. Hi Tech*, vol. 33, no. 3, pp. 387–408, 2015.
[34] A. Ramadhan, D. I. Sensuse, and A. M. Arymurthy, “e-Government Ethics : a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 8, pp. 82–86, 2011.
[35] A. Jamal, A. Ferdoos, M. Zaman, and M. Hussain, “Cyber-Ethics and the Perceptions of Internet Users: A Case Study of University Students of Islamabad,” *PAKISTAN J. Inf. Manag. Libr.*, vol. 16, pp. 8–20, 2015.
[36] D. G. Johnson, “Computer ethics,” in *The Blackwell Guide to the Philosophy of Computing and Information*, Luciano Floridi, Ed. Blackwell Publishing, 2004, pp. 65–75.
[37] E. Y. W. Wong, “How should we teach computer ethics? A short study done in Hong Kong,” *Comput. Educ.*, vol. 25, no. 4, pp. 179–191, Dec. 1995.
[38] J. H. Moor, “The future of computer ethics: You ain’t seen nothin’ yet!,” *Ethics Inf. Technol.*, vol. 3, pp. 89–91, 2001.

[39] J. H. Moor, “Reason, relativity, and responsibility in computer ethics,” *ACM SIGCAS Comput. Soc.*, vol. 28, no. 1, pp. 14–21, 1998.
[40] I. Hamburg and K. R. Grosch, “Ethical Aspects in Cyber Security,” *Arch. Bus. Res.*, vol. 5, no. 10, pp. 199–206, 2018.
[41] T. Aavik *et al.*, *Eetikakoodeksite käsiraamat*. Eesti Keele Sihtasutus, 2007.
[42] B. Berenbach and M. Broy, “Professional and ethical dilemmas in software engineering,” *Computer (Long. Beach. Calif).*, vol. 42, no. 1, pp. 74–80, 2009.
[43] J. M. Kizza, *Texts in Computer Science: Ethical and Social Issues in the Information Age*, 5th ed. London: Springer, 2013.
[44] R. Epstein, “The Impact of Computer Security Concerns on Software Development,” in *Internet Security: Hacking, Counterhacking, and Society*, London: Jones & Barlett Publishers, Inc., 2007, pp. 171–202.
[45] N. Radziwill, J. Romano, D. Shorter, and M. C. Benton, “The Ethics of Hacking: Should It Be Taught?,” *Softw. Qual. Prof.*, vol. 18, no. 1, pp. 11–15, 2015.
[46] B. Bashir and A. Khalique, “A Review on Security versus Ethics,” *Int. J. Comput. Appl.*, vol. 151, no. 11, pp. 13–17, 2016.
[47] H. Nissenbaum, “Privacy as Contextual Integrity,” *Washingt. Law Rev.*, vol. 79, no. 119, pp. 119–158, 2004.
[48] E. Towell, “Teaching ethics in the software engineering curriculum,” *Softw. Eng. Educ. Conf. Proc.*, vol. 2003–Janua, pp. 150–157, 2003.
[49] “e-Government Ethics : a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics,” *Int. J. Adv. Comput. Sci. Appl.*
[50] L.-J. Lester and Y. Dallat-Ward, “Teaching Professionalism and Ethics in IT by Deliberative Dialogue,” in *2018 Proceedings of the EDSIG Conference*, 2018, pp. 1–14.
[51] S. Hirabayashi and T. Matsuda, “Constructing Design Principles for Developing Gaming Instructional Materials for Making Cyber Ethics Education Authentic,” in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2011*, 2007, pp. 1280–1288.
[52] R. S. Bell, E. Y. Vasserman, and E. C. Sayre, “A Longitudinal Study of Students in an Introductory Cybersecurity Course.,” *Proc. ASEE Annu. Conf. Expo.*, vol. 24, no. 61, pp. 1–11, 2014.
[53] D. Leutner and J. L. Plass, “Measuring Learning Styles with Questionnaires Versus Direct Observation of Preferential Choice Behavior in Authentic Learning Situations: The Visualizer/Verbalizer Behavior Observation Scale (VV-BOS),” 1998.
[54] L. Chiang and B. Lee, “Ethical Attitude and Behaviors Regarding Computer Use,” *Ethics Behav.*, vol. 21, no. 6, pp. 481–497, 2011.
[55] L. N. K. Leonard and T. P. Cronan, “Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences,” *J. Assoc. Inf. Syst.*, vol. 1, no. 12, pp. 1–31, 2001.
[56] N. Mohamed, S. A. Karim, and R. Hussein, “Computer use ethics among university students and staffs: The influence of gender, religious work value and organizational level,” *Campus-Wide Inf. Syst.*, vol. 29, no. 5, pp. 328–343, 2012.
[57] U. E. Gattiker and H. Kelley, “Morality and Computers: Attitudes and Differences in Moral Judgments,” *Information systems research*, vol. 10, no. 3. INFORMS, pp. 233–254, 1999.
[58] S. Athey, “A comparison of experts’ and high tech students’ ethical beliefs in computer-related situations,” *J. Bus. Ethics*, vol. 12, no. 5, pp. 359–370, 1993.
[59] D. J. Howard, “Development of the Cybersecurity Attitudes Scale and Modeling

Cybersecurity Behavior and its Antecedents," University of South Florida, 2018.
[60] N. Schwarz, "Self-Reports: How the Questions Shape the Answers," *Am. Psychol.*, vol. 54, no. 2, pp. 93–105, 1999.
[61] J. Hainmueller, D. Hangartner, and T. Yamamoto, "Validating vignette and conjoint survey experiments against real-world behavior.," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 112, no. 8, pp. 2395–2400, Feb. 2015.
[62] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.
[63] L. N. K. Leonard, T. P. Cronan, and J. Kreie, "What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?," *Inf. Manag.*, vol. 42, no. 1, pp. 143–158, Dec. 2004.
[64] I. Ajzen, "Attitude Theory and the Attitude-Behaviour Relation," *New Dir. attitude Meas.*, no. January 1993, pp. 41–57, 1993.
[65] J. R. Fraenkel, N. E. Wallen, and H. Hyun, *How to Design and Evaluate Research in Education*, 8th ed., vol. 60. New York, USA: McGraw-Hill Higher Education, 2011.
[66] L. Cohen, K. Morrison, and L. Manion, *Research Methods in Education*, 7th ed. London: Routledge, 2011.
[67] B. B. Frey, *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. 2455 Teller Road, Thousand Oaks, California 91320: SAGE Publications, Inc., 2018.
[68] M. Ernits, J. Tammekänd, and O. Maennel, "i-tee: A fully automated Cyber Defense Competition for Students," in *ACM SIGCOMM Computer Communication Review*, 2015, vol. 45, no. 4, pp. 113–114.
[69] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39.
[70] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, May 2012.
[71] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, Jun. 2006.
[72] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014.
[73] G. Kahane *et al.*, "Beyond sacrificial harm: {A} two-dimensional model of utilitarian psychology," *Psychol. Rev.*, vol. 125, no. 2, pp. 131–164, 2018.
[74] Abdul, "Quality of Psychology Test Between Likert Scale 5 and 6 Points," *J. Soc. Sci.*, vol. 6, no. 3, pp. 399–403, 2010.
[75] S. Jamieson, "Likert scales: how to (ab)use them," *Med. Educ.*, vol. 38, no. 12, pp. 1217–1218, 2004.
[76] L. Hadlington, "Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 269–281, 2018.
[77] C. M. Plump and J. LaRosa, "Using Kahoot! in the Classroom to Create Engagement and Active Learning: A Game-Based Technology Solution for eLearning Novices," *Manag. Teach. Rev.*, vol. 2, no. 2, pp. 151–158, Jun. 2017.
[78] R. Dellos, "Kahoot! A digital game resource for learning," *Int. J. Instr. Technol.*

Distance Learn., vol. 12, no. 4, pp. 49–52, 2015.
[79] S. Khandelwal, "A Twitter Bug Left Android Users' Private Tweets Exposed For 4 Years," *The Hacker News*, 2019. [Online]. Available: https://thehackernews.com/2019/01/twitter-privacy-settings.html. [Accessed: 22-Jan-2019].
[80] J. W. Creswell, *Educational Research: Planning, conducting and evaluating quantitative and qualitative research*, 4th ed. Boston: Pearson Education Inc., 2012.
[81] A. Bogner, B. Littig, and W. Menz, "Introductiom: Expert Interviews - An Introduction to a New Methodological Debate," in *Interviewing Experts: Research Methods Series*, A. Bogner, B. Littig, and W. Menz, Eds. Palgrave Macmillan, 2016, pp. 1–16.
[82] S. Harvey-Jordan and S. Long, "The process and the pitfalls of semi-structured interviews," *Community Pract.*, vol. 74, no. 6, p. 219, 2001.
[83] D. Cotton and K. Gresty, "Reflecting on the think-aloud method for evaluating e-learning," *Br. J. Educ. Technol.*, vol. 37, no. 1, pp. 45–54, Jan. 2006.
[84] L. Cohen, L. Manion, and K. Morrison, *Research Methods in Education*, 6th ed. New York, NY: Routledge, 2007.
[85] M. L. Mchugh, "The Chi-square test of independence Lessons in biostatistics," *Biochem. Medica*, vol. 23, no. 2, pp. 143–9, 2013.
[86] R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," *ACM Sigmod Rec.*, vol. 22, no. 2, pp. 207–216, 1993.
[87] M. Al-Maolegi and B. Arkok, "AN IMPROVED APRIORI ALGORITHM FOR ASSOCIATION RULES," *Int. J. Nat. Lang. Comput.*, vol. 3, no. 1, pp. 21–29, 2014.
[88] E. Chandra and K. Nandhini, "Knowledge Mining from Student Data," *Eur. J. Sci. Res.*, vol. 47, no. 1, pp. 156–163, 2010.
[89] P. D. McNicholas, T. B. Murphy, and M. O'Regan, "Standardising the lift of an association rule," *Comput. Stat. Data Anal.*, vol. 52, no. 10, pp. 4712–4721, Jun. 2008.
[90] M. Shweta and K. Garg, "Mining Efficient Association Rules Through Apriori Algorithm Using Attributes and Comparative Analysis of Various Association Rule Algorithms," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 6, pp. 306–312, 2013.
[91] J. H. Price Editor and J. M. Assistant, "Limitations and the Necessity of Reporting Them," *Am. J. Heal. Educ.*, vol. 35, no. 2, pp. 66–67, 2013.
[92] D. M. Dimitrov and P. D. Rumrill, "Pretest-posttest designs and measurement of change," *Work*, vol. 20, no. 2, pp. 159–165, 2003.

Appendix 1 – Questionnaire

Following text describes the questionnaire items given to students. Headings, like “The Oxford Utilitarianism Scale”, or “Impartial Beneficence” were not given to the students with the questionnaire. They were added here to increase the understandability. The sources used to create this questionnaire were: The Oxford Utilitarianism Scale, Cybersecurity Attitude Scale, and HAIS-Q.

Followingly you will be given a list of statements in English. Please select, how much you agree with each of them. You will receive an extra point for filling this questionnaire. There are no wrong or right answers. Nonetheless, please answer truthfully – then we get an idea, what are students, who study in this course, general views. (Introduction originally in Estonian)

All the answers are using this scale:

1. Strongly Disagree
2. Disagree
3. Somewhat Disagree
4. Somewhat Agree
5. Agree
6. Strongly Agree

The Oxford Utilitarianism Scale

Impartial Beneficence

1. If the only way to save another person’s life during an emergency is to sacrifice one’s own leg, then one is morally required to make this sacrifice.
2. From a moral point of view, we should feel obliged to give one of our kidneys to a person with kidney failure since we do not need two kidneys to survive, but really only one to be healthy.

3. From a moral perspective, people should care about the well-being of all human beings on the planet equally; they should not favor the well-being of people who are especially close to them either physically or emotionally.
4. It is just as wrong to fail to help someone as it is to actively harm them yourself.
5. It is morally wrong to keep money that one doesn't really need if one can donate it to causes that provide effective help to those who will benefit a great deal.

Instrumental harm

6. It is morally right to harm an innocent person if harming them is a necessary means to helping several other innocent people.
7. If the only way to ensure the overall well-being and happiness of the people is through the use of political oppression for a short, limited period, then political oppression should be used.
8. It is permissible to torture an innocent person if this would be necessary to provide information to prevent a bomb going off that would kill hundreds of people.
9. Sometimes it is morally necessary for innocent people to die as collateral damage—if more people are saved overall.

Introduction to Attitude questions

Imagine being an IT consultant in a small start-up (BestCostConsult) that focuses on offering various IT consultation services to other companies. In addition to you, the company has 15 workers. All of the workers' pictures with contact info, including email address, are added to the company's web page.

1. How many people are working in this imaginary company (BestCostConsult)?

The Cybersecurity Attitude Scale

Policy adherence

1. I feel it is necessary to use strong passwords for my applications at work.
2. I feel it is important to follow organizational cybersecurity policies.
3. I feel it is important to never intentionally violate my organization's cybersecurity policies.

4. I feel it is in my best personal interest to follow my organization's cybersecurity policies.
5. I feel it is in my employer's best interest to hire individuals who follow the organization's cybersecurity policies.

Perceived vulnerability

6. I feel it is possible I could receive a harmful email attachment at my work email address.
7. I feel it is possible that my organization could be the victim of a cyberattack.
8. I feel it is possible that I could be a victim of a cyberattack at work.
9. I feel it is possible that an employee browsing the internet could lead to a cyberattack at my organization.
10. I feel I am vulnerable to my personal information being stolen from my organization in a cyberattack.

HAIS-Q 7 Questions

Own responsibility

1. I use a different password for my social media and work account.
2. I don't open email attachments if the sender is unknown to me.
3. When accessing the Internet at work, I visit any website that I want to.*
4. I post whatever I want to about my work on social media.*
5. I check that strangers can't see my laptop screen if I'm working on a sensitive document.
6. I wouldn't plug a USB stick found in a public place into my work computer.
7. If I saw someone acting suspiciously in my workplace, I would do something about it.

* - Question results marked with this sign (*) were inverted when analyzing, because these statements about behavior, were the opposite to behaviors in other questions. The changes were: 1⇔6; 2⇔5;3⇔4. For example, if students answered 2 then the result was calculated to 5 when analyzing.

Appendix 2 – Time Labels for Apriori Algorithm

Time	Label
3:00:00 - 6:59:59	1t
7:00:00 - 10:59:59	2t
11:00:00 - 14:59:59	3t
15:00:00 - 18:59:59	4t
19:00:00 - 22:59:59	5t
23:00:00 - 26:59:59	6t
27:00:00 - 30:59:59	7t
31:00:00 - 34:59:59	8t
35:00:00 - 38:59:59	9t
39:00:00 - 42:59:59	10t
43:00:00 - 46:59:59	11t
47:00:00 - 50:59:59	12t
51:00:00 - 54:59:59	13t
55:00:00 - 58:59:59	14t
59:00:00 - 62:59:59	15t
63:00:00 - 66:59:59	16t
67:00:00 - 70:59:59	17t
71:00:00 - 74:59:59	18t
75:00:00 >	19t