Measuring the Effectiveness of Information Security Awareness Program

Ilirjana Veseli

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2011

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Acknowledgment

I would like to thank everyone who helped me with ideas, research and exploration. I also, want to thank those who provided an inspiring and supportive environment during this project.

To begin, I thank Tone Hoddø Bakås. She encouraged me to think big and act small: an attractive attitude since it not only inspired me to read and to explore the fundamentals of information security awareness theories, but it also kept me active and optimistic during the whole project. This line of thoughts made me realize how things work in practice. Therefore, I thank her for supervising this research and for her advices throughout this project.

To continue, there are some students who need strict guidance from their advisors (micromanagement), while others are creative and don't require being micromanaged. I think that I belong to the second group.

Moreover, I am very grateful to work with Nils Kalstad Svendsen, and I thank him for reviewing the various drafts of the thesis.

I also profited from discussions with Frode Volden regarding the statistical analysis of the data, and with Nils Rui regarding the survey launch. Thus, I truly thank them.

I would like to thank my future husband Dr. Doni, PharmD for his full support, encouragement, and motivation, during two years of my master studies. Finally, I thank my wonderful mother, and three brothers for all their support and enthusiasm. This Work I dedicate to my parents.

Abstract

Many researchers and experts in the information security field stress that the user is the weakest link in the chain when it comes to information security and security assets of an organization. The human error is still the key concept that might threaten and seriously damage assets of the organization. Consequently, the challenge for many (if not most) institutions and organizations today, is to improve the information security awareness of the end user. Identifying the program that best influences and improves the user's knowledge, attitude, and behavior towards information security, is yet highly important. In order to identify this program, a method for assessing and measuring the effectiveness of information security awareness program is applied in this study. In the previous literature many methods for assessing and measuring the information security awareness are found,but there is not even one research found that shows effectiveness of the awareness program. Therefore, in this thesis a case study, and an experiment is realized in practice to examine, and represent the effectiveness of the information security awareness program.

In this study information security awareness training is realized. The level of awareness among the participants in regard to information security is assessed and measured **before** and **after** the awareness training. The purpose of this is to let the effectiveness of the awareness training be highlighted, shown, and to find out to what extended it is effective. The methodology used to accomplish this task is: the online surveys and the interviews.

The results from the statistical analysis of the data form the surveys have shown that the awareness training programs used in this case are effective. The topics discussed in the training, are: (1) Password protection and management, (2) Sensitive information handling, (3) Social engineering, (4) Physical/Office protection, (5) Incident response - whom to contact, where all of them scored higher from the group of participants that attended the training, than the group of participants that NOT attended the training. The information security awareness on *"all topics together"* (*"all topics together"* includes all from the above mentioned topics, and represent the awareness in general) is scored significantly higher from the participants that attended the training, with value of $p = 0.009$ (If $p \leq 0.01$ the observed value is "highly significant"). Regardless of these statistical facts, the interviews with IT personnel confirmed that the number of employees asking about suspicious e-mails has been increased, after the training has been realized.

The training is realized into different training styles, such as: (a) Classroom, (b) Discussion-based, and (c) Web-based training style. These training types are compared with each other, to identify their effectiveness. It resulted that the (a) Classroom training style is more effective on improving the knowledge, attitude, and behavior, among the participants in the majority of the topics. However, the (c) Web-based training style resulted to be better in the (3) Social engin-

eering topic, while the the (b) Discussion-based training resulted to be better in the topic (5) Incident Response - Whom to Contact. Additionally, some recommendations are given which helps on choosing the training style, that is best fitted to your needs.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic Covered

Chris Potter (a partner with PriceWaterhouseCoopers, and leading author of the Information Security Breaches Survey) stated:

"*It's fairly clear that people are a fundamental element of security.*"

In the technical report *"Information Security Breaches Survey"* conducted in United Kingdom from PriceWaterhouseCoopers [5] it was stated:
"*Human error rather than flawed technology is the root cause of most security Breaches*".

Experts, such as: Shaw *et. al.*,Lance Spitzner, and Michael Callahan [6, 7, 8], agree that the weakest link in the chain when it comes to information security and security systems of the organization is an insider or a user. One of the main characteristics is that the user is deeply involved in daily operations. Human's wrong behavior contributing to information security breaches is considered to be a serious problem. Even today in IT security world human error still continues to be the greatest root cause of the data breaches [5]. Users intentionally or unintentionally are given the option to bypass the security processes, and that's the reason why these processes fail. Wilson and Hash from National Institute of Standards and Technology [9] gave their opinion, about how this problem might be overcome. They said:

"*If people are the key, but are also a weak link, more and better attention must be paid to this 'asset' ".*

1.2 Problem Description

IT personnel alone might not be effective enough in stopping security breaches from happening. For that reason, the security awareness of the end users must be improved [6]. Technical controls for information security systems have been developed considerably over these latest years. Today, there is an astonishing variety of security technical controls:

- Firewalls running on PCs,
- Real time antivirus scanning on networks and computing devices,
- Sophisticated techniques to inspect and control internet traffic,
- Local disk encryption, etc.

Despite all these advanced technology, we are still witness of information security breaches, and until to date there has not been any improvement yet. The challenge for many (if not most)

institutions and organizations today, is not only investing and improving security software and services; but it is also about creating and improving security awareness of the end user. Experts [10, 11, 12] argue that the best way of achieving good information security, and make employees comply with policies and procedures of the organization, is to arrange information security awareness education and training programs. Often, one might see that users have lack of knowledge about important assets of the organization. Nevertheless, in some cases even if they posses knowledge, employees intentionally or unintentionally neglect or disrespect security procedures and policies. Thus, the main point is not only to arrange awareness programs but to arrange effective and successful awareness programs. The report *"Effective Security Awareness"* conducted from Information Security Forum [13] states:

"The purpose of an effective security awareness program should be to create a change in behavior, rather than just to educate staff about what the desired behavior should be".

In order to identify the effectiveness of the Information Security Awareness Program (ISAP) it is highly recommended to assess and measure it. Everett C. Johnson from ISACA institute in the article *"Security awareness: switch to a better programme"* claimed as followes:

"Measurements should not be limited to a verification of whether the message was received by the target audience, but must address the effectiveness of the message and method, i.e. was there a behavior change?..."[14].

According to the statements above the most important issue is not only teaching employees and implementing ISAP, but measuring it's effectiveness and making change in behavior among the employees. The aim of the awareness program is not only to understand the concept of information security, but also to practice it during everyday life.

1.3 Keywords

Information Security, Security Awareness, Effectiveness, Awareness Training, Awareness Program, Classroom Training, Discussion Group Training, Web-based Training

1.4 Justification, Motivation and Benefits

Implementing information security awareness programs for an organization, is one way to manage and control security risks caused by human's lack of knowledge and wrong behavior [10]. As it is mentioned above, security experts highly recommend to invest on teaching users about what to DO, and what NOT to do, when using IT devices in order to achieve an acceptable level of risk [15]. The intention of information security awareness is to achieve prevention and mitigation of the risks. Prevention seeks to avoid situations where a security incident is about to happen, while mitigation seeks to limit the impact of an incident when it happens.

Opinions have been expressed that information security awareness is often not effective in managing and controlling security risks [11, 16, 17, 18]. The intention of this thesis is to exam-

ine the effectiveness of information security awareness program. Hopefully, this will help us learn how one can build and continuously improve better attitude and higher awareness of information security for all employees within an organization, particularly within teaching institutions. All this will be done by measuring the effectiveness of the information security awareness training.

People that deal with information security during their everyday work, hopefully will benefit from this research, especially schools and education environments, such as Gjøvik University College. To summarize the above, investing in security awareness program will most likely reduce incidents, assure business continuity and safeguard company's reputation.

1.5 Research Questions

More knowledge is required in identifying the key elements of an effective awareness program. An effective awareness program must ensure that the participants understand their IT security responsibilities, organizational policies, and equip them with the knowledge on how to properly use and protect the IT resources entrusted to them [12]. Thus, the intention of information security awareness program is to influence the employee's knowledge, attitude, and behavior, as well as making positive changes. Recently the information security awareness programs are criticized because that they are done poorly [16], or even they are called *"ineffective"* [18]. For this reason the following question is considered:

1. Is it possible to show that a information security training increases the level of security awareness?

   The assumption is that by measuring the effectiveness of the awareness program, might be one way of responding to this question. Also it is assumed that measuring the effectiveness of the awareness program, can be achieved by measuring the knowledge, attitude, and behavior, regarding the information security awareness among the participants, **before** and **after** the program. In the literature, many methods for assessing and measuring information security awareness are found. On the other hand, neither of these methods show to what extend the awareness training is effective, nor if it's indeed effective as many claim.

   Many methods and types of information security awareness training are provided in the market, such as: classroom training, web-based training, discussion-based training, etc. Each company providing any of these training types, advertise and claim that their products and training type is the best, depending on what they offer. Thus, the question below regarding this issue is:

2. Which type of training is the most effective in achieving higher awareness level?

   The decision making process about which type of training to chose might be difficult and

confusing. Thus, this is the main reason why this research is considering this issue, and tries to give a best solutions, suggestions, and recommendations, to help many of those interested on the field, to choose the most effective method. More specifically, this research tries to measure effectiveness in different types of awareness training, e.g (a) Classroom training, (b) Discussion-based training, and (c) Web-based training, in an institution.

1.6 Summary of Contributions

The aim of this research is to find out the effectiveness of the information security awareness program on employees knowledge, attitude, and behavior. The main point is to find out if the information security program is as effective as many experts suggest. In addition, an easy method for measuring the effectiveness of awareness program in practice, will be studied. Some instructions will be given about choosing the methods of the awareness program e.g. web-based style, classroom-based style, and discussion-based group style. The intention of the security awareness program is to become aware, stay aware, and to be aware in a continuous fashion.

2 State of the Art

This chapter explains in great details the thesis inspiration and motivation. The researchers' point of view about information security awareness, it's definition and importance are discussed and analyzed. While the effectiveness of the awareness program and its measuring method are finalizing this chapter.

2.1 Information Security Awareness

The most important factor in effective information security is to make people (employees at all levels) aware for their responsibilities and their role in information security [19]. This means to make the users aware of the risk they are dealing with, and stimulate them in preventing those risks by firstly raising the awareness in the information security. Information security awareness means understanding the potential security threats, issues and incidents that may exist and we are face with, in our everyday work. Security awareness teaches employees how to protect organization's information and how to take reasonable steps for preventing security breaches [20]. The goal of information security awareness is to make positive changes on the behavior of the employees, in every organization or company. Below are few definitions which helps understand clearly the security awareness.

Wilson and Hash from NIST (National Institute of Standards and Technology) in their article *"Building an Information Technology Security Awareness and Training Program"* [9] define security awareness in this way:

"*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more normal, having a goal of building knowledge and skills to facilitate the job performance.*"

ISF (Information Security Forum) [13] uses this definition for security awareness:

"*IT Security Awareness is the degree or extent to which every member of staff understands:*

- *the importance of IT security,*
- *the levels of IT security appropriate to the organization,*
- *their individual security responsibilities,*

- *...and acts accordingly*".

Shaw et al. [6] in the article *"The impact of information richness on information security awareness training effectiveness"* have this definition:

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

Regarding the definitions provided above we can notice that they are pretty much related to each other, since they aim at the same goal. Though, the first definition is more conceptual and highlights the background of awareness programs, whereas the second and third definitions refer more by suggesting the goals, or areas of the awareness programs. These definitions are studied and considered during this project, but it is discovered the need to narrow them down and adjust to our needs. This simple definition will be used during this project:

Information Security Awareness is the level of knowledge and attitude, regarding the importance and understanding of information security, and the willingness to act and behave accordingly in a continues fashion.

2.2 The Need for Security Awareness

PriceWaterhouseCoopers in the report *"Safeguarding the new currency"* [21] defines the information and the risks that might be involved by it, like this:

"*Information is the new currency of business-a critical corporate asset whose value rise and falls depending on when, how, where and by whom it is placed into circulation as medium of exchange. Therein lie the risks. And the opportunities*".

The user is the one who first deals with information in the organization. Information security management system of the organization is dependent from human factor as its processes. In other words user is the one that has access to the most valuable assets of the organization, such as information. As a result of this, most of incidents that are caused by employee's results in far more damage to an organization rather than incidents caused from external attacks. In today's world the target groups of an attack are mostly employee, and they are attacked in such a way that their identity has been stolen, *"phishing"* or other social engineering attacks.

Why Information Security Awareness is Important? Because it is a preventive measure and several international standards refer to this as a prerequisite, such as: ISO 27001[22], COBIT [23], Payment Card Industries - Data security, and ISO 9001:2000 [24]. Thus, if an organization or company wants to be certified from one of these standards, then it must implement security

awareness program at first. This highlights the importance of information security awareness, and explains the indication of being prerequisite for complying with the standards and being certified company.

Additionally, the importance of information security awareness is described form ISF [13] through its advantages. According to this article the role of information security awareness is:

- To reduce the number of security incidents.
- To comply with external standards/best practice .
- To address management concern about overall levels of information security.
- To comply with regulatory requirements.
- To satisfy the recommendations of a review.

In the bullet points above are clearly presented the advantages in which many articles are referring and addressing to. It is said that by making the employees aware regarding the information security, and it's threats the number of security incidents might be reduced, comparing to unaware employees. As complying with the law and regulations is important for any organization, reducing the number of incidents is highly important as well. By satisfying the recommendations of the review, is meant to comply with laws and regulations, and pass the audit process. The next paragraph elaborates the objectives of information security awareness while going deeper into its advantages.

Gary Hinson in his publication *"The true value of information security awareness"* [25], states clearly the objectives of information security awareness program, saying that it makes the information assets secure by:

- Informing people about information security risks and controls in a general sense, and providing more specific information and guidance where necessary;
- Emphasizing management's support for, and commitment to, information security;
- Promulgating the organization's information security policies, standards, procedures and guidelines, and externally imposed laws, rules and regulations.
- Motivating people to behave in a more security-conscious manner, for example taking security risks into account in business decision making;
- Speeding up the identification and notification of security breaches.

With these objectives in mind we can clearly understand the importance and the need for information security awareness program. According to those, awareness can bring new knowledge about the threats, risks, and help close security holes, when management is involved.

To what extent is important for Norwegian organizations and companies to implement information security awareness program? A recent survey conducted from European Social Survey [26], places three Scandinavian countries on the top of five countries that are considered most trusting, or naive in Europe, from which the first one is Norway, followed by Denmark, Finland and Sweden. According to this study four out of five Norwegians say that they trust people entirely, while only one per cent of them say that they are skeptical. Until late 1990s everyone could fly on domestic airlines in Norway without going through any security gates or detectors. Also, Norwegians are used to leave their homes unlocked until few years ago. According to these facts we consider that Norwegian companies desperately need information security training programs, since the probability of being victim of the social engineering, *"phishing"* or other related attacks is very high.

2.3 Investments on Security Awareness

Even though many organizations now might understand the importance of security awareness, not all of them are investing to implement it as they should. A recent report *"Global Information Security Survey"* which is conducted by Ernst&Young [1], gives a clear picture about the percentage of the companies willing to invest continuously on information security awareness.

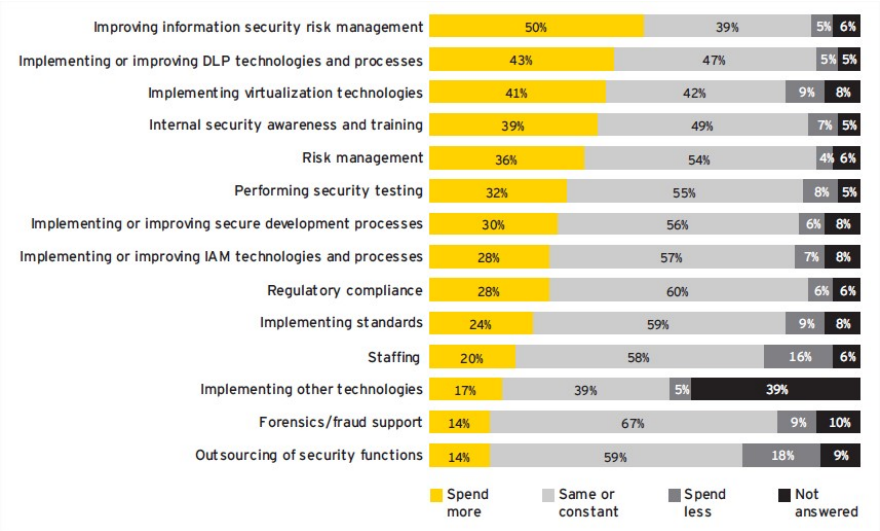

Figure 1: Further planning investments in internal security awareness and training [1]

Actually, over the last seven years a significant change has occurred on: (1) understanding, (2) giving the importance, and (3) readiness to invest on security awareness programs. According to this report the percentage of the organizations willing to invest in security awareness has become 39% last year (2010) compare to 16% on 2003. At least, *Internal Security Awareness and Training* is ranked number four from the all most important things to invest in the future, see

figure 1. However, this result is not yet something to be satisfied with. This survey also has identified an overall increase in external attacks (e.g., phishing, website attacks) as one might noticed in the figure 1 above. Also an increase in internal attacks (e.g., abuse of employee previlages, theft of information) has been 25%. These results should be seriously taken into consideration for a better and secure future.

Another report conducted from "Deloitte Touche Tohmatsu" (a Global Industry Group) with the title *"Losing ground, 2009 Technology, Media and Telecommunications (TMT)"* [27] finds that the challenged macroeconomic backdrop is causing companies to review costs in all areas, including security. The rsults showed that there was a significant drop in security investment, which is considered to have a determental impact in all aspects of TMT security. It is indicated that 32% of the respondents reduced their information security budget, while 25% raised their budget by 5%. After seriously considering these results this report comes up with important statement that is obvious and NO coment is needed;

"Companies should not forget about their long-term goals. At some point, the global economy is going to bounce back. Companies that underinvest in security now may find themselves vulnerable and unable to capitalize on the recovery. You might not have a problem in the short term, but you will have one in the long run".

Jonny Mathisen [28] in his master thesis potentiated that many of the large organizations in Norway, arrange some sort of security awareness program to increase the level of security awareness, and to change security culture positively. On the other hand according to a paper *"Unpublished Computer Crime Survey 2010"* (original title *Mørketallsundersøkelsen 2010 Informasjonssikkerhet og datakriminalitet"*) [29], conducted by Næringslivets Sikkerhetsråd on September 2010, it was said that only 1/3 of the Norwegian companies arrange a continuous awareness training for their employees, and less than a half of them arrange security awareness training for new employees. Another result to be worried about is that approximately half of the perpetrators behind the identified events are the organization's employees themselves. However, the question is, how many of these companies that arrange security awareness training, measure the effect of it?

According to these facts presented in the paragraphs above we can conclude that organizations have not invested sufficient resources to create and developing information security awareness, also their plan to invest in the future seems to be not sufficient. This implies that security awareness has not been funded as the optimal allocation of resources; in these cases it is underfunding. Monique Hogervorst [30] has common view for this evident lack of funding and she gives an explanation:

"Information security training and awareness is not recognized as a contributor to security."

Apparently in this sentence she is referring to budget holders who are supposed to fund the

information security awareness program. It could be logical to say that information security awareness is valuable and at the same time unrecognized. Probably the main reason for not sufficiently investing in information security awareness is because of the difficulties in measuring the return on investment and benefit of information security expenditure as McIlwraith sated [16]. However, it is in hands of security professionals to make the value of information security awareness more evident to the budget holders.

2.4 Human Element in Information Security

The human element of information security is still the most variable and unpredictable vulnerability source and the most uncontrollable factor in the information security [31, 32]. Thus, even those that consider themselves secure by using passwords for accessing computers or any particular data, in reality doesn't hold truth because one might choose guessable passwords or might share it, or if it is written down in a piece of paper near a computer someone can get hold of it. All this can happen because users are not aware of the importance of the information security, or they may not have a clear understanding about the risk. Paying more attention to information security involves practicing technical and theoretical (awareness) measures to reach a single goal. Information security is a critical and complex task; it is not just using usernames and passwords as a security measure [25]. Sveen et al. [33] in their article included an interesting statement saying that *"passwords only work as long as they are kept secret"*. For many years now information security programs are more focused in technical solution e.g. intrusion detection systems, firewalls, anti-virus programs, access controls etc, than in human element [31].

In a group project during the master studies we have conducted a survey in Gjøvik University College (in the course Scientific Methodology)[1] using this hypothesis *"Technology students are more aware and careful about the online security than the other students"*. The aim of this research was to get some insight about how seriously the students consider choosing a password. The results have shown that students from technology departments pay more attention to safety measures, and especially when choosing passwords (they use stronger passwords) than students of other departments, where most of them practice less safe methods. This makes information security awareness program a significant factor and a key issue in information security for any individual or organization.

Gross et al. [34] has another additional point of view according to the human element. In his research he also accepts that the user is a weak link towards information security, and that one single user could put in jeopardy the entire organization. However, in his research he claims that the analysis and resolution of the problem must address both the employee and the organizational issues. A simple example which compares two companies, where one of them is practicing more strict rules towards information security than the other, illustrates this statement better. In England a consulting officer lost his memory stick unintentionally containing sensitive personal

[1] This research has been conducted as a part of the course, and it is unpublished work. The group of five persons worked in this project (Blerta Lufaj, Fatbardh Veseli, Gazmend Bajrami, Kamer Vishi, and Ilirjana Veseli).

information for 84,000 prisoners of England and Wales. This was a breach of company's policy for handling sensitive government information securely, and destroyed its reputation [8]. In contrast to this is HIPA (Health Information Privacy Act) protocol used in health care systems in United States of America, where clearly states that any healthcare provider should not keep patients information in memory sticks or in laptops, and anyone who is prone to violation of this act will be responsible to its consequences and will face the law. These two examples gives us clear ideas that how a single employee can breach the well established information security processes of the naming organization, and in the other case where the organization laid down its laws and rules, also the consequences of breaking them in order to keep the information protected [35, 36, 37].

Another surprising and interesting example about the human element and the user's wrong behavior is written in InfoWorld technology magazine [38]. The story is about an IT administrator in the school Palm Beach County in Florida, which was sharing her password with one of the students working in a project. A student was able to change his and his friends' grades because of this. He also gave himself an "A" in a French class that he never took. This was a shock at the time of discovery. *"All my hackers are inside the network,"* says LaRocca the IT security director of this school. *"I'm not too worried about the ones from the outside."*

Based on previous facts and examples provided by authors, we consider that the main need to implement a well detailed awareness program, is to protect or secure the system from the human factor and their wrong behavior. Thus, some companies conducted security penetration testing reports, and their findings showed that their attempt to break into employee company computer systems by various social engineering methods are almost 100 percent successful [39]. Studies have also shown that about 80% of these security incidents come from staff negligence. For instance, it is very common for them to leave computers, or USB flash drives that hold sensitive information about costumers unprotected.

2.5 The Effectiveness of Security Awareness Program

The word "Effectiveness" used in this report is meaning the adequate method and program to accomplish the purpose. In our case effective information security awareness program means the program that is capable to influence the knowledge, attitude, and behavior of the participants and make positive changes in security culture of an organization. Many experts agree that information security awareness is effective, while some other have the opposite opinion about it, claiming that information security awareness is ineffective. In his book *"Information Security and Employee Behavior"*[16], Angus McIlwraith criticizes the effectiveness of information security.

"Information security 'awareness' has been promoted for many years as being fundamental to information security practice. In reality, it is something that is often done poorly - so much so that I have seen very limited progress since I started in information security over 20 years ago".

In most of the cases the statements about the information security awareness program are

made based on the assumption that it is, or will be equal to security. McIlwraith statement above let us understand that very few research is been done regarding effectiveness and efficiency of information security awareness. The importance of security awareness is discussed from many authors and organizations, but very few empirical studies are done, while none of them offer a technique which is effective in behavioral change. However, few experiments are done in measuring the effectiveness of the changes in behavior, such as Carnegie Mellon University [40], CISO (large large financial service) German organization [18], USMA (United States Military Academy) [41].

In the Carnegie Mellon study researchers established three groups consisting of 14 volunteer students each. Members from the Group 1 received a bogus *"phishing"* email. When clicked on the link attached on the e-mail, students were sent to a website that contained education materials telling about how to recognize suspicious e-mail messages, including advises to delete these e-mails without opening them. Members from the Group 2 have not received a bogus e-mail. As an alternative, they received education material relating to suspicious e-mail messages. While the members from the Group 3 did not receive any e-mail, not even were exposed to any education materials. After a week students from all groups have received another bogus *"phishing"* e-mail message. The results have shown that only 7 percent of the students from the Groups 2 and 3 were able to recognize the message as an example of *"phishing"*, while sixty four percent from the Group 1 recognized the message as suspicious. [40]

In the CISO case it was implemented an extensive and costly information security program. To all employees were sent awareness newsletters, and security related slogans and posters, such as *"security is everyone's problem"*, and they were placed in particularly noticeable locations throughout the organization. In order to test the effectiveness of the program CISO outsourced a company to perform penetration test by means of social engineering. The consultants from the outsourcing company were able to obtain the CEO's e-mail, and had gain confidential information from several systems within few days. The consultants have been moving freely throughout the company, wearing a T-shirts emblazoned with flashy logo, and not even any of the employees asked if they had permission to access the building. [18]

In the USMA case a professor published a study in which he explained the experiment done with his students. In his publication professor Ferhuson describes that for every beginning of the semester each of the cadets in the military academies were attending instructions regarding to information security. Additionally, freshmen cadets have been taught four hours more with the awareness instructions. The instructions included material relating to network security, identification and avoidance of viruses, worms, and other malware. In order to test the effectiveness of the instructions a *"phishing"* email was sent to all the cadets. In the experiment participants were randomly selected, and it was an equal number of freshmen, sophomores, juniors, and seniors. This email was sent from a bogus name *"Robert Melville, Col, UScc"*, where was included his fake address described as *"Washington Hall, 7th Floor, Room 7206."* Washington Hall was known to all cadets that does not have 7th floor. The message included there was a problem with

the cadet's grade, and the recipient was asked to click on the link to ensure that was accurate. The experiment found that eighty percent of all cadets clicked on the attached link, while ninety percent of the freshmen felled victim of this email. The professor concluded that security awareness instructions had not attained its objectives. He stated that *"Traditional classroom model is necessary but not sufficient when it comes to learning"*. [41]

All of these three studies presented here above have significant importance, since they measure the effectiveness of the awareness programs. On the other hand, they indicate question of validity of these experiments. In the Carnegie Mellon research has not been presented the material that they used to educate Groups1 and 2. Hence, it is not known if the content of the materials might have affected the results. The same comment could be given for the CISO study. Outsourcing company in CISO has tested the effectiveness by means of social engineering, but not even mentioned if this topic was included during the training, thus this could be the reason why consultants penetrate into the system. Regarding to the USMA case, probably cadets felled victim because the message was sent in the exams period, at what time the grades were especially important for the students. Perhaps, if this message would have been sent in different point in time the results might have been different. However, these results may be of value to reflect more about effectiveness of information security awareness programs.

2.6 Developing an Effective Awareness Program

According to Wilson et al. [9] from NIST institute there are three steps that one should take into consideration when developing IT security awareness and training program:

- Designing the program (which includes the development of the IT security awareness and training program plan)
- Developing the awareness and training material, and
- Implementing the program.

Besides, they also claim that awareness and training must be designed with the organization mission in mind. Awareness programs that include relevant subject matter and issues for the users are considered to be the most effective programs.

David Lacey in his book *"Managing the human factor in information security"* [42] also states that an effective awareness program should start with identification of the requirements and key problem areas, analysis of the root causes, and develop the programs that indicate corrective actions. There is always tremendous scope for improving information security awareness no matter the type of the organization. Lacey said that expressing knowledge and awareness is relatively easy fix, even if it requires consideration and planning. "It is giving the right information to the right people in the right form", he claimed. However, changing the attitude is considered much harder task. Lacey implies that changing the attitude involves a learning experience from an

activity such as reading a book, watching a movie or enrolling in a creative discussion. Changing the behavior requires clear understanding of the desired behavior, as well as acknowledgment of all the keystone of the enablers and blockers. [42]

According to Lasey [42] the awareness concept is not only teaching the employees and giving the lessons, and assume that participants will change their behavior positively regarding information security. Influencing human's behavior and changing their attitude is considered difficult process which requires experimental research and measurement. Probably the lack of reliable metrics to measure the effectiveness of information security awareness and changes in behavior is one of the factors that could contribute to effective awareness program. Many forms for communicating information security awareness and trainings exist in the marketplace today. It can be communicated through presentations, emails, publications, web pages, newsletter, posters or any other form of the corporate publication.

In the literature presented above it is found that effective information security awareness programs, begin by establishing the current situation in this field, and trying to answer the following questions:

- What employees know,
- What they think, and
- How they behave.

This triangle is also presented in the figure 2. Lacy [42] in his book also gives advices how to make a questionnaire which help to measure the awareness and behavior of the employees. But, all these come to a picking right method of teaching, or introducing employees to information security and its importance in work force.

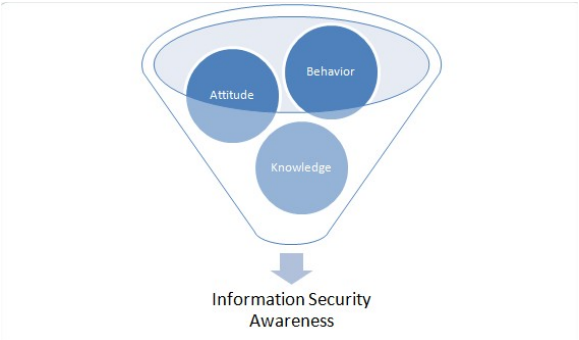

Figure 2: The triangle of information security awareness consisting of: Knowledge, Attitude, and Behavior

2.7 Measuring the Effectiveness of Security Awareness

It is difficult to state that the awareness program has reached its objectives without measuring it. Researchers or managers are confronted with two distinctive challenges when it comes to developing a measuring tool and perform the measurement. These challenges have to do with: What to measure and How to measure. Kruger et. al. [2] in the statement below explains how important it is to measure the effectiveness of information security awareness.

"Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programs to add value to an organization and at the same time make a contribution to the field of information security it is necessary to follow a structured approach to study and measure its effect.".

2.7.1 Identifying the Key Points of the Program (What to Measure?)

Some studies have been focused on what users believe and do about security in real world. At the same time some others have focused their research at security in organizational context, having in mind requirements of the organization and user participation to support compliance.

Kruger et al. [2] in the article *"A prototype for assessing information security awareness"*, gives an example on developing a model for measuring information security awareness. This model was applied in an international gold mining company. The goal of this project was to monitor changes in security behavior and as a result they revised or repeated security awareness campaign, whenever they identify the need for it to happen. Furthermore, in this paper when classifying what to measure they decided to measure these three dimensions: (1) knowledge (which was focused on what an employee knows), (2) attitude (what an employee think), and (3) behavior (what an employee does). These dimensions were subdivided into six areas as follows:

- Focus on the policy of the company,
- Keeping passwords and personal identification numbers secret,
- Using internet and email carefully,
- Using carefully mobile equipment,
- Report incidents like viruses, theft and losses, and
- Being aware that all actions carry consequences (this at the same time was the core of the program)[2].

These six factor areas were further subdivided into specific factors. For instance the second topic *"Passwords"* was divided into two subcategories such as *"Purpose of passwords"* and *"Confidentiality of Passwords"*. After that *"Confidentiality of Passwords"* was broken down again into *"Writing down of Passwords"* and *"Giving passwords to others"*. This is called tree model and it is illustrated below in the figure 3. One of the major challenges of this design was to keep expressions simple but meaningful.

However, it was found that the identified factors would not contribute in equal proportions to the final awareness level. The importance of the contributing factors was another important issue to be measured. This was achieved by allocating all factors in a specific branch of the tree factors by importance weights. For instance, different regions of the company have different weights as

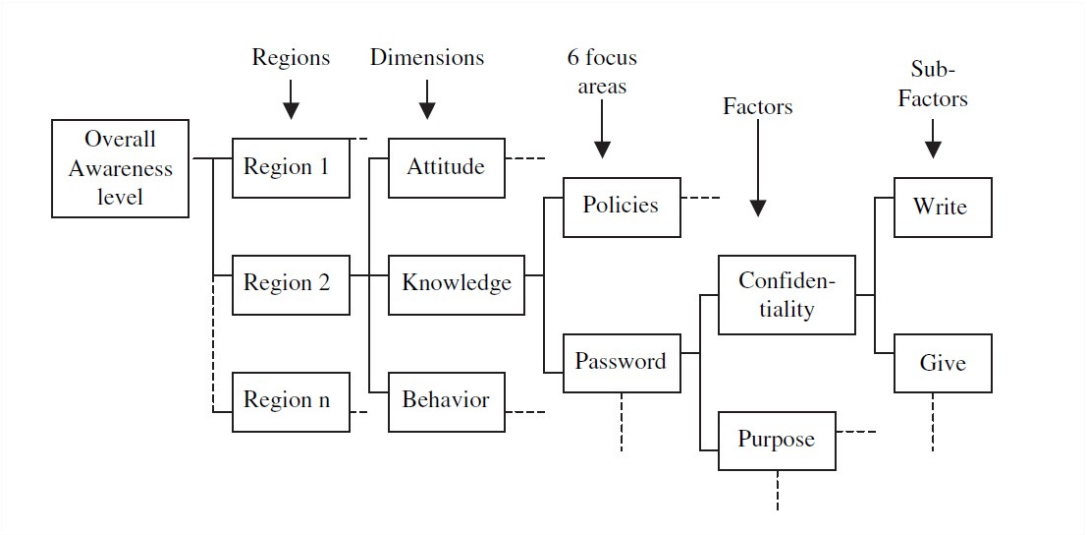

Figure 3: Tree structure of the problem [2]

they have different influence on the overall awareness levels. The three dimensions: knowledge, attitude and behavior have different importance level, while the six focus areas have different importance weights.

Another related article called: *"Looking for trouble: understanding end-user security management"* [34] the organization should focus answering to these questions:

- What do users know about security and threats?
- How do users manage their security concerns?
- Who do users believe is responsible for security, and how do they perceive their role in security?

The first question about identifying threats by users, and the sources of this information, will help designers to address user concerns and frustration. Answers gathered from the second question, help the designers and IT management to understand what really users are willing to, and capable of doing. Also, it gives a good conclusion of how well the organization trains their employees for practicing good security. Finally, from researches point of view and IT personnel, answering to the last question is simple and straightforward. They say that the responsibility for information security is on hands of the entire organization, or the responsibility is shared between users and IT staff. But, this is not necessarily the users view. The important thing is that between users and components of the organization should be maintained the relationship of trust. [34]

2.7.2 Identifying the Method of Measuring (How to Measure?)

Measuring three intangible dimensions such as: knowledge, attitude and behavior may appear to be not an easy task. Paula Davis in the *"Measuring the Effectiveness of Information Security Awareness Training"* [3] published some of the most effective methods, which help on measuring the security awareness of the employees. These methods are presented in the figure 4 below:

Attitudes	Knowledge	Behaviours
Surveys	Assessment tests	Behavioural measures
Interviews		Surveys
Focus Groups		Interviews
		Focus Groups

Figure 4: Methods for measuring attitudes, knowledge and behavior [3]

As it is illustrated in the figure 3, Paula Davis suggests that different methods should be used when measuring effect of the awareness program. When measuring the attitude for instance, it is assumed that the best result that one can get, is to use: survey, interviews, or focus groups, depending on the organization's needs (taking into consideration number of the employees, working effort, time, and costs).

Focus groups are form of a group interviews that are realized in a communication between participants in order to gather information. This method is convenient to gather the data from several participants simultaneously.

Interviews are used for collecting qualitative data. The participants are allowed to answer the open-ended questions without limitation on the time and scope. The major advantage of the interviews is that one can obtain useful data about things that cannot be easily detected (e.g. feelings, emotions, and attitudes).

The method used from Kruger et al. [2] is a good prototype of how the measurement is implemented in practice. The measurement is performed using a questionnaire. There were exactly thirty-five questions which were used to test the knowledge, attitude, and the behavior of the respondents. These questions were related with six main focus areas, in a combination with their factors and sub-factors as it is already mentioned in the previous section of this research. The questionnaire contained multiple choices, and some of the questions were answered on a 3-point scale (true, don't know, and false), while some others used only true or false answer. One sample of these questions used is presented in the figure 5 below.

However, Kruger et al. [2] denoted an important point saying that the actual behavior may not be measured accurately by a questionnaire alone, since the respondents do not necessarily tell the truth when they are asked about their behavior. They also implied that not all respond-

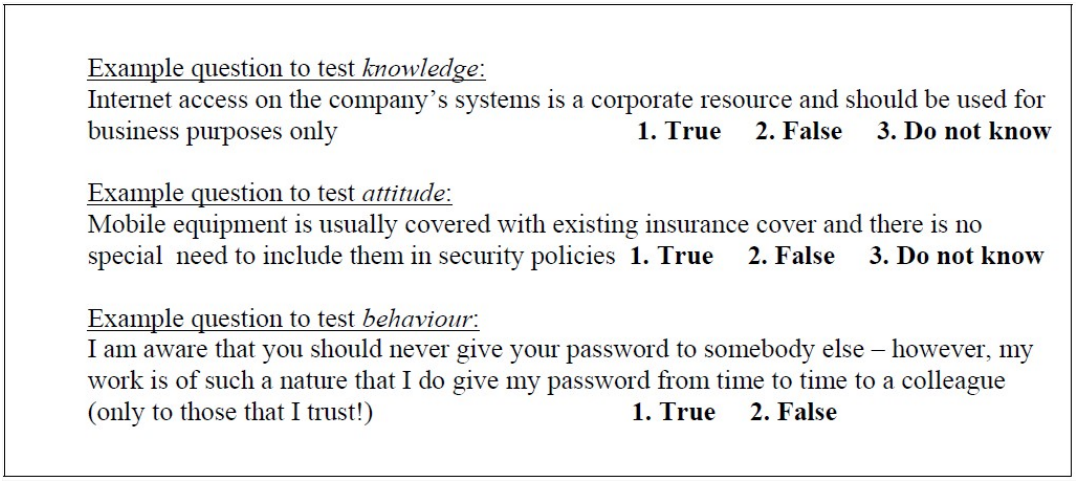

Figure 5: Sample of the questions [2]

ents will lie about their behavior. Besides, the use of questionnaire for this purpose will give at least an indication of the level of security behavior. This research also suggests that the measuring process for the behavior of the respondents should be accompanied with the physical test, while the internal audit may be valuable sources for this regard. However, one always will have another factor into play when conducting such a research, but it is always good to take into account the external factors.

Another useful and practical example about creating, maintaining, and changing security culture within the organization is done by Schlienger et al. [43] in the article "*Analyzing Information security culture: Increased trust by an appropriate information security culture*". This paper gives another similar idea with that of the Kruger et al. [2] when it comes to analyzing the security culture of the organizations, particularly explaining what to analyze, and how to analyze it. This research was done in Swiss Telecommunication Company Orange which offers mobile services. The methodology of this research was done using a survey. At the very beginning phase Schlienger et al. [43] analyzed the security policy of the company. By doing this, they wanted to understand the official rules, which are supposed to influence security behavior of the members of the organization. However, they were focused on this question:

- Do the employees know what the security policy states and do they also support it?

There were exactly ten questions, and each question analyzed three different parts: (1) individual attitude, (2) perception of the company's attitude (official values: security policy) and c) best solution. According to Schlienger et al. [43] this trichotomy gives interesting insights and reveals gaps between the individuals and company perception. Since the user has to reflect for the best possible solution it also has a didactic impact. In this research the questions were asked

in such a broad way and the focus was always on the center with information security. This research is an ongoing project and one could see the difference in socio-culture security measures among the respondents. *"The society will be more aware as time goes by"*, stated Schelienger et al. [43], and they continue *"information security is e new topic that many people can't yet wrap their brain around it, but soon it will be as important as having an e-mail today"*.

2.8 Learning Process

Learning process is interesting and unique among people of different ages. It is very simple process, as one learns he or she will get enriched with information until he/she stops learning, at that time next natural process comes which is forgetting what you learned. Therefore it is very important to keep learning always and never stop or give up. This process will best be explained by the figure 6 *"learning curve"*.

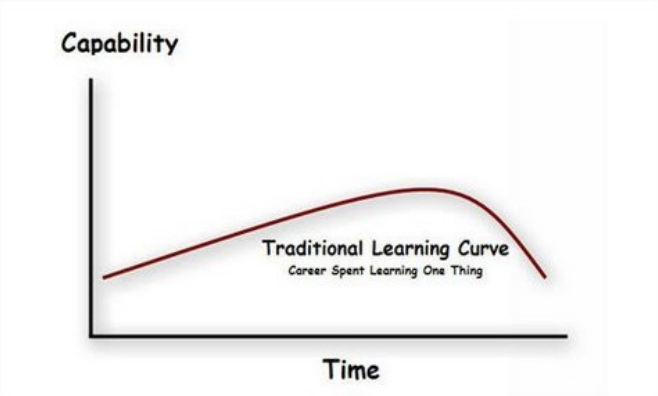

Figure 6: Traditional learning curve [4]

The figure 6 above explains how he/she learns and gets enriched with information, and reaches a peak on the graph, which is the highest level of knowledge. The process of forgetting takes event when he/she stops learning, and the curve in the graphs starts to downgrade when process of forgetting starts. This is related to classical style of learning. For instance a student after graduating from a school has reached the highest level of knowledge, but if he/she is not learning anymore, the process of forgetting the lessons learned starts.

The second graph presented in the figure 7 is more related to life-long learning, where people learn a little everyday and that grows with age. More you read and study the more you learn, and more you are exposed to the information, which you could be more likely to recall if necessary. In this research we are going to focus when the maximum learning peak has been reached and when the slope starts to downgrade. This process might be relevant with awareness training process in information security. Whenever the training takes place, the employees of the organization get aware about the new threats and consequences, which in this case would look similar

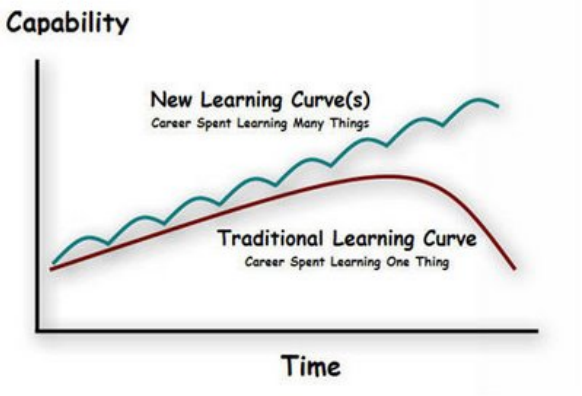

Figure 7: Continuous learning curve [4]

with the graph in the figure 7. However, if the next training is not arranged the process of forgetting lessons learned begins, and the graph for this process would be similar to 6. We will try to find out when the phenomenon of the forgetting about the lessons learned takes place, meaning that when it is the adequate time to arrange next awareness program, in order to prevent information security awareness from decreasing among employees.

3 Research Methodology, Strategy, and Approach

This chapter, is intended to describe the working method, which is used to find out the answers of the research questions, presented in the first chapter 1.5. The project begins with a simple question: Could scientific research help us understand and perhaps measure the effectiveness of the awareness program? In other words, could the same research tools used in the marketplace for security awareness, influence the employee's knowledge, attitude, and behavior? Is it possible to measure these changes? We believe the answer is yes.

3.1 Research Strategy

The overall research strategy consists of several sequential parts described in the following steps:

- Literature review about what is already known in the field.
- Quantitative data gathering (internet-based survey).
- Qualitative data gathering (interviews with IT and management).
- Analytical and statistical analysis of the data.
- Discussion of the results.

Broadly speaking, there are two types of research methodology: qualitative and quantitative method approach [44, 45]. In this research we use both methods since they are relevant approaches in our case, as it is suggested in the book: *"Research Design"* from John W. Creswell [45]. These method approaches were primarily used to develop knowledge, cause and effect, usage of measurements and observations, and testing theories. According to this book the best way of designing a qualitative research is first to identify the area of interest, and use existing literature to formulate research questions. The second step is designing the methods and tools for data gathering. In the end analytical and statistical analysis techniques, and processes are employed to present the results of gathered data. These rules for qualitative research design are followed and the overall methodology and the process steps of this project are illustrated in the figure 8.

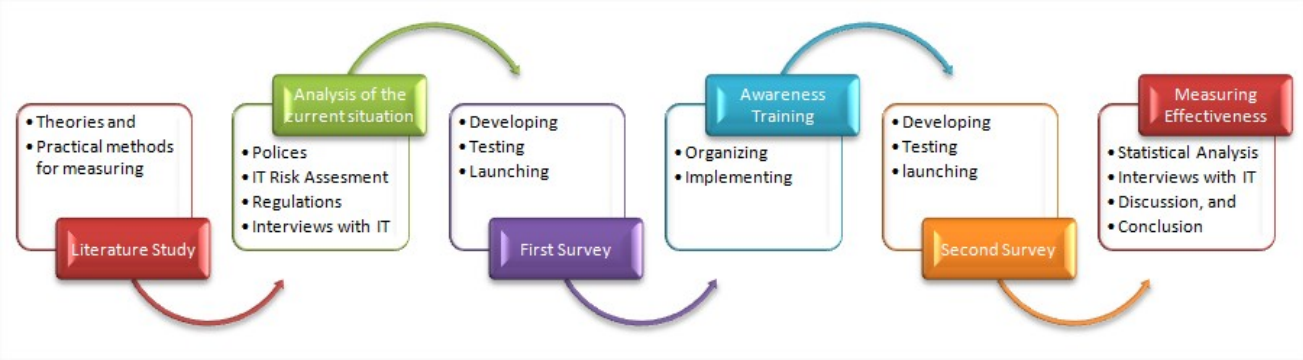

Figure 8: Research steps strategy

The picture 8 and following sections of this chapter explain in great details the overall research approach, methodology, and strategy of this thesis project.

3.2 Research Literature

The literature used in this research is concentrated on the related areas with: information security, security awareness and training, effectiveness of security awareness, information security culture, metrics for assessment, measuring the success of the awareness campaign, types of the trainings. Several sources are used to find out relevant literature, e.g. GUC library, and online library databases, such as: IEEEXplore Digital Library, ACM Digital Library, SpringerLink, ScienceDirect, CiteSeer and so on. Also, other relevant web sites and publication reports from security organizations, including search engines, to not forget some searches about psychological approach to changes in behavior.

From the literature study, it has been discovered that few theories exist related to measuring security awareness of the end user. On the other hand, empirical data exist to a lower degree. The entire methodology of this thesis is based from the findings on the previous literature.

3.3 Demonstration of the Case Study: Application to an Education Institution

Gjøvik University College (GUC) is chosen institution where this experiment is being developed and implemented. At first the intention was to apply this study in a private company, but GUC offered close collaboration and willingness to help on the realization of this project, and because the time limit of the project. It is estimated that at least one year is needed for such project, if chosen to implement in another company/organization.

GUC is an educational environment which offers different areas of study. Information security is an important academic focus for GUC. Last year (on 2010), GUC has completed Risk assessment for its facility and resources. After that security policy is developed, but for the time being

it is not yet issued; it is waiting for the board approval and signature. This means that employees of GUC, still did not have the opportunity to go through security policy of their institution. However, there exist a document for IT regulations named *"regulations for use of college computing resources"* (with original Norwegian name "*reglment for bruk av høgskolens datautstyr*"[46]). Yet, at GUC there is no information security awareness program implemented, and not either any security measurement done on this regard.

3.4 The Survey

The surveys are considered to be an excellent tool, for drawing out information from large number of participants, and to make possible the identification of broad tendency. The previous literature such as [2, 3, 43], strongly recommends to use quantitative data gathering method, when measuring the effectiveness of the awareness program. The physical test, such as observation of the end user (to get to know if they behave in accordance with security rules and regulations), is another method that is recommended in these articles, especially when analyzing the end user behavior, and the security culture of the organization. Nevertheless, due to the lack of time we will not consider physical test in this project, except the contacts and interviews with IT department.

Internet-based survey is the method used as our data gathering technique. The advantage of choosing internet-based survey, is because it makes possible statistical analysis of the results, and comparing the results with different groups of participants. In this experiment two surveys were used for the data gathering, one **before** and one **after** the completion of the awareness program. The first survey, measures current level of security awareness among participants, while the second survey, is intended to measure the effectiveness of the awareness program. A short review of the plan for the data gathering is presented as follows.

The Target Group

The employees of GUC are the population for this survey. GUC currently employs 327 people. The e-mail request to participate in the survey was sent to all 327 of them. It is assumed that the group is representative such that there are participants from: different ages (from 18 years old and further), different working department, both genders (male and female), different employment contract (full time, part time).

The Invitation to the Surveys

The e-mail request for participation is distributed with a prior agreement. Therefore, an agreement is made in advance with upper management of GUC for a permission to send out the e-mail invitation in their behalf. The aim of this idea was to get the employees attention and enlarge the number of participants. It is assumed that if the request is sent from the management's behalf the probability of having more participants would be higher. It is estimated that about 327 employee possibly will receive the request to participate in the survey.

The Survey Preparation

The survey itself was prepared specifically for GUC needs. The attempt was to pay special attention while forming the questions, and conducting the questionnaire, by following the survey rules stated at [47]. It is considered having short, meaningful, and understandable questions/statements, on the other hand, avoid the abbreviations and open ended questions. Also, the questions was carefully designed and implemented, in order to encourage participants to answer honestly, rather than giving the *"expected"* answers. According to *"Creative Research System"* [47], there are many steps that needs to be followed during the survey questioning, but here are presented some general rules, which at the same time are followed here:

- Consider meaning of the words and expressions used in the questions.
- Consider what information the respondents are asked to be able to answer the questions.
- Consider the scale of the answers the respondents are asked to give.

If these basic rules are not considered the survey would lead to misunderstandings of the questions and longer response time, which could lead to a higher drop-out rate.

3.4.1 The First Survey

The aim of the first survey, is to identify the current level of security awareness among the participants, towards information security and security regulations of GUC. Therefore, this makes possible to identify the weakest areas of information security, that the employees are lacking on. In addition, it is assumed that there is a possibility to take countermeasures against identified threats, and also increase the level of security awareness in those areas. This could be achieved by applying the adequate security awareness program, and by choosing the adequate topics to cover during the training phase. Hence, to be more concrete this survey helps to develop security awareness program and prioritize the topics that should be included, in order to increase security awareness among the employees within institution.

The Overall strategy of the questions is based on the measurement and methodology from the previous literature [2, 6, 34, 43], which is concentrated on testing employees:

- Knowledge (what do employee know regarding information security),
- Attitude (what do employee believe regarding information security), and
- Behavior (what the employee do regarding information security).

The ideas for choosing the question topics were based on literature studies, the actual hypothesis, and facts concerning issues of the institution. The facts from the organization issues were

identified from the (1) IT Risk Assessment, (2) IT regulations, and (3) The interviews with IT (The list of the events and incidents regarding information security that most often occur within organization). The goal of the interviews with IT was to capture the insights which help as guidance for developing the first survey questions, in conjunction with the GUC needs. The duration of the interviews was estimated, and it took approximately between 30-45 minutes. The topics of discussion included but were not limited to: The employee's lack of knowledge, (mis)behavior, and attitude, regarding the information security. Basically, the *"problems"* (events and incidents), that IT personnel most often experiences during their everyday business.

3.4.2 Topic Questions

The findings discovered from the analysis stated on the above paragraph, are analyzed in great details and compared to the literature study, such as [2, 13, 48]. The topic questions were organized in this order:

- Personal information about respondent,

1. Password management and protection,
2. Sensitive information handling
3. Social engineering
4. Physical/Office protection
5. Incident response - whom to contact

The first set of the questions asking about personal informations, were designed to perceive demographic knowledge, needed to characterize the respondents to the survey. The questions about the gender, age, working department, and type of employment, were asked. The idea of the question about working department was to make comparisons between departments and see if department of computer science and media technology is more aware than the other departments.

The other topics are intended to measure the awareness in terms of knowledge, attitude, and behavior among participants. Questions related to password protection and management, was designed to measure awareness behavior, except the one that was intended to measure the knowledge (such as: What do you think is a good password? See Q26 in Appendix A). The other questions about sensitive information handling, social engineering and physical/office protection, were more concentrated on measuring the awareness behavior, while the question about incident response - whom to contact, was intended to measure the knowledge, and reflect if participants have the knowledge whom to contact in case of an incident or security breach. The main reason of having more question/statement regarding the behavior, is because it is assumed that if the employees behave in accordance with information security rules and regulations, they most likely know about what the desired behavior should be, and as a results they have knowledge and

attitude regarding to the statements. This is done because the intention was to keep the survey completion time approximately 10 minuets. If for example there were three different expression types of statement for the same statement, e.g. statement regarding the knowledge, the attitude, and the behavior (e.g in the Kruger et. al. [2] article, see figure 5), then it would be required approximately 30 minutes time to complete the survey. Also, the third guidance from the above subsection 3.4, is taken into consideration, such as the awareness question/statement required five point scale answering to the questions. The idea behind this of having two more scales than in the figure 5 example, was to follow the progress of the employees after the training. Thus, it is assumed that by having more options to the answers the evaluation of the effectiveness of the training would be more obvious.

3.4.3 The Second Survey

The purpose of the second survey is to measure the effectiveness of the awareness program, which at the same time is the basis for this project. In other words, the importance of all this is to find out if the goal of the awareness program is achieved, and what are the results, precisely what needs are being met, not being met well, or not being met at all for each area of information security. Besides, the expectations of information security awareness program, also the difficulties to fulfill them will be drawn out on completion of the second survey.

Most of the question topics in the second survey were repeated, except for the first section of the questions. In the first section, about personal information were added two more questions, such as, the question about training participation, and defining the type of the training, also the question asking participants to evaluate the training (for more details see Appendix B). The question asking about training types, helps to compare the effectiveness between the training groups such as classroom-based, discussion-based, and web-based style. Also, the question "*what do you think is a good password*" was deleted, since it has open ended answer and did not allow us to make neither statistical analysis, nor analytical analysis, since the survey was anonymous and it was difficult to make comparisons for the answers before and after the training, and not even identify changes. In addition the question statement *"I think more about information security in my everyday work after the training"*, is added. The main idea behind this was to observe how this will be evaluated from different group of participants, such as: classroom, discussion-based, and web-based training groups. Also, to make comparisons between groups and see which group would be scored higher.

Design Issues

The focus was to keep the completion time around 10 minutes. Obviously, this would not give us very detailed measure of awareness, but since the respondents are recruited on voluntarily basis, the focus was to get as many completed forms as possible.

Almost all of the questions from the first survey were mandatory, except for the question *"what do you think is a good password"* which needed open-text answer, thus it was not man-

datory. Most of the questions contained multiple choice answers. In the second survey, two of the questions were optional, while the others were mandatory. The reason for using extensively mandatory questions, was because there was a need for completed surveys, to be able to analyze and use the results. One of the main points of the data gathering was to measure the effectiveness of security awareness program, thus partially completed surveys would be useless.

The surveys were prepared in both Norwegian and English languages using a software tool made available from GUC called *"Enalyzer Survey Solution"* (online survey software) [49]. Therefore the respondents had the opportunity to choose the language before initiating the survey. *"Enalyzer"* ensures safety and security of the data collection. Also, it gives the opportunity to export data into excel sheet or more advanced tools, such as SPSS [50].

3.5 Quality Assurance

The importance of qualitative research study has been seriously taken into consideration during the whole project, as it is described in the literature [44, 45, 47, 51]. The intention was to follow the steps provided in the literature for achieving qualitative study. The overall project work was done under the supervision, especially the surveys. A close work with supervisors has been done, and the surveys were tested as pilot project at first. Once we felt that the survey was near completion, we sent it out to 16 people with various levels of expertise on the area. It was requested from them to take the survey and comment on anything they did not understand, or had odd thinking in any way. Also, it was asked to measure the time needed to complete the survey. Later on, the comments were considered and reviewed, also the recommendations have been considered for further changes to the survey. The participants from the pilot group were consulted about every change regarding their comments, and the surveys were finalized. Consequently, it is assumed that the data from the survey are valid.

The surveys are self assessment, and that fact of not giving honest answers was considered, so the questions were carefully designed to motivate respondents to answer honestly, rather than giving an *"expected"* answer. The results of the surveys for all of the participants were confidential information, and have been treated as such. Therefore, also the anonymity of data processing was guaranteed. To each participant an informed consent was given about the anonymity, before deciding to participate in the survey. They were free to choose if they want to participate in the survey or not.

Considering these facts presented above, if chosen to repeat the questionnaires we believe that the same results will be produced. After all this said above, we assume that the data from this survey are reliable and valid.

3.6 Strategy and Plan for Data Analysis

In this section a short summary of the strategy and plan, for statistical analysis of the data from the surveys is presented. The plan is described in the following steps:

Surveys Responses include available information on numbers of completed and in-completed interviews. The distribution of the data among survey respondents, and comparisons between subgroups are identified. This being done using descriptive statistics, such as frequencies, bar-charts, plots, etc.

Descriptive Analysis about variables with interesting values will be presented, by means of standard deviation, score range, and related.

Awareness Level among participants, on the data gathered from the first survey will be investigated, presented, and discussed. This is the starting point that influences prioritizing the topics of the awareness program to be developed.

Awareness Program is organized and implemented. There were three types of trainings, such as: classroom, discussion-group, and web-based training. The participants are selected in terms of working departments (for further details refer to the next chapter).

Effectiveness of the Awareness Program will be examined. Comparison between the results from the first and the second survey will be made. Changes in awareness in terms of knowledge, attitude, and behavior will be discussed. Also comparison between the training groups, and their effectiveness will be expressed. To compare the means between two groups, the t-test such as the dependent sample, and the independent sample t-test, are used. While comparing the means between several groups, or to be more specific comparing several means, the ANOVA test is used. The confidence interval for all tests is 95%, which is reccommended for social science analysis. By statistical significance is understood that the observed mean differences are not likely to be due to sampling error, and it is expressed with *"p"*.

- If the $p > 0.1$ - the observed difference is *"not significant"*.
- If $p \leq 0.1$ - the observed difference is *"marginally significant"*.
- If $p \leq 0.05$ - the observed difference is *"significant"*.
- If $p \leq 0.01$ - the observed difference is *"highly significant"*[52, 53].

Tools for Analysis of the results from the gathered data, are used such as SPSS.

4 Awareness Training, Organization and Implementation

This chapter includes details about the development and implementation, of the information security awareness program. The demonstration about how the training is planed and implemented, and explanation about selection of training groups are given. In the last section, statistics of the participants into training groups are illustrated. In the figure 9 below are shown the steps for organizing and implementing the awareness program.

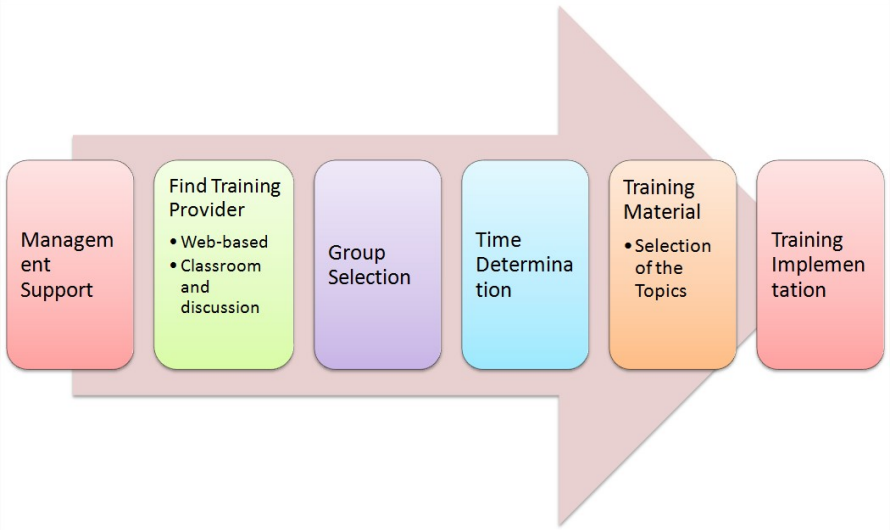

Figure 9: Training organization and implementation process

The steps presented in the figure 9 are followed during the implementation and organization of the awareness training program. In the following sections, explanations and details are given for each of these steps.

4.1 The Need for Management Support

The interviews with management of GUC were realized before deciding to implement the project. The goal was to get the management attention and support for the project, by describing benefits of it. It is estimated that duration time of the interviews was approximately from 30 to 45 minutes. The focus of the topics discussed included, but where not limited to: Importance of security awareness, methodology of the study, project benefits regarding information security for GUC, etc. For the completion of this project we received full support from GUC management and IT personnel.

4.2 The Group Selection (Based on the Working Department)

At first, the all 327 employees of GUC are divided into two main groups: web-based training and classroom-based training group. The groups are selected based on the working department. The employees from each department are partitioned into two groups of the employees, except the *"external workers"* (the original Norwegian name *"Eksterne"*). The external workers are part time employees, which are not regularly in their working place. Therefore, we decided to not partition this group at all and place it in the web-based training group. This decision was made to reduce the risk of having smaller group in the classroom training, and also to give the opportunity in order to all of the employees participate in the training.

Furthermore, from the classroom training group one small group of employees is derived consisting of 20 employees. This group is named discussion-based group, and is formed on the same idea based on the working department. The three created groups mentioned above (web-based, classroom-based, and discussion-based group) are intended to be representative groups, consisting mixed subgroups of employees from all four departments. The intention of designing representative groups is to have fair comparison between groups and meaningful results, when analyzing the data gathered from the surveys after the awareness programs take place.

4.3 The Time Determination

Setting up the date and time for the training was not an easy task, at least not for the classroom and discussion-based training. After considering all of the alternatives, the idea came up to identify appropriate date and time based on *"meeting for all (employees)"* (original Norwegian name is *"alle møte"*). The GUC arranges regular meetings for all employees every week. This occasion was good opportunity to let us suggest that probability of having bigger group of participants could be higher.

4.3.1 The Training Invitations

For the training invitations the same strategy is used like for the survey invitation. The e-mail invitation to all employees were sent on the management behalf, for the same reason prompting the employees into massive participation. Also, the same tools and techniques are used like in the survey invitations. The e-mail invitation was recommended as a request from the management, and was NOT mandatory.

4.4 The Selection of the Training Topics

The selection of the training topics is based on the facts listed in the following subsections.

The Results from the First Survey

The results of the first survey are analyzed in great details. From these results are identified the weakest points, towards information security awareness among the participants. In the following only a short list of them is presented (for more detailed analysis look at the chapter 6, under the section 6.2).

- Password management and protection (From the 159 completed survey, responses to the statement *"I write down the password in a piece of paper near my computer"*, were like this: 6 totally agree, 16 agree and 3 are not sure).
- Social engineering (159 respondents answers to the statement *"I don't have problem to tell my password to IT people if I am asked to"*, like that: 6 totally agree, 17 agree, and 28 not sure).

The IT Risk Assessment

The IT risk assessment document is taken into consideration and analyzed carefully. The list of the weakest points is extracted from it, and further discussed with supervisors, and adjusted with literature study specified for this area of interest. Because of confidentiality of this document we cannot publish the list of the possible threats, neither the findings from this analysis.

The Interviews with IT Personnel

The interviews and open discussions with IT personnel (especially with the head of the IT) are realized before and after the training, as it is indicated in the need for management support section (4.1) earlier. The topic of interviews were focused on the list of the events and incidents, regarding information security that most often occur in GUC, and that IT personnel most often faces. Another intention of these interviews was to find out the causes of the events and incidents, more specifically the areas of security awareness that the employees are lacking on. The suggestions of IT personnel about how to avoid these events and incidents in the future are taken into consideration while selecting the topics for the awareness training. The contacts and interviews with IT personnel are considered one of the qualitative methods used in this project.

The Academic Perspective

The identified points presented above (IT risk assessment, Interviews with IT personnel, The Results from the First Survey) are further analyzed and discussed. The literature in related area with information security topics and security awareness, is used for this purpose, such as [12, 13, 48]. The comparisons between academic literature, and our findings are made while the common topics are selected. These topics are:

- Password management and protection,
- Sensitive information handling (both hard and electronic copy),
- Social engineering (*"phishing"*, *"voice phishing"*),

- Physical/Office protection (unauthorized facility access),
- Incident response - whom to contact.

The fact is known and accepted that these are minimum necessary topics comparing to the world's newest threats, and the requirements of GUC needs. However, we also have to bear in mind the views from pedagogical perspective, which proves that an adult cannot remember more than five to six topics for one class session. Another additional fact is considered, that information security terminology and topics are considered difficult for non-technical employees. Someone can argue that we could arrange more than one session. Well that is true, but our time limitation does not allow this to happen. The only thing we can do is to hope that in the near future someone will proceed further with the project, and continue this process.

4.5 Training Types and Training Providers

In the subsections below, details are given regarding each of the training types. The company providing the classroom-based and discussion-based training, also the company providing web-based training, preferred to remain anonymous. Further, only the details about how the training is organized and implemented are shown.

4.5.1 The Classroom-based Training

The classroom training session was prepared and organized in both languages: Norwegian and English. The invitations were sent to 125 employees. Both Norwegian and English sessions were planned to last not more than 30 minutes. There were 26 participants out of 125 invitations (in average of 20.80% from the invited employees), and the session was in Norwegian language only, since no one from English speaking employees showed up. The training went well and everything went according to the plan, except that it lasted about 10 minutes longer.

It is considered that the main reason for having such a small participation group, is because the training was considered recommended and not required. The reason that nobody from the English speaking employees appeared, could be because most of them are working in the Faculty of Computer Science and Media Technology, and probably they consider themselves specialized in the field. Another reason for not having a massive participation could be the time factor; probably this was not a convenient date and time for most of the employees, so they decided to skip it.

4.5.2 The Discussion-based Training

For the discussion-based training the invitations were sent to 22 employees, while only 9 employees participated in the training, in other words 40.90% from the invited employees showed up. The duration time of the discussion-based training was planned about 40 minutes, but it lasted 15 minutes longer then expected. The group was mixed with participants from different working departments, and they had interesting discussion with each-other about everyday work and security events. They learned a lot from one another since one of the participants was expert in information security. They were outlining security challenges of the institution and how to

overcome these challenges. The major concern for most of them was how to easily remember passwords.

The Instructors of Training

The teachers for classroom and discussion group training were experts in the area of information security. One of them has experience with IT and information security for more than 25 years, while the other holds PhD degree in the information security and is working in this field.

4.5.3 The Web-based Training

The e-mail invitations to participate in the web-based training were sent to 180 employees. The e-mail was sent from an outsourcing company that offers web-based training. The all session took six working days period of time, and one lesson was sent per each day which includes one topic. The topics selected were the same as for the classroom and discussion-group training. From all 179 participants receiving the lessons, 38 of them were active and reading through all the lessons, meaning that 21.11% of participants were active. From all these 38 active participants 19 of them were completing all 6 lessons, 6 of the participants completed 5 lessons, while the other 6 participants completed 4 lessons.

One of the factors that could have indicated for not having massive participation in the web-based training, is because the e-mails with the lessons were sent from the outsourcing company, thus many of the employees considered them as *"phishing"* e-mails. Some of the employees asked the IT department if that was *"phishing"* e-mail containing viruses. Another indication could be the same as for classroom and discussion group trainings, since the invitation to participate in the training was not required. Also all from the external workers were placed in this group, and they may not check their e-mails regularly, so this could be another indication as well.

Among all these training types, we can conclude that all of them are producing something valuable to the end user in one form or another. About classroom training as classical teaching style, we don't have a lot to say except the calculations about how many participants were there, and their concern about how to easily remind passwords. It is difficult to conclude if the focus of the participants was 100% in the tutorials and teaching materials. While for discussion-based this is more obvious, since all of the participants are involved in discussion, and the teacher can easily get the perception if they got the idea about the topic, also what is their attitude regarding that topic. The web-based training style, is not giving any impression if the participants understand what they are reading, nor what they think about specific topic. However, it produces statistical results about how many participants are going through the lessons, and how many of them complete the training. More details will be given about which one among these types of trainings is more effective and why, in the section 6.6.

5 The Response Data

This chapter will include the data responses and statistics regarding both, first and second survey. Further details will be given for each of them separately in the following sections.

5.1 The First Survey Responses

Neither of the books [44, 54] gives a precise explanation about the size of the desired sample for the small population such as 327 employees in our case, though it is suggested that the bigger the size the better is the sample. However, it is assumed that the number of respondents in the first survey is quite satisfied. The total number of 159 completed survey forms out of 327 sent requests, gives enough data source for satisfying the statistical analysis that will be conducted in the next chapter.

Table 1: Second survey responses

Sent survey requests	327
Completed Surveys	159
Completion Rate	48.62%
Uncompleted forms (after started)	10
Average Completion time	9 minutes

The percentage of completion rate is 48.62%, as it is presented in the table 1. The completion rate may not be sufficient as it is suggested 50% per smaller than 500 group sample, however we need to consider 36 external workers here. If chosen not to send survey requests to this group the percentage of completion rate would be 54.63%, which would be higher than it is recommended in the literature for an average small sample group. And, since this experiment it is trying to measure the effectiveness of the awareness program, and since the participation was vulentirly, we consider that our sample in the survey is enough to dicover what we need. The total number of dropouts or uncompleted survey forms after it has been inciatiated is 10 or the average of 5.9%.

5.1.1 The Respondents

The aim objective of a sample group from a population is to get as representative selection of the population as possible. In the next subsection the details about the sample group of the first survey will be given.

The Sample Distribution Based on Gender, and Working Department

In general GUC has four main working departments, such as: (1) Administration, (2) Faculty of Health, Care and Nursing, (3) Faculty of Computer Science and Media Technology, and (4) Faculty of Technology, Economy and Management.

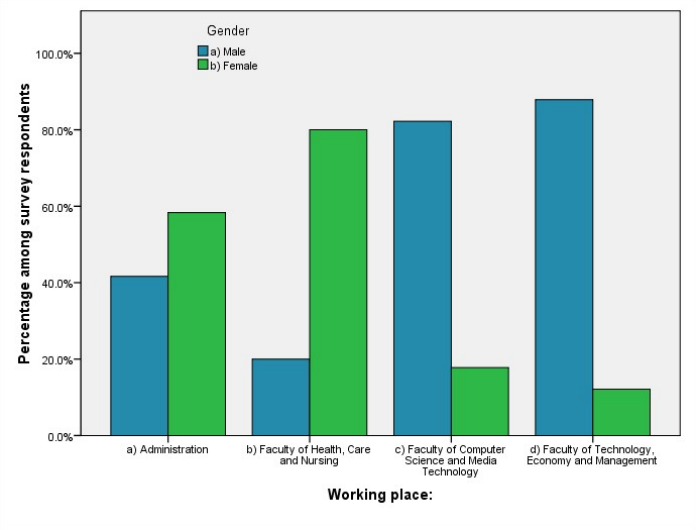

Figure 10: First survey responses based on gender, and working department

The participation in the first survey among departments was 22%, 28%, 28%, and 21% respectively. As it is presented in the figure 10 the sample was representative, since there were almost equal number of participants among all departments. Even though it may not appear representative, the fact that Faculty of Health Care and Nursing, and Faculty of Computer Science and Media Technology employ more employees should be considered. The gender distribution in the first survey was somewhat skewed among the participants, and departments. As one can see male employees participated with 57%, while female employee participated with 43% in total. The reason for having skewed participation in this case is because GUC employs more male than female employees. Gender participation for each department beginning from (a) Administration as visualized in the figure 10 was: 41.66% male and 58.33% female, 20% male and 80% female, 84.44% male and 17.77% female, while in the (d) Faculty of Technology, Economy, and Management the participation was 87.87% male and 12.12% female. These figures are also realistic, since the fact is known that more females than males are studying nursing, and more males than females are studying science and engineering.

The Sample Distribution Based on Age, and Employment

The age for our sample is mixed, but as it is shown in the figure 11 there is significant number of participants above 50 years old.

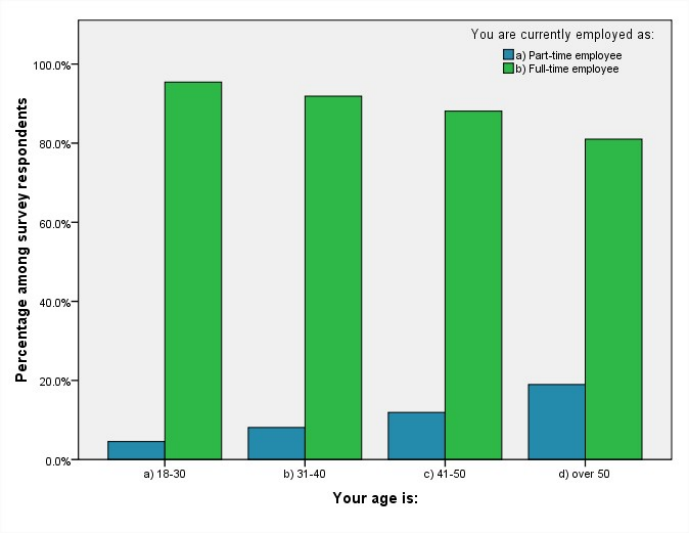

Figure 11: First survey responses based on age, and employment

There are 14% of participants from 18−30, 23% from 31−40, 26% from 41−50, and 36% over 50 years old. This happened because GUC has employees over the age 18, and more of them are over the age 50. If the employment type is compared, being that (a) Part-time or (b) Full-time employees, one can see from the figure 11, that the second option (b) is dominating in all cases of the age distributions. As it comes into view from the above figure, in the results of the first survey most of the respondents belong into full time employment option. The percentage among the participants in the first survey was: 13% part time employees, and 87% full time employees in total.

5.2 The Second Survey Responses

On the second survey were identified lower number of participants compare to the first survey. In total there were 110 participants. There were number of the reasons indicating to have lower participants in the second survey than in the first one. However, the main objective of the second survey is to measure the effectiveness of the awareness training, thus the focus was to include the participants that have completed the training, in order to realize measurements and analysis of the data. Also, another reason for closing the survey with this number of participants is because of the time limitations of the project. The table 2 gives the statistics of the respondents for the second survey.

The survey request was sent to all 327 employees and in total gathered 110 responses. The completion rate of the second survey is 33.63%, while the average completion time was nine minutes, the same as the first survey.

Table 2: First survey responses

Sent survey requests	327
Completed Surveys	110
Completion Rate	33.63%
Uncompleted forms (after started)	7
Average Completion time	9 minutes

5.2.1 The Respondents

It is indicated in the previous section 5.1.1 that the main objective of a sample group is to get representative selection. However, the main objective of our sample in the second survey is to get responses from employees that participated in the training, for the reason already mentioned in the above paragraph. In the following subsections, specifications about the respondent sample group are given. The same logic is used as for the first survey; however some additional variables are added.

The Sample Distribution Based on Gender, and Department

The participation in the second survey regarding the working department was approximately similar to the first survey, with very few changes. It is seen in the figure 12 that the participation in percentage for four working departments, consisting of: 22%, 32%, 22%, and 25% from (a) Administration, (b) Faculty of Health, Care and Nursing, (c) Faculty of Computer Science and Media Technology, and (d) Faculty of Technology, Economy and Management respectively.

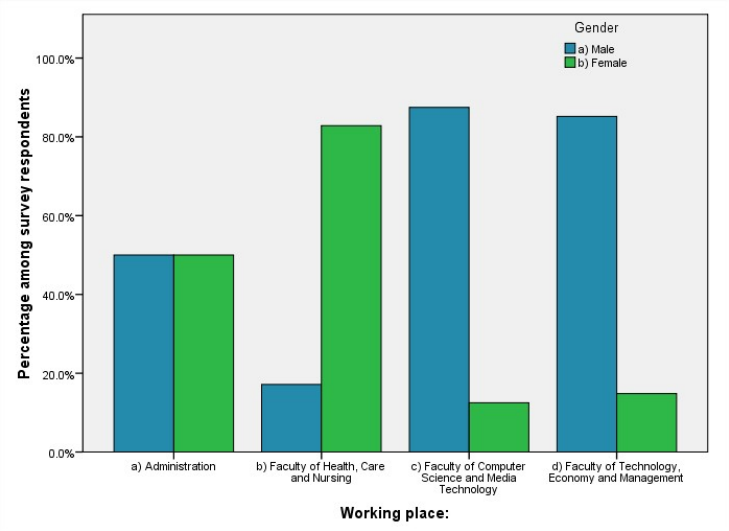

Figure 12: Second survey responses based on gender, and working department

Again there was a skewed participation between male and female employees. The male participation was 56% and 44% was the female participation in total. It was equal participation

number between males and females in the (a) Administration department, from 50% each. In the (b) Faculty of Health, Care and Nursing there were 17.14% males, and 82.85% females. In the (c) Faculty of Computer Science and Media Technology the average for males was 87.5% and for females was 12.5%. And in the last department in (d) Faculty of Technology, Economy, and Management the participation was 85.18% for male and 14.81% for female.

The Sample Distribution Based on Age, and Employment

The age sample representation was almost in the same range as for the first survey. The average was as follows: 5%, 21%, 30%, and 44%, for $18-30$, $31-40$, $41-50$, and over 50 years old respectively. The average of the employment contract was 10% for part time employees and 90% for full time employees. This is also elaborated in the figure 13.

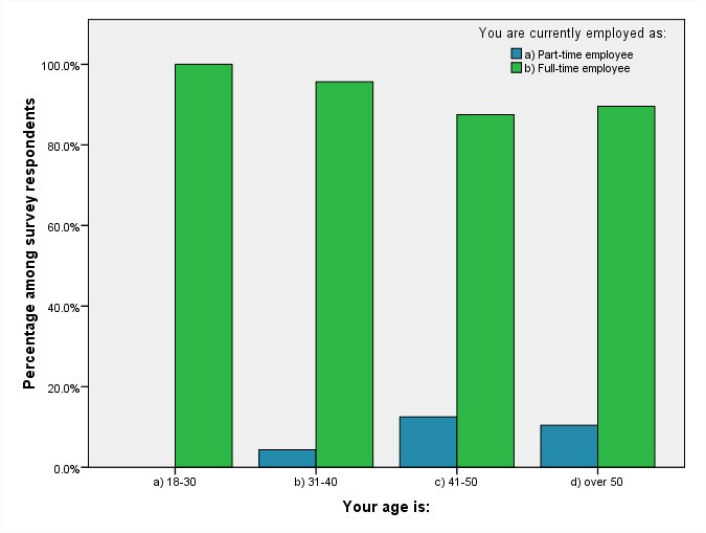

Figure 13: Second survey responses based on age, and employment

The Training Participation

In the chapter 4 some statistics are given in regards of the training participation. The classroom training (including discussion-based training, since this subgroup was made from classroom training group, see section 4.2 for more details) had in total 35 participants and an average of participation from 23.80%, while web-based training had 38 participants in total, and the average of participation was 21.11%. On the other hand, in the second survey the participation was: 20(18%) participants in (a) Classroom-based training, 6(5%) participants in (b) Discussion-based training, and 38(35%) participants in (c) Web-based training, while 46(42%) participants were not taking part in neither of training groups, as you may see the figure 14.

In the question asked *"Why you did not take part in the training?"*, the 9(8.2%) respondents answered that they did not have time, 33(30%) answered that the time and date was not suitable,

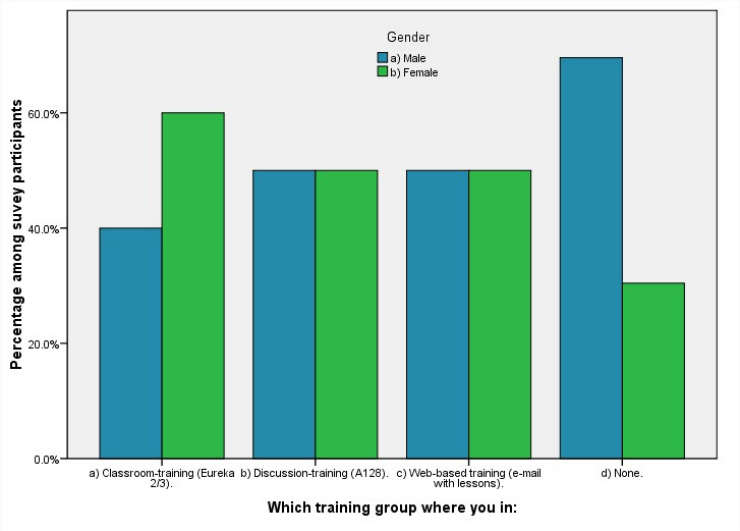

Figure 14: Training participation based on the type of training, and gender

2(1.8%) felt that the training was not important for their job, while 8(7.3%) answered that they were experienced in the field. And since this question was optional it gathered only 52 answers (for detailed question please refer to Appendix B, question number Q6. Another important question for us, which gave the opportunity to the respondents to evaluate, and express their opinion about the training is presented in the figure 15.

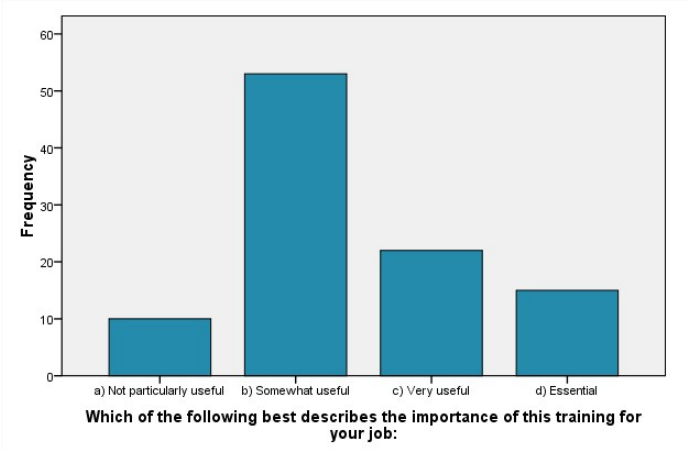

Figure 15: Training evaluation from participants

Since this also was optional question, it gathered 100 responses, and most of the respondents (53 responses, with average 48.2%) have rated the training as somewhat useful, 22(20%) of them evaluated as very useful, 15(13.6%) considered essential, while 10(9.1%) respondents considered

the training not particularly useful.

6 Statistical Analysis and Discussion

6.1 Preparation

The online survey software "Enalyzer" [49] offers the opportunity to export the results from the surveys to Excel sheet, including descriptive statistics from the surveys and for each question separately, as well as the raw data. Considering the fact that we had two surveys to compare with each other it was decided to use SPSS software [50], as it is considered more sophisticated tool than Excel. The books such as [52, 53] are used for the introduction to statistics with SPSS.

In subsection 3.4.3 is discussed about the types of the questions, and that most of the questions had mandatory answers, including the reasons for choosing this method. It is also seen from the descriptive statistics and distribution rate in the chapter 5 that in total were 10 uncompleted survey forms in the first survey, and 7 in the second, with the average from 5.9% each. Thus, the idea of having most of the questions with mandatory answers worked out satisfactorily in both surveys. It was decided to not export uncompleted survey forms to SPSS, even though SPSS handles cases of missing values. However, it was a flow in the survey software and many string data were included in the data file while exported. Thus, it was needed special attention to determine which data should be removed from the data file after they were converted into SPSS data file for further analysis.

The answers to the questions in the row data are represented as values between 1 and n, where n represents the number of the answer alternatives. After combining the results from both studies (survey one and two) into one data file, it was realized that few of the answer alternatives needed a value recode. Since the majority of the questions asking about awareness had the same scale from totally disagree to totally agree, with the value recode this scale was reversed converting the scale into the opposite order, from totally agree to totally disagree. This alternative order makes a less aware choice score lower and a more aware choice score higher. The questions that needed value recode are presented in the table 3, and the numbers are based in the second survey (see Appendix B). An example of a value recode is given in the Appendix C.

Table 3: Recoded (or reversed) questions

Q8	Q9	Q11	Q12	Q14	Q15	Q16	Q17
Q18	Q21	Q22	Q23	Q24	Q25	Q27	Q29

The results from the surveys will be presented in the following sections. At first the questions' grouping, then statistical results and frequency distribution, also the facts from the first survey are displayed and discussed, while later the data from both surveys are compared between each

other in order to observe the effectiveness of the awareness program.

6.1.1 Questions' Selection and Grouping

The groups of questions are made for the simplicity of the analysis before starting the analysis on the data and measuring the awareness level among the employees. The groups are called indexes and are based on the question topics as it is described in the earlier chapter, particularly on the subsection 3.4.2. Each group is calculated separately consisting of two to seven questions, depending on the topic. There are created exactly six groups of questions or indexes, as presented in the table 4. The numbers of questions in the groups are based on the second survey (see Appendix B). The second survey had more questions, though it was easier to move the data from the first survey to the second for each question separately. This is the main reason why the analysis and question numbers are based on the second survey.

Table 4: Groups of questions - (indexes)

Gr. 1	Password management and protection	Q8	Q9	Q10	Q12	Q13	Q14	Q29
Gr. 2	Sensitive information handling	Q18	Q19	Q23	Q24	Q25	Q26	Q27
Gr. 3	Social Engineering	Q11	Q17					
Gr. 4	Physical/office protection	Q15	Q16					
Gr. 5	Incident response - contact to whom	Q21	Q22					
Gr. 6	Total index - all questions together	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 5		

Only the questions included in this table are considered during the statistical analysis of the results. The questions Q20 and Q28 are not belonging to any of the groups. In view of the fact that question Q28 is additional question belonging to second survey only, it is not considered while analyzing the results from the first survey, either for comparing the results from the surveys between each other. However, the results from these questions are presented below in this chapter. The question Q20 is considered that it is not measuring information security awareness, instead it has to do more about the feeling that the employees have regarding policies and regulations of the institution.

6.1.2 The Distribution of the Data

After the question groups are made, as presented previously then the normality of the distribution among the groups is tested. At the time when scores were grouped and presented in a frequency table it was seen that the overall score looked pretty normally distributed for our sample, see figure 16.

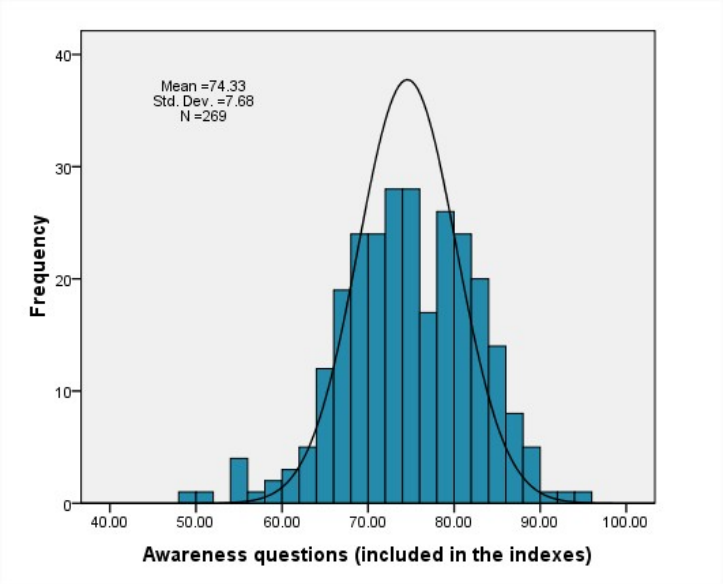

Figure 16: The total index score

The values for skewness was $-0,324$ and the value for kurtosis was $+0,243$, and according to [53] a value between -1 and $+1$ is acceptable. Thus, it can be concluded that the distribution of the gathered data for all of the question groups was normally distributed. Each of the topics are tested separately for the normality of the distribution, and they resulted to be normally distributed, but for the simplicity the other plots will not be displayed here. However, the figure 17 is the fact for normality distribution for each of the topics.

The Kolmogorov-Smirnov and Shapiro-Wilk test compare the same mean and standard deviation testing whether distribution is normal. If $p < 0.05$ then the observed value is significantly different from normal distribution, if $p > 0.05$ the data are normally distributed. But, according to [52] these tests have their limitations, because with a large sample size (which in our case is very big $df = 269$) it is very easy to get significant value. Thus, the significant test doesn't neccessarly show whether the diviation from normality is enough to bias any statistical procedures that we apply to the data. In this case we can conclude that the data is still normally distributed.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Password management and protection	.088	269	.000	.980	269	.001
Sensitive information handeling	.099	269	.000	.964	269	.000
Social Engineering	.237	269	.000	.814	269	.000
Physical/office protection	.153	269	.000	.907	269	.000
Incident Response - whom to contact	.149	269	.000	.941	269	.000

a. Lilliefors Significance Correction

Figure 17: Test of normality using Kolmogorov-Smirnov and Shapiro-Wilk test

6.2 Awareness Level - Results of the First Survey

The results from the first survey presented here below are based on the training topics. These results are seriously considered for choosing the training topics, among many other reasons as explained earlier.

6.2.1 Password Management and Protection

At first it is decided to present the results from the first survey. The reason for applying this method is because we want to give to the reader the explanation and justification of choosing the training topics mentioned in the subsection 4.4. For few of the training topics the base was the results from the first survey, while the reason for relying on this is self explained, if one can follow results from the samples of the questions presented here. At this point, descriptive analysis and the answer frequencies for the questions that are identified as having lower awareness scores are presented. The illustrations are based on the question topics, and from each topic are chosen few questions. The first topic is *"Password Management and Protection"*, which is presented with two samples.

In the first sample statement *"I write down a password in a piece of paper near my computer"* shown in the figure 18, the respondents answered differently. More to the point, the most of the answers were *"totally disagree"* with the statement, which gives the idea that current situation in place, might be *"fair"* or *"good enough"*. However, if the point of view from Gross et. al. [34] is considered here, which argue how a single user can put in jeopardy the entire organization, than the previous statement of *"fair"* or *"good enough"* doesn't hold truth. In fact the 6 (or 3.8%) responses were *"totally agree"*, 16 (or 10.1%) *"agree"*, and 3 (or 1.9%) were *"not sure"* for saving passwords in a paper near a computer, which is something to be concern about and that

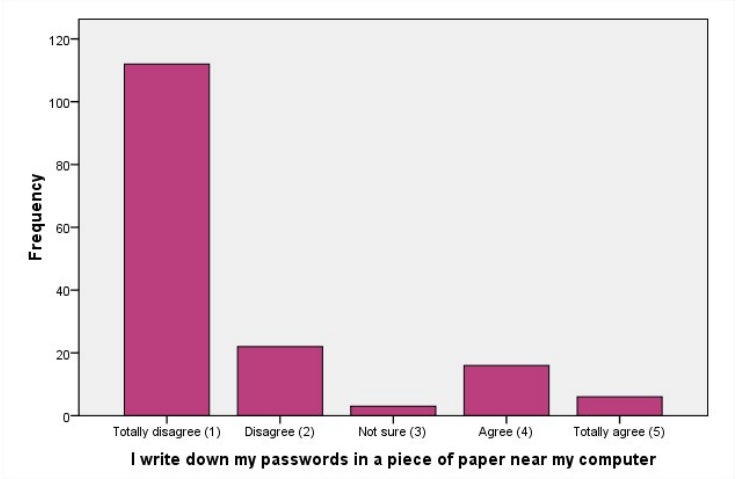

Figure 18: The responses for the statement *"I write down a password in a piece of paper near my computer"*

need special consideration in educating employees, and hopefully improving information security awareness in this regard.

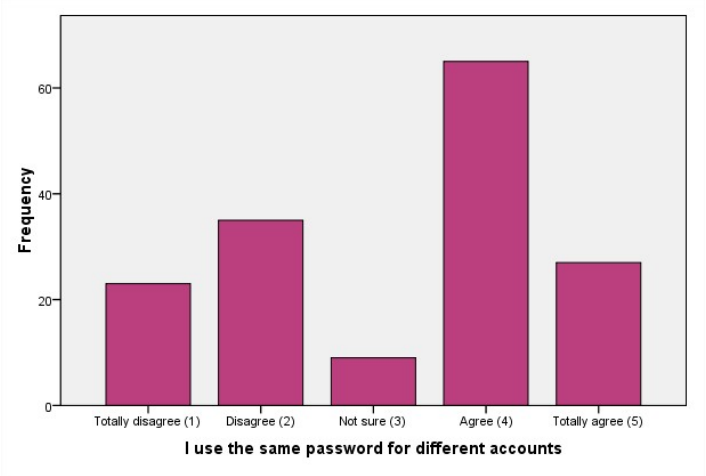

Figure 19: The responses for the statement *"I use the same password for different accounts"*

From the observation of the results it is found out another reason which supports the idea of including *"Password Management and Protection"* as a topic of discussion during the training phase. In the figure 19 is shown the statement *"I use the same password for different accounts"* including the *"drastic"* responses (if we are allowed to refer it that way). As it is seen there are more responses *"agree"* than *"disagree"*. Actually, the 159 respondents answered to this statement as follows: 27 (or 17%) totally agree, 65 (or 40.9%) agree, 9 (or 5.7%) not sure, 35 (or 22%) disagree, and 23 (or 14.5%) totally disagree.

6.2.2 Sensitive Information Handling

One of the facts that made us believe that *"Sensitive Information Handling"* topic should be included in the awareness training is because of the results to the statement presented in the figure 20.

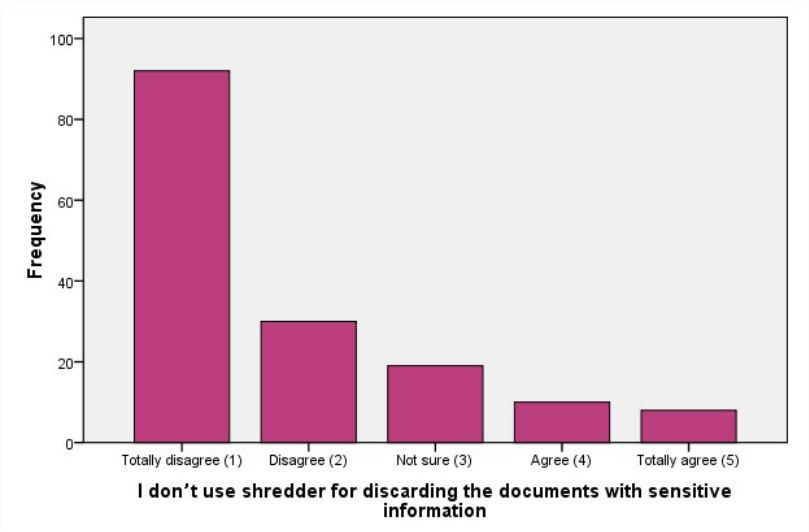

Figure 20: The responses for the statement *"I don't use shredder for discarding paper documents with sensitive information"*

In this action statement *"I don't use shredder for discarding paper documents with sensitive information"* the respondents had these answers: Totally agree 8 (or 5.0%), agree 10 (or 6.3%), not sure 19 (or 11.9%), disagree 30 (or 18.9%), and totally disagree 92 (or 57.9%) responses. It is considered that even these small figures with the responses *"totally agree"* and *"agree"* have a significant weight, to not mention the worst case scenario and the possible consequences of what would happen if someone can get hold of at least one of the sensitive data. For instance, if unauthorized persons can get access to personal information about students (such as transcript of records), the reputation of the institution would be destroyed, and most likely the number of students would decrease. This could have tremendous impact on the most valuable assets for the institution, which are the students.

6.2.3 Social Engineering

In the literature [39, 55] are given enough reasons arguing why social engineering is considered one of the most vulnerability element towards information security and security systems of the organizations. Social engineers use human element rather than technology flows to hack into systems. Even in the *"black hat"* conference [56] is discussed about social engineering, with the strong emphasis on the importance of the user awareness.

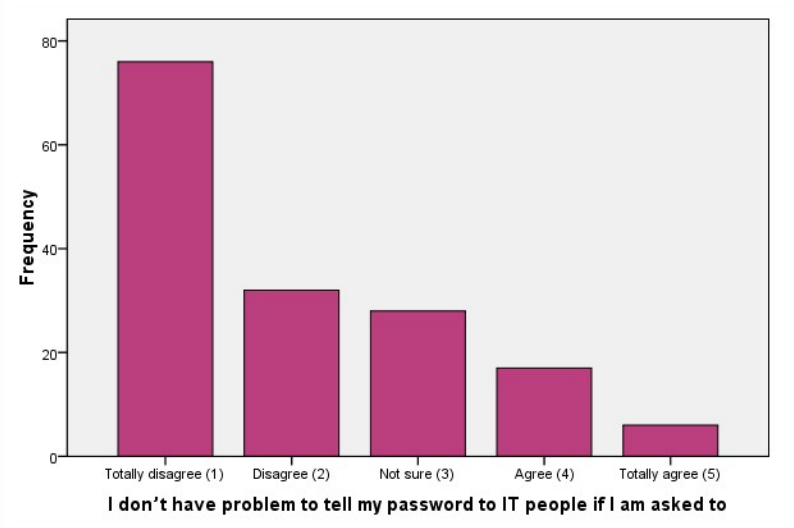

Figure 21: The responses for the statement *"I don't have problem to tell my password to IT people if I am asked to"*

Another additional fact that supports the above points of view, about covering *"Social engineering"* topic in the training, is brought from the answers gathered on the statement *"I don't have problem to tell my password to IT people if I am asked to"*. In the figure 21 are illustrated the results, which consist of: 6 (or 3.8%) totally agree, 17 (or 10.7%) agree, 28 (or 17.6%) not sure, 32 (or 20.1%) disagree, and 76 (or 47%) totally disagree responses. According to these results one may persuade many questions, such as: what if someone impersonates him/herself while making a phone call pretending to be an IT employee, and asking for password? This and other related questions no longer need comments.

6.2.4 Physical/Office Protection

The responses from the statements: *"I don't use password protected screen saver"* and *"I don't lock the door of my office during office hours, even if I am away"* (for further details to the second statement refer to Appendix D), brought enough reasons to believe the necessity to include *"Physical/office protection"* topic in the training as well. In reality the first statement has gathered extreme results. The responses were like this (look at figure 22: 42 (or 26%) totally agree, 33 (or 20.8%) agree, 14 (or 8.8%) not sure, 16 (or 10.1%) disagree, and 54 (or 34.0%) totally disagree.

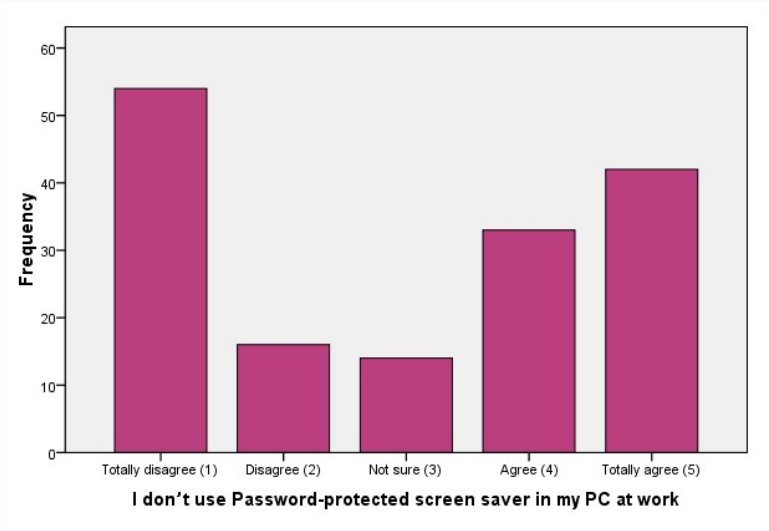

Figure 22: The responses for the statement *"I don't use password protected screen saver"*

6.2.5 Importance of Incident Response, and Whom to Contact

Education Center for Applied Research (ECAR) has released an article with the title *"Incident Response: Lessons Learned from Georgia Tech, the University of Montana, and The University of Texas at Austin"* [57], in which besides others it was stated:

"...you can limit the damage done and lower the costs of recovery. By knowing whom to call and what to do next, you can decrease the amount of time it takes to recover and possibly save you and your staff from additional disasters along the way."

In the above statement is emphasized the importance of knowing whom to contact in case of an event or incident. If the employees don't know whom to contact many events and incidents can happen and go unrecognized and undetected. Thus, for an institution might be created the false idea that they are safe, and no incident is occurring. Moreover, encouraging employees in reporting the incidents helps in closing the possible holes, and discovering vulnerabilities in the system.

In the statement *"In case when one of my colleagues is breaching the information security rules and regulations, I pretend that I am not seeing"* (figure 23) the majority of the responses where between *"not sure"* and *"disagree"*. However, there were many responses *"agree"* to the above statement. The figures of the results in the above statement are: 1 (or 0.6%) totally agree, 10 (or 6.3%) agree, 57 (or 35.8%) not sure, 60 (or 37.7%) disagree, and 31 (or 19.5%) totally disagree. According to these results it is considered that there is a desperate need to show the benefits of reporting the incidents and whom to contact if something suspicious is happening. Therefore, taking into account all this said, it is considered reasonable to include the topic about

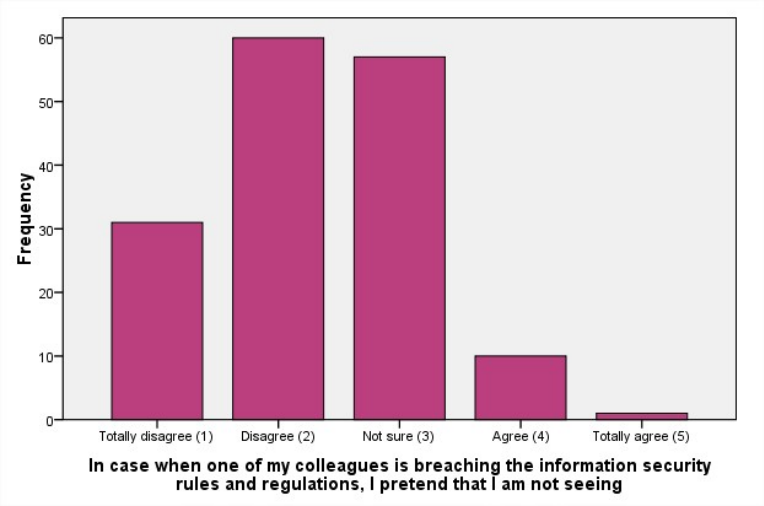

Figure 23: The responses for the statement *"In case when one of my colleagues is breaching the information security rules and regulations, I pretend that I am not seeing"*

incident response in the training. For the effects of the training and if the pretended objectives are or are not met you can read in the following sections.

6.2.6 Are The Employees of Computer Science and Media Technology Department More Aware than the Others - (Results of the First Survey)?

The intention of testing this assumptions was to find out the questions already planned for this project. One of the questions mentioned in the subsection 3.4.2 was to find out if there were difference among departments, especially between Faculty of Computer Science and Media Technology and others.

			Sum of Squares	df	Mean Square	F	Sig.
Password management and protection * Working place:	Between Groups	(Combined)	49.827	3	16.609	1.453	.230
	Within Groups		1771.922	155	11.432		
	Total		1821.748	158			
Sensitive information handeling * Working place:	Between Groups	(Combined)	170.255	3	56.752	4.238	.007
	Within Groups		2075.720	155	13.392		
	Total		2245.975	158			
Social Engineering * Working place:	Between Groups	(Combined)	19.793	3	6.598	2.518	.060
	Within Groups		406.182	155	2.621		
	Total		425.975	158			

Figure 24: Compare means test between departments and awareness

The compare means test between the questions topics and working department is executed. The results showed that most of the departments scored approximately the same in most of the topics. It was only one significant difference between Faculty of Health, Care, and Nursing department and others. This department scored higher in *"Sensitive Information Handling"* than the others. Furthermore, if you look at the picture 24 above, you will see that $p = 0.007$ (or $sig. = .007$) meaning that this result was highly significant. Also the same department scored lower in *"Social Engineering"* topic, with a $p = 0.06$, and it was marginally significant. In the picture 24 are presented the p values for both cases in the first and second row (see the sig. (significance) column).

6.3 The Differences in Awareness Between Sample Subsets - for Two Surveys

In chapter 5 is seen the sample distribution and the participation for both of the surveys. The sample was somewhat skewed between gender, age, department, and employment. Yet, it is tried to discover if there might be differences between sample subsets, which might help to better predict about how the employees of the institution will score on the overall awareness, and also on the selected topics separately.

6.3.1 The Differences on Gender

The awareness mean score is compared between the two genders. For the analysis both tests are used such as, independent sample test and ANOVA. In total it is seen the Mean of 72.94 for the males and 76.13 for the female, which is obvious that females scored higher in majority of the topics, and the difference is significant at level 0.1%, (or $p = 0.001$).

			Sum of Squares	df	Mean Square	F	Sig.
Password management and protection * Gender	Between Groups	(Combined)	52.786	1	52.786	4.239	.040
	Within Groups		3324.597	267	12.452		
	Total		3377.383	268			
Sensitive information handeling * Gender	Between Groups	(Combined)	215.687	1	215.687	16.782	.000
	Within Groups		3431.540	267	12.852		
	Total		3647.227	268			
Social Engineering * Gender	Between Groups	(Combined)	11.015	1	11.015	4.473	.035
	Within Groups		657.521	267	2.463		
	Total		668.535	268			
Physical/office protection * Gender	Between Groups	(Combined)	8.892	1	8.892	1.727	.190
	Within Groups		1374.848	267	5.149		
	Total		1383.740	268			
Incident Response - whom to contact * Gender	Between Groups	(Combined)	19.108	1	19.108	10.540	.001
	Within Groups		484.066	267	1.813		
	Total		503.175	268			
All topics together * Gender	Between Groups	(Combined)	675.275	1	675.275	11.915	.001
	Within Groups		15132.279	267	56.675		
	Total		15807.554	268			

Figure 25: Compare means test between genders and awareness

In the figure 25 are shown the all topics and the significance level for each of the topics sep-

arately, including all topics together. The topics in which female employees scored higher than males employees are: (1) Password Management and Protection with the significance level of $p = 0.04$, (2) Sensitive Information Handling with significance level of $p = 0.000$, (5) Incidents Response-Whom to Contact with the significance level of $p = 0.001$. Weather, males scored higher only in one topic (3) Social Engineering with significance level of $p = 0.035$. The difference between genders in the topic (4) Physical/Office Protection is not significant, but if the Means scores are compared still the female employees scored higher than males.

6.3.2 The Differences on Age and Department

The tests for observing the differences between age and department were similar as for the tests used in the previous example about gender. However not much of the differences are observed from these executed tests. In all questions together that measure the awareness is not observed significant difference among groups, moreover in some topics there are some differences. For instance, in the topic (1) Password Management and Protection there is significant difference (where $p = 0.033$) between the Faculty of Computer Science and Media Technology and other departments. Meaning that, this department scored higher than the others. At the same time, in the topic (2) Sensitive Information Handling the departments, such as: (a) Administration and (b) Faculty of Health, Care, and Nursing scored higher than the others, with the significance level of $p = 0.001$.

The test for discovering the differences on the age showed similar results as for the departments. Only two differences regarding the ages are discovered, and those in the topics (4) Physical/Office Protection and (5) Incidents Response-Whom to Contact. In the topic (5) participants over the age 50 scored higher than the others, with the significance level of $p = 0.043$, whilst in topic (4) participants between the age $31 - 50$ scored higher than the other, with the significance level $p = 0.023$.

Also, there is not any significant difference discovered among the participants from full-time and part-time employees.

6.4 The Effectiveness of the Training - (Statistical Analysis)

In order to find out if the training added value to information security culture of the institution, and if it was effectiveness the statistical analysis are applied. The mean scores between group of participants that attended the training, and the group of participants that did NOT attend the training are compared and tested. ANOVA and independent sample tests are used for testing this assumption. The group of those that attended the training consists of: classroom training, discussion-based training, and web-based training. While the group of Not attended consists of those that did not attend neither of the training, or with the other words the group of the participants that chose *"None"* as the answer in the question *"Which training group where you in?"* (See Q5, in appendix B). The results showed that there is a significant difference between groups,

thus the participants from the group that attended the training scored higher in all topics. In the figure 26 are presented the values for all topics and differences of the means between groups.

	Training	N	Mean	Std. Deviation	Std. Error Mean
Password management and protection	Not Attended	46	23.0217	3.86143	.56934
	Attended	64	24.6094	3.42084	.42760
Sensitive information handeling	Not Attended	46	27.2174	3.80592	.56115
	Attended	64	28.1250	3.37357	.42170
Social Engineering	Not Attended	46	8.9783	1.48308	.21867
	Attended	64	9.2031	1.28705	.16088
Physical/office protection	Not Attended	46	7.3913	2.18559	.32225
	Attended	64	8.0313	2.10041	.26255
Incident Response - whom to contact	Not Attended	46	7.1304	1.42375	.20992
	Attended	64	7.7969	1.18428	.14804
All topics together	Not Attended	46	73.7391	8.78998	1.29601
	Attended	64	77.7656	7.17301	.89663

Figure 26: Compare means score between the groups Attended and Not Attended the training

Generally, if all means between groups are compared then it is clear that the group of employees that attended the training are scored higher in all topics separately, than the employees that did not attended the training. The topic (2) Sensitive Information Handling has the Mean value of 28.12 for those that attended the training and value of 27.21 for those that did not attend. The topic (3) Social Engineering resulted in the Mean value of 9.20 for the attended group and the value of 8.97 for not attended group. The topic (4) Physical/Office Protection has the Mean value of 8.03 for attended group and the value of 7.39 for not attended group. Though, as it is mentioned above in general all topics are scored higher from the participants that attended the training against those who did not.

The topics that have shown a significant difference between groups are: (1) Password Management and Protection, and (5) Incident Response-Whom to Contact. The first topic is significantly different at the level value of $p = 0.025$, while the fifth topic is significantly different at level value of $p = 0.009$, meaning that those that attended the training scored higher than those that did not attend the training, including also all topics together where it seems that the training had positive effect, since the difference between groups was significant at level value of $p = 0.009$.

6.5 The Effectiveness Among the Training Types

To find out which of the training type between (a) Classroom training, (b) Discussion-based training, and (c) Web-based training is more effective a different types of tests are executed, such as: Compare Means test, Independent Sample t-test, and One-Way ANOVA (including means plot). The results show that traditional style of training, such as (a) Classroom training participants scored higher than participants from the other training styles. In the figure 28 is presented means

			Sum of Squares	df	Mean Square	F	Sig.
Password management and protection * Training	Between Groups	(Combined)	67.460	1	67.460	5.174	.025
	Within Groups		1408.213	108	13.039		
	Total		1475.673	109			
Sensitive information handeling * Training	Between Groups	(Combined)	22.047	1	22.047	1.739	.190
	Within Groups		1368.826	108	12.674		
	Total		1390.873	109			
Social Engineering * Training	Between Groups	(Combined)	1.353	1	1.353	.719	.398
	Within Groups		203.338	108	1.883		
	Total		204.691	109			
Physical/office protection * Training	Between Groups	(Combined)	10.961	1	10.961	2.402	.124
	Within Groups		492.894	108	4.564		
	Total		503.855	109			
Incident Response - whom to contact * Training	Between Groups	(Combined)	11.887	1	11.887	7.149	.009
	Within Groups		179.577	108	1.663		
	Total		191.464	109			
All topics together * Training	Between Groups	(Combined)	433.910	1	433.910	6.975	.009
	Within Groups		6718.354	108	62.207		
	Total		7152.264	109			

Figure 27: Compare means test between groups of training, Attended and Not attended

plot of the awareness in the all five topics together.

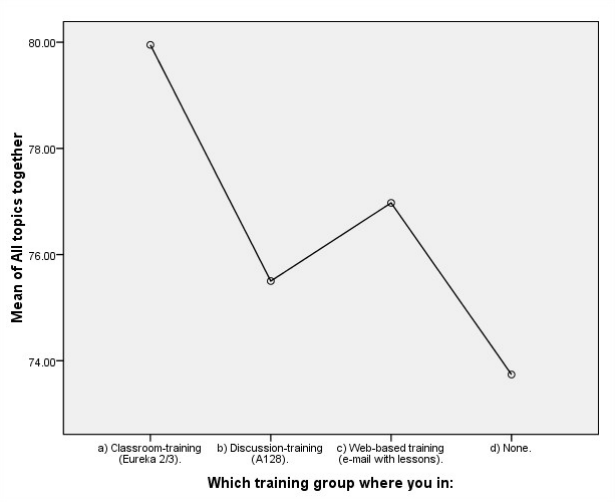

Figure 28: Compare Means for (6) All topics together (awareness) between three training types

The topics that gathered significantly higher scores in classroom training are: (1) Password Management and Protection with level value of $p = 0.011$, (5) Incident Response-Whom to Contact with level value of $p = 0.036$, and all topics together with the level value of $p = 0.028$. These presented topics have significant difference increase in linearity as well. The table of results is presented in the figure 29, where N is representing the number of responses, while $Std.Deviation$ is representing standard deviation. The other results (figures) for each of the training topics separately are presented in Appendix E.

Which training group where you in:		Password management and protection	Sensitive information handeling	Social Engineering	Physical/office protection	Incident Response - whom to contact	All topics together
a) Classroom-training (Eureka 2/3).	Mean	26.2000	28.3000	9.2500	8.1000	8.1000	79.9500
	N	20	20	20	20	20	20
	Std. Deviation	3.54816	3.27832	1.51744	2.04939	1.25237	7.57055
b) Discussion-training (A128).	Mean	23.0000	27.8333	8.5000	8.6667	7.5000	75.5000
	N	6	6	6	6	6	6
	Std. Deviation	2.52982	5.07609	1.51658	1.50555	.83666	5.39444
c) Web-based training (e-mail with lessons).	Mean	24.0263	28.0789	9.2895	7.8947	7.6842	76.9737
	N	38	38	38	38	38	38
	Std. Deviation	3.23400	3.21636	1.11277	2.22746	1.18790	7.08438
d) None.	Mean	23.0217	27.2174	8.9783	7.3913	7.1304	73.7391
	N	46	46	46	46	46	46
	Std. Deviation	3.86143	3.80592	1.48308	2.18559	1.42375	8.78998
Total	Mean	23.9455	27.7455	9.1091	7.7636	7.5182	76.0818
	N	110	110	110	110	110	110
	Std. Deviation	3.67944	3.57216	1.37036	2.15000	1.32535	8.10044

Figure 29: Means values for awareness among training types

The answers of the statement *"I think more about information security in my everyday work after the training"* are combined with the types of trainings to reflect about their effectiveness. The *figure* 30 is representing the results from this measurement. The majority of the answers are with the *"Not sure"* option as it is seen, which are chosen from respondents that did not attend any of the trainings.

Most of the answers *"totally agree"* are selected from participants of (a) discussion-based training, whether the answers *"disagree"* and *"totally disagree"* are selected from participants of (a) classroom training, (c) web-based training, and (d) none of the training. The responses to this statement are: 9 (or 8.2%) totally disagree, 15 (or 13.6%) disagree, 47 (or 42.7%) not sure, 31 (or 28.2%) agree, and 8 (or 7.3%) totally agree.

After the independent sample t-test of this statement, between the group of participants that attended the training and the group of participants that not attended the training is discovered a significant difference. Hereupon, the participants that attended the training scored higher with the $Mean = 3.34$, while participants that did not attended the training scored lower, with the $Mean = 2.83$, and the Levene's Test [52] for equality of variances resulted significantly different between groups, with the values of $p = 0.005$.

In Regard to the statement *"Policy and regulation about information security disturbs or delays me doing my regular work"*, the respondents had this attitude: 4 (or 1.5%) totally disagree, 21 (or 7.8%) disagree, 67 (or 24.9%) not sure, 107 (or 39.8%) agree, and 70 (or 26.0%) totally agree to the statement. These results presented here are combined between both surveys,

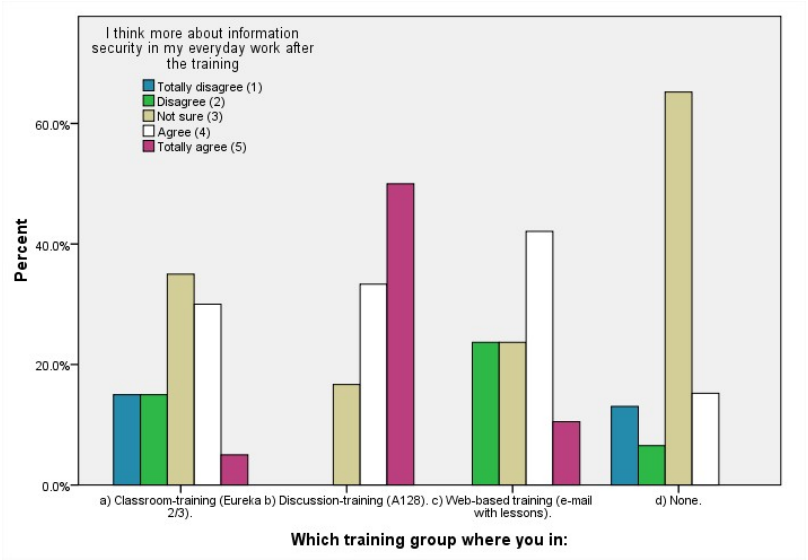

Figure 30: Average of responses for the statement *"I think more about information security in my everyday work after the training"* by training types, and non-training

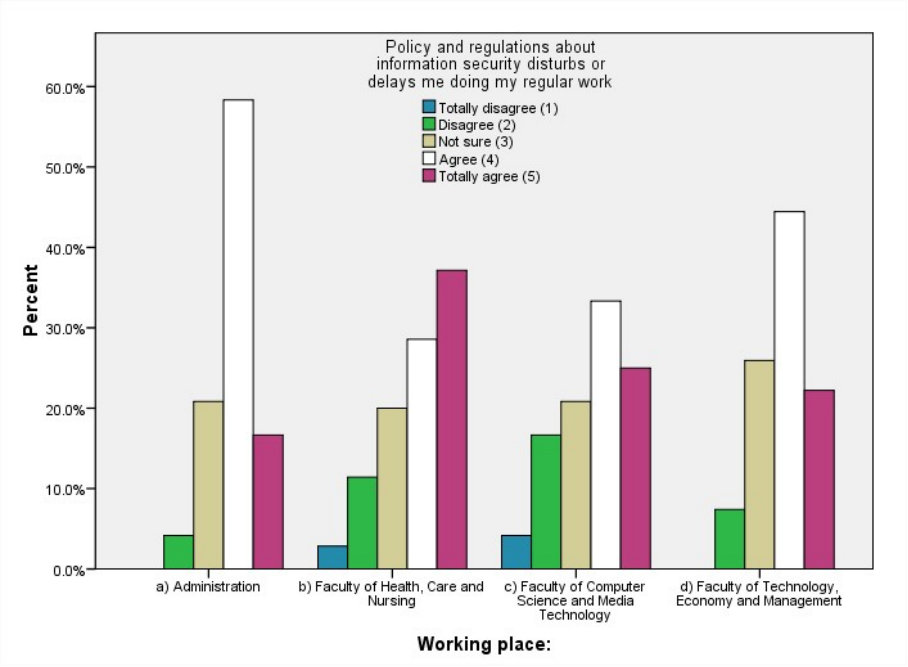

Figure 31: Average of responses for the statement *"Policy and regulation about information security disturbs or delays me doing my regular work"* by department

and also independent sample t-test is used to compare the results between surveys. Therefore, not any significant differences are discovered between surveys, however there is a slightly difference between the mean scores, where the mean of survey number two is lower (3.79), than the mean of survey number one (3.82).The figure 31 illustrates the responses to this statment according to departments.

6.6 The Effectiveness of the Awareness Program

In the section 2.5 is elaborated what is really meant with *"effectiveness"* of the awareness program in this project. On the other hand, during the implementation of the project and analysis of the results, it is discovered the need to redefine and extend the meaning of the *"effective awareness program"*. Even though, it is mentioned that effective awareness program means the program that is capable to influence the knowledge, attitude, and behavior of the participants, and make positive changes in the security culture of an institution, it is discovered that not only this issue makes the *"effective awareness program"* complete. Accordingly, it is discovered the need to analyze more carefully the circumstances, and enumerate the objectives which add/remove values and influence the effectiveness of the awareness program. Therefore, the *"effective awareness program"* means:

Figure 32: The cycle of effective awareness program

1. The program that is capable of influencing (1)the knowledge, (2) the attitude, and (3) the behavior of the participants in a positive way.
2. The program that makes the participants' think more about information security.
3. The program that reaches the highest number of participants.
4. The program that better respond to changes of the threats regarding the information security.
5. The program that has low costs.

The requirements mentioned above and presented in the figure 32 define the effectiveness of the awareness program. If these requirements are fulfilled then it might be concluded that the program is effective. Unfortunately, either one from three types of training, used in our experiment fulfills all of the above requirements. Therefore, each one of the training types will be compared and discussed in further details against these requirements.

The first requirement about the program that is capable of influencing the knowledge, attitude, and behavior of the participants in a positive way is considered the most important among the others, and for that reason all of three training types are compared to this to reflect which one's results are better. If we look back in the previous section 6.6, the results from the statistical analysis showed that (a) Classroom training type is more effective than the others on influencing the knowledge, attitude, and behavior among participants, and make positive changes. Since most of the questions in the survey were asking about the behavior of the participants, give us the right to conclude that classroom training is more effective on influencing the behavior as well.

The second requirement about the program that makes the participants' think more about information security is considered the second most important one. To conclude which one of the training types fulfills this requirement better, we looked back in the figure 30. Since it was difficult to find out from this figure, another ANOVA test is run to compare means between groups.

I think more about information security in my everyday work after the training

Which training group where you in:	Mean	N	Std. Deviation
a) Classroom-training (Eureka 2/3).	2.95	20	1.146
b) Discussion-training (A1 28).	4.33	6	.816
c) Web-based training (e-mail with lessons).	3.39	38	.974
d) None.	2.83	46	.851
Total	3.13	110	1.015

Figure 33: ANOVA test for the statement *"I think more about information security in my everyday work after the training"* by training types, and non-training

The results presented in the figure 33 show that (b) Discussion-based training scored higher than the the others, with the Mean value of 4.33. This resulted to be highly significant value where $p = 0.001$. According to this result it is concluded that (b) Discussion-based training is better than the others in the second requirement.

The third requirement about the program that reaches the highest number of participants is considered important as well, but it is considered difficult to conclude on this matter. Regarding the statistics presented in section 4.5 it resulted again that (b) Discussion-based training was more effective in gathering participants, with the participation of 40.90% calculated from the sent invitations. Since it was low participation among all of the trining types, there are identifyed few issues that are dirctly indicating on this, such as:

- Management visibility and commitment.
  Even though this project was supported form the management, in the invitation to the training was not stated that it is required to participate the training as it should, instead it was said it is recommended to participate the training.
- Pre-program and continuous information and *"marketing"*.
  Even though in the e-mail invitations to the first survey it was stated: *"Thank you for participating in the survey, you will be invited soon to participate in the training"*, somehow this was not enough *"marketing"*, at least not for (c) Web-based training. Many of the participants receiving the web-based training invitations thought of it as *"phishing"* e-mail.

According to these facts presented above, it is considered that it would not be *"fair enough"* to conclude and chose the training type that fulfills this requirement. Thus, we consider all of three training types equal on this requirement.

The fourth requirement about identifying the program that better responds to changes of the threats regarding the information security, is also difficult to be stated and chose one of the best training types. In this case it is necessary to consider some objectives, such as:

(*) Outsourcing or Internal training provider.
(!) Continuous or One time training.

These two objectives are dependent on each other, for instance: if you chose (*) Outsourcing company and (!) One time training, then we believe that (c) Web-based training is better responding to changes of the threats, since it is almost impossible to find the suitable time for every employee; if you chose (!) Continuous and (*) Internal training provider, then (a) Classroom training would be better responding to changes of the threats, since it resulted to be more effective in the first requirement.

The fifth requirement about the program that has low costs is also difficult to predict, since it depends from the previous stated objectives, plus more. Here also need to be considered the type of the organization/institution that want the training, and its location (one or multiple). E.g. if the organization or institution is spread out in different locations the costs would be lower to chose (c) Web-based training. However, it is also difficult to define the type of training with lower costs.

7 Conclusion

In order to conclude about the results found during this thesis project, we focus on giving a short answers to the research questions presented in the section 1.5. In the next paragraphs are presented the questions and observed answers based on the facts found during the whole process of this project.

Is it possible to show that a information security training increases the level of security awareness?
The previous literature, the research strategy and methodology, the research tools used during the entire process, and the experiment done in practice, helped us conclude that information security awareness training is a typical instrument to further improve and influence the knowledge, attitude, and behavior, regarding the information security among the participants, and that the methods used in our case are enough effective. From the analysis of the data resulted a significant differences between the groups of participants that attended the training, and the grouped of participants that did not attend the training. Therefore, it is found that the group of participants that attended the training scored higher, than the group of participants that did not attend the training in all of the selected topics, including: (1) Password protection and management, (2) Sensitive information handling, (3) Social engineering, (4) Physical/Office protection, (5) Incident response - whom to contact. Also, the facts regarding the employee's behavior observed from IT department after the training has been realized, make this conclusion even stronger.

According to statistical analysis in this case study, the awareness program and the methodology used was highly effective. The facts that training participants scored higher (based on mean values) in all of the above training topics, help us conclude on this matter. Also, *"all topics together"* (this index *"all topics together"* consists of all five topics from the above paragraph), which present the awareness in general scored significantly higher with value of $p = 0.009$ (Remind: If $p \leq 0.01$ the observed value is *"highly significant"*). Despite these statistical facts, the confirmations from IT department, that the number of employees asking about suspicious e-mails has been increased after the training has been realized, make this conclusion even stronger.

However, it is found in [58] that besides the above methods, also the enforcement of the policy, rules, and regulations should be improved (if not yet in place then set them up) by using the reinforcement theory, such as reinforcement, punishment, and extinction, in order to add value to information security awareness program, and make changes in the behavior. If the consequences of breaking the rules are extensively understood and known from the employees, then it is believed that the chances of causing incidents from the inside employees will be reduced.

Based on these facts presented above and those found in the literature study, it might be

stated that generally the information security awareness programs have positive influence on the employee's knowledge, attitude, and behavior in real life working environment.

Which type of training is the most effective in achieving higher awareness level?
Many searching tools are used to find out what is discovered until now about the training types. Yet, there is not any scientific research found on regard to this issue, on the other hand many companies providing awareness training argue differently, depending on what training types they offer. There are many requirements identified, which influence the decision of choosing the best training type, and that make it more difficult (see 6.6). However, if considering to choose a program method that best influences the knowledge, attitude, and behavior of the participants, then it is discovered that traditional style of learning, or (a) Classroom training style is better. This conclusion is derived from statistical analysis of the results, which have shown that in the majority of the topics, and in the *"all topics together"*, participants in classroom training scored higher than participants from other training types, except for the topic (3) Social engineering, which was scored higher from participants of the (c) Web-based training.

In the literature it is strongly recommended to have management support, in order to prompt the employees into massive participation, since neither of the training method would work without participants. This recommendation is also confirmed in our case, and it is suggested to not even start thinking of having neither of the awareness training program without prior approval from the management. If chosen to implement (a) Classroom, and (b) Discussion-based training, determination of the suitable time for the majority (if not all) of the employees is highly important. When it comes to the costs, mainly the need is to consider the duration of the training (in case the company deals with production the duration of the training directly affects it), and the geographical distribution of the institution/organization (if the institution is spread in different locations, the web-based training style would be more convenient). (For more detailed information on the last research question please refer to 6.6 and the last paragraph of 8).

8 Future Work

At the beginning of the thesis the idea was to include the question:*Is it possible to measure the half-life of the security awareness program?*, as one of the research questions. The life-long of the awareness program, especially the half-life of the program is the period of time that the effect of security awareness program takes to decrease by half. This finding will help to measure the period of time that is necessary to arrange next program, in order to not let security awareness fall down, after some time. The strategy for answering to this question was to launch the third survey after two to six months, but due to the time limitations of the project this issue was ignored. The plan was to compare and carefully analyze the results of the second and third survey, and discover if any significant difference might be found. The assumption is that participants of the third survey would score lower in the awareness training topics, than the participants from the second survey. This assumption is based on the learning process presented in the section 2.8. It is strongly recommended to further explore this assumption and find an answer to the above question.

Some faults are identified during this project, which are strongly recommended to be improved in the future. One is that in the real life working environment this type of project need management support and commitment. Therefore, it is highly recommended that the invitations to surveys and to awareness training should include *"mandatory"* statement, NOT *"recommended"* as we did in our case. Another fault is that these type of research should not consider having anonymous surveys, in order to follow the progress of the individuals after the training. Advantage of having distinctive surveys is to be more specific in measurements and analysis, whilst this would make the conclusion about effectiveness of the awareness training more powerful. If the anonymity is considered important issue in your case, then one solution to this might be to assign numbers for each individual, and the same number would be used from the same individual during the whole process.

Another fact is known that individuals have different learning styles. According to Randall Shirley [59], in general there are three types of learning: (1) Listening learners, (2) Touch/experience learners, and (3) Seeing learners, which in our case would be equivalent to (a) Classroom training, (b) Discussion group training, and (c) Web-based training, respectively. Typically, there are different people whom are more comfortable in one of these learning style, and can percept better if they chose the method that is best fitted to them. According to this, we believe that if given the opportunity to the employees to chose the training method by themself, the effectiveness of the training would be more powerful and would scored higher, also choosing the most effective training type would be more easier. One solution to this would be to include additional question in the first survey, such as:

Which training type do you like most? (with alternatives)

- Classroom training.
- Discussion group training.
- Web-based training.

Another advantage of including this question would the easier way of grouping the participants into training. To conclude this chapter it is highly recommended to considered all of these issues mentioned above in the future, for such experiments and practical examples.

Bibliography

[1] Ernst&Young. 2010. Outpacing change - ernst&young's 12th annual global information security survey. http://www.ey.com/TW/en/Issues/Managing-risk/Information-security-and-privacy (Last visited 10/05/2011).

[2] Kruger, H. & Kearney, W. 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289 – 296.

[3] Davis, P. 2008. Measuring the effectiveness of information security awareness training - whitepaper sai global. http://www.oceg.org/view/measuring-the-effectiveness-of-information-securit (Last visited on 17/03/2011).

[4] Intelligence, I. June 2007. It's a "sprint" not a "marathon". http://incentive-intelligence.typepad.com/incentive_intelligence/2007/06/its_a_sprint_no.html/ (Last visited on 10/05/2011).

[5] PriceWaterhouseCoopers. 2004. Information security breaches survey (technical report). http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html (Last visited on 17/04/2011).

[6] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. January 2009. The impact of information richness on information security awareness training effectiveness. *Comput. Educ.*, 52, 92–100.

[7] Spitzner, L. october 2010. How to build an effective information security awareness program. http://searchsecurity.techtarget.com/magazineContent/How-to-build-an-effective-information-security-awareness-program (Last visited on 17/04/2011).

[8] Callahan, M. December 2008. The weakest link in protecting corporate data. http://www.prosecurityzone.com (Last visited on 27/04/2011).

[9] M. Wilson, J. H. October 2003. Building an information technology security awareness and training program. *National Institute of Standards and Technology*.

[10] Herold, R. 2005. *Managing an Information Security and Privacy Awareness and Training Program*. Auerbach Publications, Boston, MA, USA.

[11] Stewart, G. 2009. A safety approach to information security communications. *Information Security Technical Report*, 14(4), 197 – 201. Human Factors in Information Security.

[12] NIST. April 1998. Information technology security training requirements: A role- and performance-based model. *National Institute of Standards and Technology (Special Publication 800-16)*.

[13] ISF. April 2002. Effective security awareness (workshop report). *Information Security Forum*.

[14] Everett C. Johnson, (International President, I. & Institute), I. G. February 2006. Security awareness: switch to a better programme.

[15] Herold, R. September 2010. How information security, privacy training, and awareness benefit business. http://www.compliancehelper.com/article/56659-how-information-security-privacy-training-and (Last visited on 10/05/2011).

[16] McIlwraith, A. 2006. *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Gower Publishing Company.

[17] Pahnila, S., Siponen, M., & Mahmood, A. January 2007. Employees' behavior towards is security policy compliance. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 156b.

[18] Williams, A. May 2007. The ineffectiveness of user awareness training. http://techbuddha.wordpress.com/2007/05/02/the-ineffectiveness-of-user-awareness-training/ (Last visited on 03/04/2011).

[19] Sr., T. P. L. June 2005. Information security awareness: The psychology behind the technology. *AuthorHouse*, 1(ISBN-13: 978-1420856323).

[20] Division, I. S. July 2008. Security awareness program - strategic plan recommendation (oregon secretary of state security). www.oregon.gov/DAS/EISPD/ESO/SecPlan/SOS/Awareness.doc (Last visited on 19/04/2011).

[21] PriceWaterhouseCoopers. October 2008. Safeguarding the new currency (findings from the 2008 global state of information security study). http://www.pwc.com/gx/en/information-security-survey/pdf/safeguarding_the_new_currency.pdf (Last visited on 31/05/2011).

[22] Petropoulo, D. September 2006. Iso/iec 27001:2005 a brief introduction. http://www.fvc.com/FVC/FVCWEB/files/ISO27001%20Introduction.pdf (Last visited on 21/05/2011).

[23] Institute), I. G. 2007. It governance using cobit and val it (student book, second edition). http://www.isaca.org/Knowledge-Center/Academia/Documents/Educational(Last visited on 24/04/2011).

[24] ENISA. July 2007. Information security awareness initiatives: Current practice and the measurement of success. http://www.enisa.europa.eu/act/ar/deliverables/2007/kpi-study/en (Last visited on 20/05/2011).

[25] Hinson, G. April 2003. The true value of information security awareness. http://www.noticebored.com/html/why_awareness_.html (Last visited on 14/04/2011).

[26] Survey, E. S. October 2009. Naive nordmenn og skeptiske øst-europeere? http://www.nsd.uib.no/nsd/nsdnytt/doc/nsdnytt_09-2.pdf (Last visited on 18/04/2011).

[27] Tohmatsu, D. T. 2009. Losing ground - 2009 technology, media and telecommunications (tmt) global security survey. http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/266b773b93912210VgnVCM100000ba42f00aRCRD.htm (Last visited on 27/05/2011).

[28] Mathisen, J. Measuring information security awareness - a survey showing the norwegian way to do it. Master's thesis, Gjøvik University College, June 2004.

[29] Sikkerhetsråd, N. September 2010. Mørketallsundersøkelsen 2010 informasjonssikkerhet og datakriminalitet. http://www.nsr-org.no/morketall.htm (Last visited on 28/05/2011).

[30] Hogervorst, M. 2008. Information security training and awareness.

[31] Coporation, S. I. May 2007. Information security awareness report tm. http://www.secureinfo.com/downloads/reports/SecureInfo-InfoSec-Report-Dec-2007.pdf (Last visited 31/05/2011).

[32] Xuemei, L., Yan, L., & Lixing, D. 2009. Study on information security of industry management. In *Information Processing, 2009. APCIP 2009. Asia-Pacific Conference on*, volume 1, 522 –524.

[33] Sveen, F., Rich, E., & Jager, M. 2007. Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers*, 9, 481–492. 10.1007/s10796-007-9052-5.

[34] Gross, J. B. & Rosson, M. B. 2007. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*, CHIMIT '07, New York, NY, USA. ACM.

[35] of Health, U. D. & Human Services), O. f. C. R. February 2006. Hipaa administrative simplification.

[36] of Health, U. D. & Human Services), O. f. C. R. May 2003. Summary of the hipaa privacy rule.

[37] Hanley, P. 2005-2010. Online backup and storage and hipaa compliance. http://datapreserve.com/wp-content/uploads/HIPAA-and-Data-Backup-Storage-DP-20100810.pdf (Last visited on 03/04/2011).

[38] McMillan, R. 2007. Hack this school network, win a router. http://www.infoworld.com/d/security-central/hack-school-network-win-router-039 (Last visited on 16/04/2011).

[39] Kevin D. Mitnick, W. L. S. 2003. *The Art of Deception: Controlling the Human Element of Security*.

[40] Spice, B. October 2007. Carnegie mellon researchers fight phishing attacks with phishing tactics. http://www.cmu.edu/news/archive/2007/October/oct2_phishing.shtml (Last visited on 14/04/2011).

[41] J.Ferhuson, A. October 2005. Fostering e-mail security awareness: The west point carronade. http://net.educause.edu/ir/library/pdf/eqm0517.pdf (Last visited on (05/04/2011).

[42] Lacey, D. May 2009. *Managing the human factor in information security - How to Win Over Staff and Influence Business Managers*.

[43] Schlienger, T. & Teufel, S. September 2003. Analyzing information security culture: increased trust by an appropriate information security culture. In *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, 405 – 409.

[44] Maxwell, J. A. 2005. *Qualitative research design - (An interactive approach) (2nd Edition)*.

[45] Creswell, J. W. July 2002. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (2nd Edition)*.

[46] (IT department), G. U. C. September 2010. Reglment for bruk av høgskolens datautstyr. http://www.hig.no/it_tjenesten/it_reglement (Last visited on 15/05/2011).

[47] System, C. R. 2011. Survey design (chapter from the survey system's tutorial). http://www.surveysystem.com/sdesign.htm (Last visited on 15/02/2011).

[48] Coporation, S. I. May 2007. Noticebored security awareness topics. http://www.noticebored.com/html/topics.html (Last visited on 14/03/2011).

[49] Enalyzer survey solution software. http://www.enalyzer.com/ (Last visited on (31/04/2011).

[50] Inc, S. Spss for windows. http://www.spss.com/spss/ (Last visited on 13/05/2011).

[51] G.Koomey, J. April 2008. *Turning numbers into knowledge - Mastering the art of problem solving (Second edition)*.

[52] Field, A. 2009. *Discovering statistics using SPSS (Third edition)*.

[53] George, D. & Mallery, P. 2010. *SPSS for Windows - Step by step (A simple study guide and reference 17.0 Update - Tenth edition)*.

[54] Paul D. Leedy, J. E. O. 2010. *Practical Research - Planing and design (Ninth edition)*.

[55] Allen, M. June 2006. Social engineering: A means to violate a computer system. http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529 (Last visited on 30/05/2011).

[56] Coffey, D. & Viega, J. 2007. Building an effective application security practice on a shoestring budget. http://www.blackhat.com/html/bh-usa-07/bh-usa-07-speakers.html (Last visited on 22/04/2011).

[57] for Applied Research), E. E. C. 2003. Incident response: Lessons learned from georgia tech, the university of montana, and the university of texas at austin. http://net.educause.edu/ir/library/pdf/ers0305/cs/ecs0307.pdf (Last visited on 28/04/2011).

[58] Barnett, T. Encyclopedia of management. http://www.enotes.com/management-encyclopedia/reinforcement-theory (Last visited 31/05/2011).

[59] Shirley, R. Which one are you? http://www.worldwidelearn.com/education-articles/how-do-you-learn.htm (Last visited 23/05/2011.

Appendix: A - The First Survey

In the following pages we included the survey questions approximately as they are visualized in used online survey software to the respondents. For the simplicity the survey presented here is presented in English language only. We also numbered the questions consecutively as we needed to refer to a few of them in chapter 6.

Q1. Gender

- a. Male
- b. Female

Q2. Your age is:

- a. 18-30
- b. 31-40
- c. 41-50
- d. over 50

Q3. Working place:

- a. Administration
- b. Faculty of Health, Care and Nursing
- c. Faculty of computer science and media technology
- d. Faculty of Technology, Economy and Management

Q4. you are currently employed as:

- a. Part time employee
- b. Full time employee

Please, read the following statements and rate each of them on a 5 point scale. E.g. number '4' indicates that you absolutely agree with the statement. Mark '5' if you are not sure, but try to

make a choice.

Nr	Question Statement	Totally dis-agree (1)	Dis-agree (2)	Not sure (3)	Agree (4)	Totally Agree (5)
Q5	I write down my passwords in a piece of paper near my computer					
Q6	I save my passwords in my cell-phone or memory stick					
Q7	I use passwords that I can easily remember so I don't have to save them					
Q8	I don't have problem to tell my password to IT people if I am asked to					
Q9	Taking a line from a song and using the first initial from each word would be an example of a good password					
Q10	I use at least two different passwords. One is for working purposes, and one for private use					
Q11	I use the same password for different accounts					
Q12	I don't use Password-protected screen saver in my PC at work					
Q13	I don't lock the door of my office during my working hours, even if I am away					
Q14	I open unexpected files or e-mail attachments or files, that I receive form unknowen or known sender					
Q15	I share sensitive information about my work with all my colleagues (such as information about projects, personal information about students, etc.)					
Q16	We regularly talk about how to protect sensitive information with my colleagues					
Q17	Policy and regulations about information security disturbs or delays me doing my regular work					
Q18	Only IT department is responsible for taking care of information security in GUC					
Q19	In case when one of my colleagues is breaching the information security rules and regulations, I pretend that I am not seeing					
Q20	I put my paper documents that contain sensitive information in the recycle bin for paper					
Q21	I don't use shredder for discarding the documents with sensitive information					
Q22	I save sensitive information in memory stick or external hard drive					
Q23	I keep my desk clean from sensitive documents most of the time					
Q24	I write information about my work/research, or students in social networking sites (facebook, twitter, myspace)					

Q25. My password is shorter than 8 characters

- a. Yes it is shorter
- b. It is exactly 8 characters
- c. It is longer than 8 characters.

Q26. What do you think is a good password? (This question requires open answer, and it is optional)

Appendix: B - The Second Survey

In the following pages we included the survey questions approximately as they are visualized in used online survey software to the respondents. For the simplicity the survey presented here is presented in English language only. We also numbered the questions consecutively as we needed to refer to a few of them in chapter 6.

Q1. Gender

- a. Male
- b. Female

Q2. Your age is:

- a. 18-30
- b. 31-40
- c. 41-50
- d. over 50

Q3. Working place:

- a. Administration
- b. Faculty of Health, Care and Nursing
- c. Faculty of computer science and media technology
- d. Faculty of Technology, Economy and Management

Q4. you are currently employed as:

- a. Part time employee
- b. Full time employee

Q5. Which training group were you in:

- a. Classroom-training (Eureka 2/3)
- b. Discussion-training (A 128)
- c. Web-based training (e-mail with lessons)
- d. None.

Q6. Why you did not take part in the training? (optional question)

- a. I did not have time
- b. The date and time didn't suit me
- c. It is not important for my work/job
- d. I do not need training, I'm experienced in the field

Q7. Which of the following best describes the importance of this training for your job: (optional question)

- a. Not particularly useful
- b. Somewhat useful
- c. Very useful
- d. Essential

Please, read the following statements and rate each of them on a 5 point scale. E.g. number '4' indicates that you absolutely agree with the statement. Mark '5' if you are not sure, but try to make a choice.

Nr	Question Statement	Totally dis-agree (1)	Dis-agree (2)	Not sure (3)	Agree (4)	Totally Agree (5)
Q8	I write down my passwords in a piece of paper near my computer					
Q9	I save my passwords in my cell-phone or memory stick					
Q10	I use passwords that I can easily remember so I don't have to save them					
Q11	I don't have problem to tell my password to IT people if I am asked to					
Q12	Taking a line from a song and using the first initial from each word would be an example of a good password					
Q13	I use at least two different passwords. One is for working purposes, and one for private use					
Q14	I use the same password for different accounts					
Q15	I don't use Password-protected screen saver in my PC at work					
Q16	I don't lock the door of my office during my working hours, even if I am away					
Q17	I open unexpected files or e-mail attachments or files, that I receive form unknowen or known sender					
Q18	I share sensitive information about my work with all my colleagues (such as information about projects, personal information about students, etc.)					
Q19	We regularly talk about how to protect sensitive information with my colleagues					
Q20	Policy and regulations about information security disturbs or delays me doing my regular work					
Q21	Only IT department is responsible for taking care of information security in GUC					
Q22	In case when one of my colleagues is breaching the information security rules and regulations, I pretend that I am not seeing					
Q23	I put my paper documents that contain sensitive information in the recycle bin for paper					
Q24	I don't use shredder for discarding the documents with sensitive information					
Q25	I save sensitive information in memory stick or external hard drive					
Q26	I keep my desk clean from sensitive documents most of the time					
Q27	I write information about my work/research, or students in social networking sites (facebook, twitter, myspace)					
Q28	I think more about information security in my everyday work after the training					

Q29. My password is shorter than 8 characters

- a. Yes it is shorter
- b. It is exactly 8 characters
- c. It is longer than 8 characters.

Appendix: C - The Value Recode

This section includes the complete recode values performed before the statistical analysis, see the table below for detailed explanation.

Question Number	Answer Alternative	Regular Value	New Value
Q8			
Q9			
Q11			
Q12			
Q13			
Q14	Totally disagree (1)	(1)	(5)
Q15	Disagree (2)	(2)	(4)
Q16	Not sure (3)	(3)	(3)
Q17	Agree (4)	(4)	(2)
Q18	Totally agree (5)	(5)	(1)
Q21			
Q22			
Q23			
Q24			
Q25			
Q27			
Q29			

Appendix: D - The responses to the statement - *"I don't lock the door of my office during office hours, even if I am away"*

The responses to the statement *"I don't lock the door of my office during office hours, even if I am away"*, presented in the figure 34, are: 8 (or 5.0%) totally disagree, 21 (or 13.2%) disagree, 13 (or 8.2%) not sure, 33 (20.8%) agree, and 84 (or 52%) totally agree. As it is shown here the majority of the responses are form the options totally agree and agree to the statement, which also strongly supports the idea of including "Social Engineering" as a topic during the training process.

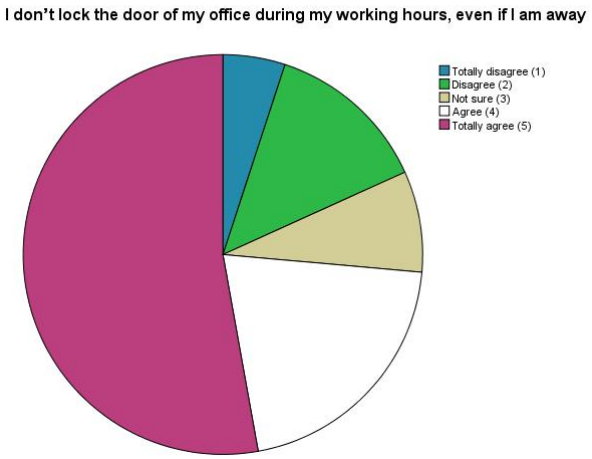

Figure 34: The responses for the statement *"I don't lock the door of my office during office hours, even if I am away"*

Appendix: E - The Training Type Effectiveness

As it is explained in the section 6.6 here below are presented the results for each of the training topics one by one. For each of the topic the Means scores are compared against the three training types, and in the figures below are presented the results for each of them separately. (1) Password Management and Protection is scored higher from participants of (a) Classroom training. (2) Sensitive Information Handling is scored higher from participants of (a) Classroom training also. (3) Social Engineering is scored slightly higher from participants of (c) Web-based training. (4) Physical/Office Protection is scored higher from participants of (b) Discussion-based training. (5) Incident Response - Whom to Contact is scored higher from participants of (a) Classroom training.

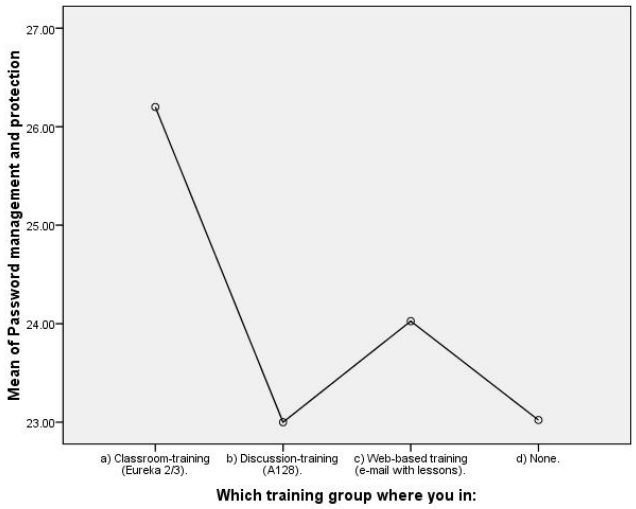

Figure 35: Comparing Means for (1) Password Management and Protection between three training types

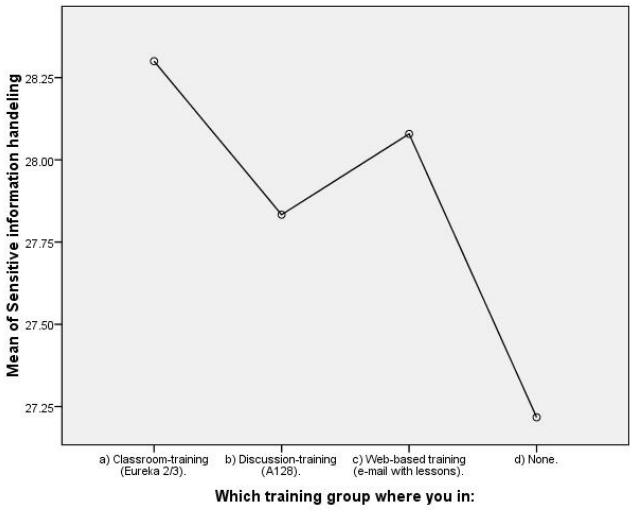

Figure 36: Comparing Means for (2) Sensitive Information Handing between three training types

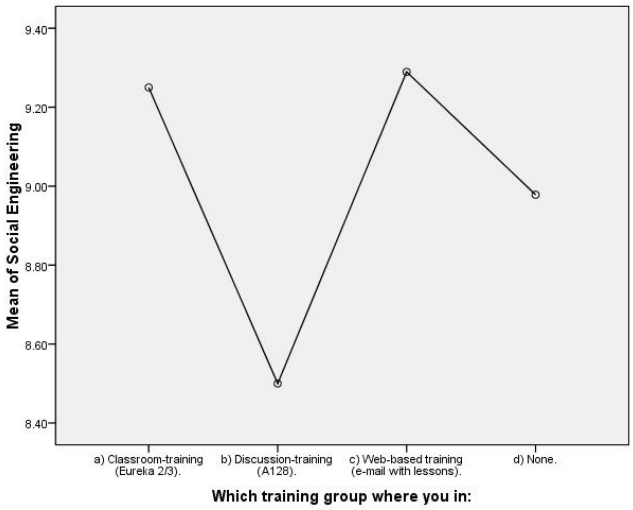

Figure 37: Comparing Means for (3) Social Engineering between three training types

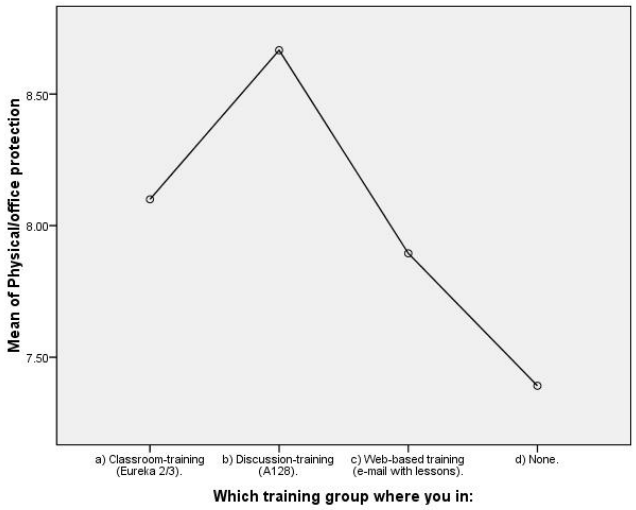

Figure 38: Comparing Means for (4) Physical/Office Protection between three training types

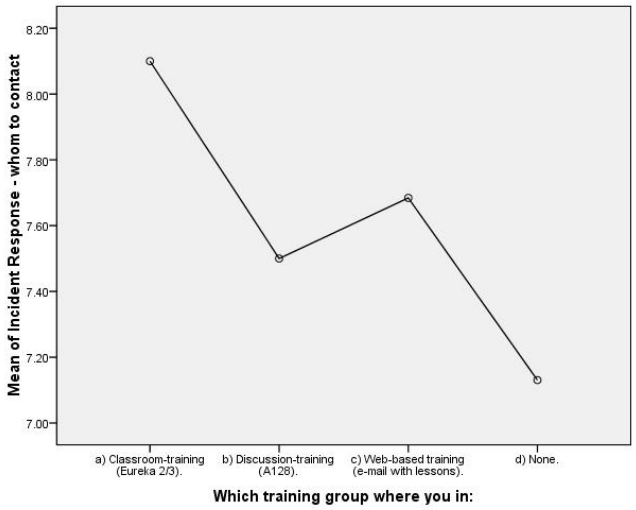

Figure 39: Comparing Means for (5) Incident Response - Whom to Contact between three training types