Implementing and improving awareness in information security

by
Hallvard Kjørvik

Thesis submitted in Partial fulfillment of the
Requirements for the Degree Master of Technology in
Information and Communication Technology

Faculty of Engineering and Science
University of Agder

Grimstad
May 2010

Acknowledgement

This master thesis is submitted in partial fulfilment of the requirements for the degree Master of Science in Information and Communication Technology at the University of Agder, Faculty of Engineering and Science.
I want to thank my supervisor and project supplier, Jose J. Gonzalez, whose help has been invaluable in completing this project. Also I would like to thank the teachers at UiA, that was helpful and gave advise when I needed it.

Grimstad, May 2010.

Hallvard Kjørvik

Contents

List of Figures

1 Introduction

1.1 Background

The users are by many regarded as an important part of the total level of security in an organization e.g. (Wilson and Hash, 2003; Albrechtsen, 2007; Marks and Rezgui, 2009; Da Veiga and Eloff, 2010). The users importance is their knowledge on what and what not to do in a given situation. The problem is that in order to improve this knowledge effectively or only to know the level of it is has to be measured.

The aim of this thesis will then be to compare definitions of security awareness and to determine a good method that can be used to measure security awareness.

1.2 Problem statement

The objectives of this project are:

1. To discuss existing definitions of awareness in information security with emphasis on the feasibility of assessing/ measuring awareness.
2. To compare procedures to measure and/or audit awareness, with emphasis on charting their advantages and disadvantages.
3. If possible, to propose an improved procedure to measure and /or audit awareness.
4. Choosing the best procedure available to carry out a field study.

1.3 Problem solution

The problem solution that was used in this thesis was divided in two parts, one that was mostly theoretical and one mostly practical.

Part one - theoretical

The first part started with a search for literature about the following topics:

1. A definition of security awareness.
2. Methods that could be used to measure security awareness.

After the literature search was finished the discussion on definitions of security awareness was performed, followed by a comparison of different methods for measuring awareness. When the comparison of methods was finished, possible changes to the method was proposed.

Part two - practical

The second part of the thesis was to use the measuring procedure from the previous part to perform a field study. In order to be able to do this some general steps was necessary:

1. A more detailed plan of how to perform the survey was made by analyzing the procedure.
2. Once all required preparations were complete the measuring procedure was completed.
3. Execution of the measuring stage.
4. The resulting survey from the previous step was analyzed in two stages:
   4.1 One where the performance of the study were evaluated.
   4.2 One where the results from the study were evaluated.

1.4 Report outline

The rest of this document follows this structure.
The third chapter starts with describing the methodology that was used in the project and continues with an overview of the theoretical background.

The forth chapter contains the solution to the project, and is divided in three main parts, the first compares and evaluates different definitions of security awareness, the second part evaluates and compares different methods for measuring of security awareness, while the last part test the method developed in the previous one.
The fifth chapter discuss the results of the project while the sixth summarizes the project.

2 Theoretical Background

2.1 Methodology

In order to ensure the efficiency of the process of searching for literature it was put into steps. This would also help to minimize the chance of not finding a relevant document.

2.1.1 Databases used

For the purpose of acquiring relevant information, this project used databases made available by the university.

- **ACM** - http://portal.acm.org/dl.cfm
  Association for Computing Machinery (ACM) is a large online database that contains conference papers magazines and journals.
- **IEEE Xplore** - http://ieeexplore.ieee.org/
  IEEE Xplore is a database that contains conference papers, magazines and journals, mostly from Institute of Electrical and Electronics Engineers (IEEE).
- **ScienceDirect** - http://www.sciencedirect.com/
  ScienceDirect contains journals and books published by Elsevier.

In addition to searching the above mentioned databases, Google scholar was used in order to try to find documents that the search on the different databases missed.

2.1.2 Search method

As was mentioned in the section on Methodology; a procedure that could be used to search for information had to be used.

Limitations

The search for relevant literature concentrated on documents after 2006, but documents published since 2000 where also included in the search.

The justification for the limitation in the search area stated above was that the literature review done by Puhakainen (2006) was determined to be of such a high quality, and therefore not likely to have missed much of importance relating to security awareness.

The extension of the search to 2000 was in case some of the recent literature that could be off interest to this thesis was not included in that from Puhakainen. The limitation was not a fixed rule since articles found that where published before 2000 would be used if they contributed to the result.

Pre-seach analysis

As discussed in the previous paragraph, before the search was performed a study was done of the paper from Puhakainen. The result from that will be listed below.

- A framework and assessment instrument for information security culture (Da Veiga and Eloff, 2010)

Iteration one

The search process started by using the term "security awareness". It was used since the project was about security awareness, so this was a phrase that was determined to be very likely to appear.

Step 1

The first search was done on all the databases use the search words listed above. Subsequent searches will use this in addition to keywords gained from analyzing the results.

Step 2

The Second search was done using Google schoolar with the same search phrase as in step one. This was done since it may be possible to find articles that were not found in the regular searches. This search would only find documents on the databases from ACM and ScienceDirect, since only thise had been indexed by Google.

Step 3

This would inspect the documents found and see if they use interesting documents as reference.

Step 4

This step was to inspect the the documents found and try to find other documents that reference them.
This was possible on ACM and ScienceDirect.

Step 5

Examine the above found documents and see if there were keywords that were common among them.

2.2 Literature search

2.2.1 Search for definitions of security awareness

The first search was done primary for papers discussing the definition of security awareness, but papers containing a method for measuring of security awareness were also listed.

Iteration one

Step 1

The first search was done using the terms *security awareness* in the abstract.
Number of interesting papers: four

- A prototype for assessing information security awareness (method for measuring security awareness). (Kruger and Kearney, 2006)
- Information security management: An information security retrieval and awareness model for industry (Kritzinger and Smith, 2008)
- Health care management and information systems security: awareness, training or education (Katsikas, 2000)
- A comparative study of information security awareness in higher education based on the concept of design theorizing (Marks and Rezgui, 2009)

Step 2

Number of interesting papers: one

- Five Dimensions of Information Security Awareness (Siponen, 2001)

Step 3

Number of interesting papers: none

Step 4

A study of the keywords showed that the words “information security” was common.

Iteration two

Step 1

A new search was performed with “security awareness” in the abstract and “information security” as a keyword. **Number of interesting papers: one**

Step 2

Number of interesting papers: none

Step 3

Number of interesting papers: none

Step 4

No new keywords found.

2.2.2 Search for methods for measuring of security awareness

The search for methods that measured security awareness started with looking at the key terms from the method found in the previous search, "A prototype for assessing information security awareness". Along with the other terms that were found to be relevant. Those terms were "Information security; Quantitative modelling; Knowledge; Attitude; Behaviour". Those terms were tested to see if they provided additional results.

Iteration one

Step 1

The first search was done using "security awareness" in the abstract and "information security" as key terms. in addition to this, and in order to find papers that contained information about how to measure security awareness, the terms "measure" a "measuring" were added as a full text search on the assumption that relevant papers would use those terms in the text.
This search was done twice on all the databases, on time with "measure" and on time with "measuring" in order to see if there were differences. The result showed that this was not the case.

Number of interesting papers: none

Step 2

Number of interesting papers: one

- A framework and assessment instrument for information security culture (Da Veiga and Eloff, 2010)

Step 3

Number of interesting papers: none

Step 4

Number of interesting papers: none

Step 5

No new keywords found.

Iteration two

No additional documents found.

2.2.3 Additional documents

In addition to the search described in the previous section, an additional document was provided by the supervisor

- A design theory for information security awareness (Puhakainen, 2006)

2.2.4 Result

The following criteria were used to provide information about the papers in the next section.

- The sources used
- Author
- Publisher
- Publication date
- Relevance to the thesis.

This information was then used to highlight issues with the paper if that was determined to be necessary.

Results relevant to definition of security awareness

Building an Information Technology Security Awareness and Training Program

This is a standard developed by Wilson and Hash (2003) working for the National Institute of Standards and Technology (NIST) in USA, it is mainly for use in federal agencies, with the purpose of explaining what organization should do in relation to design, develop, implement, and maintain an IT security awareness and training program.

It was written by NIST (National Institute of Standards and Technology) and published in the Special Publications (800 Series), that specialices in information security publications. It does not seem to cite sources other than papers produced by NIST, but those seem to have good references. The publishing date was 2003, and while it is not the most recent work about constructing a security awareness program, the definition it provides of security awareness is still relevant.

A comparative study of information security awareness in higher education based on the concept of design theorizing

Marks and Rezgui (2009) explored the challenges and threats facing the modern universities with an emphasis on the differences between universities in developing countries and developed countries. The study was done on three universities; one in UK, on in USA and one in United Arab Emirates (UAE). In the UK and UAE it was done by interviews, questionnaires,

documentation, and observations. At the university in USA information from an earlier survey was used.
The findings from the study were that the threat that the universities face was mostly the same. But that the difference was the causes and reasons for those threats, and how they are perceived. They also proposed a method for how to improve security awareness by the use of Sequential Design Theory based on the work by Puhakainen.

The authors was Adam Marks from Embry-Riddle Aeronautical University; USA, and Yacine Rezgui from Cardiff University; UK. While both have written several papers, several of the papers that they have contributed on in the past have been on other topics than security awareness. The paper was published in International Conference on Management and Service Science. In the paper Marks and Rezgui uses their list of sources extensively to support their statments. This document was of interest to the thesis because of its discussion off a definition off security awareness.

Information security management: An information security retrieval and awareness model for industry

The study by Kritzinger and Smith (2008) presented a conceptual view of a method for Information Security Retrieval and Awareness (ISRA). The model focused on the non-technical parts of security since, as they argue, those have in comparison with the technical parts always been neglected. The result was a model divided in three parts. The first part was the ISRA dimensions; a description on how to store information in such a way so that it would be possible to retrieve it based on different security levels and the needed information. The second part of the ISRA model focused on the actual retrieval of information as mentioned in the first part. The last part of the model, measuring and monitoring, focused on the measuring of the level of awareness in the organization.

The authors were Elmarie Kritzinger and Elm Smith, both from the University of South Africa where both have contributed to several papers within the field of computer science. The paper was published in the journal "Computers & Security" by Elsevier. An extensive list of sources are provided that are used to suport their argument. Kritzinger and Smith provided a discussion on the subject of measuring security awareness and in addition to this they gave a definition of security awareness.

Health care management and information systems security: awareness, training or education?

In this paper, Katsikas (2000) discusses a methodology for determining the training needs for health care personnel and the question of how much managers at health care institutions needed to be told in regard to the security of information systems. He answered this by first discussing training as three levels; awareness, training and education. He then discussed the European system for training of health care personnel that were then compared against the result of his discussion of the characteristics of the target group.

His conclusion was that managers needed to be at the level of training. And also that the European system for training of health care personnel would benefit with some improvements.

The author of this paper was Sokratis K. Katsikas have have written several papers on the topic of computer science. This paper was published in "International Journal of Medical Informatics" by Elsevier. In the paper Katsikas uses only a limited number of sources. This and the fact that the paper was published in 2000 was offset by the fact that the interest in the paper was its definition of security awareness.

Five Dimensions of Information Security Awareness

In this paper, Siponen (2001), set a as a goal to outline the various dimensions of security awareness, and then outline some key issues around them. The result from this was the following five dimensions: organizational, general public, sociopolitical, computer ethical and finally the institutional education dimension,. In addition, the target groups in each category were determined along with the danger of disclosing information to the members of the different groups.

The author were MikkoT. Siponen who has written several papers within the field of computer security. The paper was published in "Computer and Security" that is a special interest group from ACM. Siponen has an list of references that he uses extensively in the paper. While the date of publishing was 2001, it were still of use for this thesis since the main interest in it was its definition of security awareness.

Results relevant to method for measuring of security awareness

A prototype for assessing information security awareness

A project by Kruger and Kearney (2006) had as a goal to develop a prototype for how to measure security awareness. The resulting method was developed for use in an international mining company that because of this operated in many regions. This ensured that the method developed was adaptable and easy to use in different locations. This was done by giving all the questions a weighting so that its importance could be changed according to the regions need. In order to fulfil the requirements, as mentioned in the article, the procedure identifies 3 main categories to measure: "knowledge (what you know), attitude (what you think) and behaviour (what you do)".

The authors of the paper was H.A. Kruger; North-West University South Africa, and W.D. Kearney that works with IT security. The paper was published in "Computers & Security" in 2006. They make good use of their list of sources, and explains where more information about certain topics can be found. The importance of this paper was the fact that it was the only method found that describeed in detail a method for measuring of security awareness.

Information security culture

This paper published by Martins and Eloff (2002) had as an aim to use an assessment approach to improve information security culture. They started the paper by defining organizational culture and then using this definition to define information security culture.

The method that they used in order to assess the security culture, was to first identify the different organizational levels, and then making questions from nine issues that were identified

as important at all the organizational levels.

Those questions were designed so that they attitudes and perceptions of the employees regarding the issues were identified.

This method was then used to test the security culture in an organization. The results from this test were that the method developed could be used to measure security culture especially, and as a tool in order to improve the security culture in an organization.

The author of the paper was A. Martins and Jan, H. P. Eloff, both from Rand Afrikaans University South Africa. Eloff have written several papers on the topic of information security, while no additional documents where found from Martins. The paper was published in "IFIP International Conference on Information Security", and has a list of sources that are extensively used throughout the paper. The paper was published in 2001, and was of interest since it describe a method that can be used to measure security awareness. While the article appears to be well written, it was not published on some of the databases primarily used in this thesis.

A design theory for information security awareness

A doctorate study from 2006; "A design theory for information security awareness" gave two results. The first was a comprehensive review over the then existing literature in the field. The second was the understanding that existing methods did not provide evidence of their effectiveness, and three theories for how to improve security awareness:

1. IS security awareness training.
   This theory attempt to improve users IS security behaviour towards compliance with IS security policies and instructions.
2. IS security awareness campaigns.
   Tries to achieve organization wide changes in users security behaviour.
3. Punishment and reward.
   The use of reward and punishment as a means to improve users IS security behaviour.

Security awareness training was tested in practise, but while the conclusion was that more research was needed, the results indicated that the theory was relevant for designing practical training. Another observation from the test was that how the users complied to the rules were not only dependent on level of knowledge or skills, but also on motivation.

The author of the thesis was Petri Puhakainen from the University of Oulu, Finnland.

Puhakainen uses a large list of sources in his work. The thesis was published in 2006, and as such is relatively new. The work was interesting mainly since it was a thorough work on the subject of security awareness, and therefore could be used as a starting point for the thesis.

3 Solution

3.1 Comparison of definitions of security awareness

According to Hansche (2001), current approaches to security awareness can be divided in two categories, one where security awareness is seen as a method to attract users attention to security awareness and a second category where the meaning is the users understanding of security awareness. As this projects goal was a method for measuring of security awareness, it was the second interpretation mentioned above that would be explored.
In order to achieve this, it was important to have a set of criteria that could be used while discussing existing definitions.

The important aspects of the definition were that it should give a clear explanation of what security awareness is, and do so in terms that were easily understandable. Another important aspect was the feasibility of measuring security awareness. In addition to this the description of security awareness should not be so that it only fits a special kind of organization. And because of the users importance in security (Wilson and Hash, 2003; Albrechtsen, 2007; Da Veiga and Eloff, 2010), the definition should specifically mention the users and their role in it.

3.1.1 The feasibility of measuring awareness

The feasibility of measuring security awareness can be discussed using the definition off security awareness from chapter 3.1; *Comparison of definitions of security awareness*. As described in the chapter, the definition views security awareness as a concept and the users understanding off it.

Possible methods to acquire this information can be to define relevant topics within the subject of security awareness, and then make questions for the users to answer within those topics.
The result from those questions can then be used to determine the level of awareness, either by comparing several measurements, or by comparing the result to a predefined scale.

3.1.2 Comparison of definitions

The comparison was done mainly by the wording, but also by trying to understand the greater concept of the paper. But if the paper did not provide a proper discussion, it was the wording of the definition that was used. One of the problems with this are that the meaning applied to the definition by this paper may not be the same as the one to the original author.

The exception to the section above was the subject of the possibility of measuring awareness. The reason for this was that following the argument given in section 3, security awareness can be defined as two types, a level of understanding and as a method. An example can be passwords. While the method seek to educate the users in how to handle passwords and the concept is concerned with the level of knowledge that users have, both can be measured. Training can be measured by doing it before and after it has taken place, while the current level of understanding can be found by measuring.

In his paper Katsikas (2000), uses this definition of security awareness:

> *awareness activities aim merely at attracting the attention of individuals to the subject, in our case security, and at allowing them to recognize the concern for information systems security and to respond accordingly.*

While it was clear from the paper that Katsikas view awareness as a concept, the wording may make the definition understood as if it was a method. If viewed as a method it gives a clear description of security awareness that can be used in general and that specify the users importance.

Siponen (2001) share the view that security awareness can be viewed as a method:

> *The concept of information security awareness is taken in the literature to mean that users should he made aware of security objectives (and further committed to them).*

The quotation shows that in this document, Siponen agrees with the definition that security awareness is a method for training users in secure behaviour. As in the example above it gives a clear description of security awareness as a method while stating the users role.

Marks and Rezgui (2009) adopt the view that security awareness is a method:

> *users should be made aware of IS security objectives and consequently committed to them*

This definition, as with the two mentioned above, is more concerned with security awareness as a method to educate users in the concept of security awareness in an organization.

The document from Wilson and Hash (2003) view security awareness as a concept:

> *Awareness is not training. The purposes of awareness presentations are simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.*

This definition of security awareness is specific about its intent and mentions the key principles that this project is interested in. Other papers agree with the above mentioned definition, among them Wasim (2006).

A somewhat better worded definition was a summary of security awareness given by Kritzinger and Smith (2008) as shown below:

> *Information security awareness is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with.*

This definition agrees with the one from NIST in that security awareness should be viewed as the users understanding of security awareness, while as mentioned being better written.

While the definition from Fergle et al. (2009) agreed that awareness was not training,

> *the state where subjects are capable to perceive information security elements such as segregation of duties, non-repudiation, and authorization in their environment leading to a better understanding and prediction of security conditions*

the examples it uses is technical and it can't be assumed that everyone will understand them without an explanation.

3.1.3 Result

The definitions that were best according to the criteria mentioned in chapter 3.1, was the one from Kritzinger and Smith and Wilson and Hash, both gave a good description of what security awareness is, but the one from Kritzinger and Smith was worded better.

> *Information security awareness is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with.*

3.2 Comparison of methods for measuring of security awareness

3.2.1 Comparison of methods

Only two methods were found that described how to measure security awareness; the prototype developed by Kruger and Kearney (2006), and one that was used to assess information security culture by Martins and Eloff (2002).

Information security culture

Describtion

The paper describes a method that can used to assess the security culture in an organization.

The first step was to identify three levels in the organization that each contained one or more issues that were determined to be important:

- **Organizational**
  - Policy
  - Benchmarking
  - Risk analysis
  - Budget
- **Group**
  - Management
  - Trust
- **Individual**
  - Awareness
  - Ethical
  - Change

A questionnaire should then be developed that fitted within the categories mentioned above, it would then be used to assess the attitudes and perceptions of the employees.

Comments

As a method to be used for measuring of security awareness, it lacked details on how to evaluate the result, and it also focused on different categories that was mostly of a non-technical type.

A prototype for assessing information security awareness

Description

The paper gives a description of the process that they used in order to develop the test, and some of the challenges that they had. It starts with a description of the task that led to the development of the test. This task was that an international mining company that wanted to measure the result of a security awareness program.

The first task was how to arrive at a measurement of the awareness level in the company. It was decided that this should be achieved by measuring each division, and then combine the different measurement in a global number.

It was decided to measure three aspects: “knowledge (what you know), attitude (what you think) and behaviour (what you do)”. Here they give a brief reason for selecting it and some sources if more theory was desired. They also identified the challenge of developing the measuring tool; what to measure and how to do it, and how to perform the measurement. Those aspects were then divided into the six focus areas from the existing security awareness program. And then further broken down into several factors and sub-factors if necessary. The example that they used was passwords. That was divided into the Purpose of passwords and Confidentiality of passwords. Confidentiality of passwords was divided into the areas Writing down of passwords and Giving passwords to others.

A problem was that not all the aspects had an equal importance in each division. This was solved through the use of a weighting system that gave each part an number that enabled the differentiation of importance based on the requirements of the current location.

The second task; how to measure, was solved by solving the values generated by the different questions in a bottom-up procedure. This can be seen on figure 1 below, where each answer alternative have a different point value. The points for each question were added to the total for each aspect. That again where added together to the value for the different focus area, backup in the example, and finally each focus area where combined to make a total number that represented the level of security awareness.

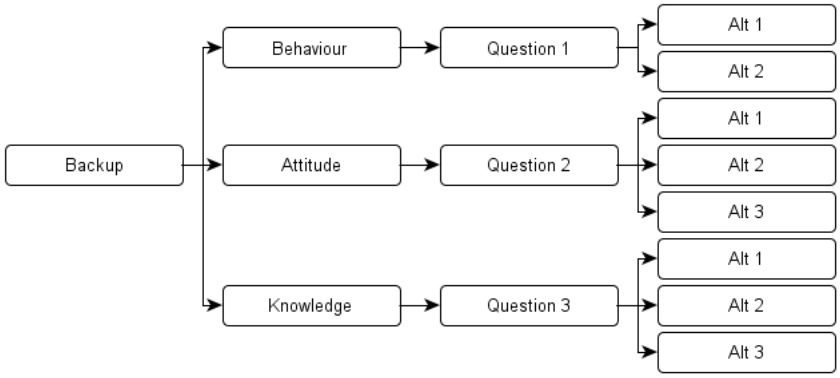

Figure 1: Example on how to evaluate

Comments

As stated by Kruger and Kearney, one advantage of this method was that it gave a output on all the different levels so that it was easy to see the details and while it at the same time was possible to see the end result.

Also the way the method was described so it should not be a problem to adapt it to different organizations that have different priorities when it comes to what is important in security awareness.

They state that some of the questions were made so that they tested more that one aspect, more information regarding this would be preferable. Also, it was not mentioned how those

questions influence the final result, but one assumption can be that they influence the different aspects equally.

3.2.2 Best method found/made

Of the two methods that were found, the method from Kruger and Kearney (2006) was chosen as basis for the survey since it was the one that described the process of measuring and evaluating security awareness in any detail.

3.2.3 Proposed improvments

The proposed improvements that will be made are mainly the aspects commented on in chapter 3.2.1; subchapter Comments.

Evaluating questions that testing more that one aspect.

In the paper, Kruger and Kearney states that some questions were used to measure more than one aspect. But how those questions were evaluated was not made clear. A proposed method to evaluate those questions are to treat each instance as a separate question for the purpose of the calculation of the result.

3.3 Method for measuring awareness

As stated in chapter 1.2, goal three was to develop a method that could be used to measure security awareness.

This survey may not fit perfectly in any kind of organization, be it a special kind of organization; like a school, or a be restricted to certain prerequisites; an example being that the organization have to follow a special awareness plan, since it was not made specifically for any kind kind of setup.

But by using the methods that will be described, and possibly using the existing survey as a basis, it should be possible to make a survey that can be used in a specific environment.

The work on the method was divided in four stages and in the following order:

- Construction of a test version of the survey and a method for calculating of the result.
- Work on the theory required for the main survey.
- Construction of the final survey and calculating method.
- The testing and evaluating of the survey.

The reason for the order to the tasks is that before starting the master, a project about security awareness was conducted, and a part of that was two interviews about the measuring of security awareness. And since this made it possible, it was decided to divide the theory part of the master project in two.

3.3.1 Preliminary study on measuring awareness

Following Kruger and Kearney (2006), the work process used in order to develop this survey was based on the following four questions: *what to measure, Why measure it?, How to measure it?* and finally *How to evaluate the result.*

What to measure and why

Gathering of info

The basis for the preliminary survey was the work by Kruger and Kearney, and two interviews conducted earlier on this topic where the following was mentioned as important to include in a survey:

- The survey should make it clear if the users knew and understood the rules. It should also discover the understanding people had about their importance in the organization. Additionally, information about were the users learned what they can about security should be made clear.
- Passwords, and how the users felt about them should be made clear, and also how they were handled. Also the knowledge if the user makes hard passwords, and also if they had different passwords for different places.
- The survey should include questions about physical security. Printouts can also be placed in this category, how the users treat them, if they are forgotten at the printer, if they are thrown without thinking about what they contain.

- Data stored on portable devices, the meaning with this was how the users treated data. Were they conscious about the risks involved in storing data on laptops or on memory sticks?

In addition to the above mentioned results from the interviews, it became apparent that the survey should contain questions regarding the use of Internet.

Choosing categories and questions

Kruger and Kearney start by selecting the main categories for use in the survey and for this the following were chosen:

- **General security** contained questions that did not fit in the other categories.
- **Internet** covered questions related to the direct use of the Internet.
- **Backup** was about questions related to the performing of backup.
- **Physical security** covered topics about the physical side of information security.
- **Password** covered the handling and understanding of passwords.

Each of the above mentioned themes were then divided into the three categories knowledge, attitude and behaviour. This was different from the work by Kruger and Kearney and followed the argument from chapter 3.2.1.

Questions were then developed to fit in the different categories. An example of the questions developed can be seen in figure 2 It should be noted that since this was a preliminary survey, not all of the categories where covered sufficiently. The completed questionary can be found in appendix A.

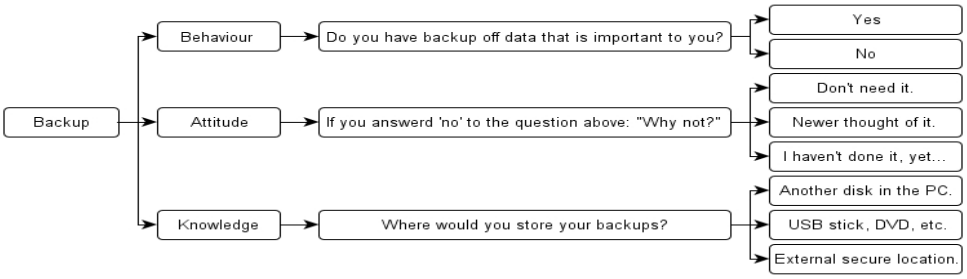

Figure 2: Questions from backup

How to measure it?

It was decided that the measuring should be done by the use of a multiple choice questionnaire. The reasons for this was that it was relatively quick to complete, and that it was easy evaluate, provided that a method for doing so was established. The drawback to the use of multiple choice was, as mentioned by Kruger and Kearney (2006), that not everybody answers honestly. But since the test was anonymous, the expectation was that most people would answer honestly.

Evaluation of the result.

The result was analyzed in two stages: one where the survey in itself was evaluated, mostly based on the feedback given by the students participating in the survey. The second stage was the development of a simple method for evaluating the actual result.

Evaluation of the survey

As stated above the evaluation was done mostly by the comments from the students participating in the survey, but also by a new understanding of the questions.

The performance of the survey

The actual performing of the survey did not result in special difficulties, except in the cases where some students didn't fully understand the questions, this will be discussed further in the next section.

The survey took approximately seven to eight minutes to complete, and was therefore close to the estimated time of around ten minutes.

The questions

1. *General security*
   - 1.1 *Do you update your computer regularly?*
     This question can be rephrased to ask if the user know it the computer he/she is using is updated regularly.
   - 1.2 *Assuming one of your computers is not important for you in any way, should you care if it gets infected by a virus?*
     A possible alteration is
   - 1.3 *In your regular computer use, are you then using an account that has full access to you computer? This is an account that has more rights than a normal user, usually an administrator account.*
   - 1.4 *Would you consider using a program to ensure that your computer and the programs that are installed on it is up to date?*
2. Internet
   - 2.1 *When you get to a web page that you dont know, and it asks you if you want to run a script on the page, do you answer yes ?*
   - 2.2 *Do you, or have you, placed information on the Internet that tells when you will leave for a vacation?*
   - 2.3 *Are you conscious about what private information you share on the Internet?*
     The wording should be changed so that the question is more clear about the fact that all information placed on the Internet can be used against you.
   - 2.4 *Do you use Facebook?*
   - 2.5 *If you answered yes to the question above, did you know that, while a picture exists on Facebook, that you grant Facebook a licence for it?*
     The intention of the question was to determine if the users knew what they signed. This question may have to be reworded.

3. Backup
   - 3.1 *Do you have backup off data that is important for you?*
     The question can be reworded to ask if the user know if data is backed up.
   - 3.2 *If you answered no to the question above; Why not?*
     It is possible to make the question so that it answers the question of why the user don't know.
   - 3.3 *Were would you store your backups?*
     The question should have specified how many answers that could be marked. Also it may not be that relevant
4. Physical security
   This section would benefit from having more questions. The existing questions are
   - 4.1 *Have you left your computer in an unlocked room?*
   - 4.2 *Do you lock the computer when you leave it?*
5. Password
   - 5.1 *Are you conscious about your use of passwords? That is, do you distinguish between critical and non-critical use?*
     There were comments from some of the students participating in the survey that the wording made this question unclear.
   - 5.2 *Is your computer password protected?*
   - 5.3 *Passwords and were they are used, can be written down and stored at a secure location.*
   - 5.4 *Passwords should only be remembered.*
   - 5.5 *Passwords can be written down, but it should not be possible to guess were they are supposed to be used.*
   - 5.6 *One of your friends cant access Fronter to get some files, and you cant send them to her. Is it OK do lend her your password?*
     The question should have the possibility to select "I know that it is bad security behaviour, but I would have done it."
   - 5.7 *How strong do you consider the following password?*
     Kyfdsh2gv
   - 5.8 *How strong do you consider the following password?*
     #Oyhfpyggyope
   - 5.9 *How strong do you consider the following password?*
     Mvdyqp_amrf

calculation of result

The result was calculated by following this procedure:

1. The options to each questions where assigned a value between one and five, based on how correct the alternative was determined to be.
2. The total sum for each option was then calculated.
3. The combined sum for each option was then added together and used as a score for each question.
4. The sum for each question was then used to calculate the score for each category.

5. The value for each category was added together to make a total score.

In order to make it possible to differentiate between the categories. A modifier was inserted into the model. This was done on each question and on each category.

Conclusion

This preliminary survey made clear that there are several mistakes that are easy to make while constructing a survey, and also that it is some aspects of it that need to be addressed before the main survey can be constructed with a possibility that it will be a success.

The number of questions in each category should ideally be the same since otherwise, one category can have a bigger impact on the final score than its importance would warrant. But this may be countered by the use of importance weightings.

The survey should be tested by a third-party before the main survey. This so as to discover questions that are difficult to understand the meaning of, or where; as happened with in this instance, the number of legal options on some answers.

The category "General security", is not ideal on the basis that it is not precise. So while it is useful for questions that don't fit into the other categories, it is difficult to use for evaluating purposes without looking at the specific questions, thereby defeating the purpose of having a category.

In addition to the comments mentioned above some more questions may be relevant:

- Questions regarding the use of laptops:
- Where to use them.
- Where not to use them.
  - How users treat unsafe locations. Would they access the company mail from a Internet cafe?

Method for measuring awareness

The developing of the main survey had the benefit of experience from the preliminary survey along with a better understanding of the literature and what to include in the survey.

3.3.2 What to measure and why

The main survey was performed at the school, and the the target group was the students, so the development of the categories described here and the questions described later in the chapter, had to reflect this.

Choosing categories

The development of the categories to be included in the main survey started by using the same argumentation as for the preliminary survey. In addition to the preliminary survey, discussions with security teachers at the University where performed in order to try to discover new categories or questions that should be included. The result from those discussions were new questions and a new category; "E-mail". In addition, using the argumentation from chapter 3.3.1 Conclusion, the category "General security" was redefined to "General computer security". This reflects the questions that it contains better while being more precise.

- **General computer security**
  This category contains questions regarding the general use of a computer. Two examples can be the frequency of updates if the computer is password protected. The category was included since the safe usage of computers is important within IT security.
- **E-mail usage**
  This category covers questions about the safe usage of E-mail. It was included since it is an important part of the complete security picture in that much communication is perfomed using it, and the fact that it is often used to spread malicious software and spam.
- **Use of Internet**
  Questions about the use of Internet included questions about safe use of Internet both in terms of behaviour and knowledge. The importance is the fact that the use of Internet is a common activity for many students.
- **Backup**
  Backup was included since it is important that the students work is not easily lost. The questions developed tried to reflect this by asking about who it is that have the responsibility for the existence of backup, but also if they actually perform backup of work that is not done at the school.
- **Physical security**
  Physical security was included as a topic since many of the students handle data either since they have portable computers or another portable storage device. Examples of questions developed is if the students are likely to leave the computer (or another device) unguarded. In addition to the treatment of equipment, the handling of data in the form of printouts was also in this category.

- **Password**
  The last category covered the use of passwords, how they are stored and the how they are made. It was included as a category since the use of password is important when it comes to security. The importance derives from the fact that it is the method that is used most frequently when it comes to access control, either alone or together with another device.

Development of questions

The construction of the questionnaire followed the guidelines on the development of a multiple choice survey from Svartdal (2009).
In this part Svartdal explains among other things how a multiple choice questionnaire should be made, how to word the questions and the sequence of the questions.

From it the following was used in the development of the questions:

1. *The sequence of the questions is important.*
   Svartdal mentions that interesting questions should come first in the survey, since this has been proven to increase the number of responses. In this case it means that the questions not related to security awareness should come last.
2. *The wording of the questions*
   Svartdal starts this part by stating that the questionnaire should as easily understood as possible, and then goes on to create a list of aspects that is important:
   - 2.1 The question should be as specific as possible.
   - 2.2 The wording of the question should not be ambiguous or unclear.
   - 2.3 The use of loaded language should be avoided. This means that the wording should not try to appeal to the emotion off the one answering the questions.
   - 2.4 Hypothetical questions should be so that the premise is not to far fetched.
   - 2.5 Leading questions should be avoided.
   - 2.6 The wording of the questions should be neutral in the sense that the creator's views should not be possible to spot in the questions.
   - 2.7 Svartdal mentions that people often wish to appear positive, also in a survey where they can be anonymous. So question that could imply negative social answers may not get a correct answer. The example he gave was the question: "How much did you give to organization X". The understanding was that for this survey, questions that ask about behaviour that was wrong, or illegal should be minimized.
3. *The construction of the answers*
   Svartdal mentioned that the answers, can be either open or close-ended. The obvious difference is that the open-ended questions demands that the respondent must answer the question in their own words, while the close-ended questions have fixed answers.
   The advantage with open-ended questions is that they allow the respondent to express what he or she thinks about a subject. The disadvantage is that it takes longer both to answer such questions and for the questioner to evaluate them. Close-ended questions, given that they are designed so that they cover the aspects expected by the respondents, are both faster to answer and easier to evaluate.
   Following the above discussion this questionnaire will only have close-ended questions.

4. *sources of errors*
   Svartdal also mentions some common sources of errors:
   4.1 One was that some people have a habit of always agreeing (or disagreeing) with the question at hand. This he explained can be eliminated by designing some the questions such that if the respondent always agrees with the questions, he contradicts himself.
   In order to try to guard against this, the answers from question 14 and 19 will be used to try to find those that "always" agrees or disagrees.
   4.2 Another possible source of error is that some people have a tendency to answer questions the way they think they should to it rather than answering what they actually mean.
   4.3 In addition to the two previous points, the discussion about the wording of the question, found above, can be a source of error in itself since if the user as an example misunderstand the question then the result will be wrong.

Testing of the survey

Before the survey was made available for the students, a few were selected to participate in a pre-study in order to test the survey. Those students were selected so that they were of varying degree of computer experience. This was done in order to try to discover questions that where designed so that they relied to much on technical knowledge in order to be answered.

Description and reasons for questions

- Passwords
  1. **Question:** How would you consider the following password? *Oyhfpyggyope*
     This question tried do discover the users understanding, and therefore ability to recognize a good question.
     – **Possible answer:** Very strong, strong, OK, Weak, Very weak
       This password was considered strong since it had a mix of length, special characters, upper and lower letters.
  2. **Question:** How would you consider the following password? *Mv1dyqp_amrf*
     The argumentation was the same as the previous question.
     – **Possible answer:** Very strong, strong, OK, Weak, Very weak
       This password could be considered very strong since it had a mix of length, special characters, upper and lower letters and numbers.
  3. **Question:** How would you consider the following password? *Kyfdsh2gv*
     The argumentation was the same as the previous two questions.
     – **Possible answer:** Very strong, strong, OK, Weak, Very weak
       This password could be considered "OK" since it only had a mix of upper and lower letters and numbers.
  4. **Question:** Are you conscious about your use of passwords, that is, do you distinguish between critical and non-critical use? An example is if you use the same password for your mail and you net bank.
     This question was important since some places is critical, so that the password used

in one place should not be used other places. The reason is that if a third party gains access to the password on one of places, access should not be possible to the other place.
In addition, the E-mail should have a password that is used anywhere else, since the E-mail can often be used to reset the password to other places, making it important to keep it confidential.
  - **Possible answer:**Yes, No
    The alternative that identifies good behaviour was "yes".

5. **Question:** How often should a password be changed? This question tried to discover people's attitude towards how often they think a password should be changed. This is important in that people should not be required to change passwords to often, since this can more easily lead to unwanted behaviour e.g. like writing the password on a note that is stuck to the computer monitor or something similar. In addition, a password should be changed n a regular basis.
  - **Possible answer:**After: 1 month, 3 months, 6 months, 12 months.
    The most realistic answers here is 6 or 12 months. Since, as argued above, anything less may be considered counterproductive in terms of security.
6. **Question:** Are your computer password protected? One of the important, and one of the easiest, method of securing a computer is to use a password to protect it.
  - **Possible answer:**Yes, No, Don't know
    The best answer here is yes, while the worst might be considered "Don't know" since such an answer demonstrates that the user is unaware of the current state, compared to the answer "No" where he at least demonstrates knowledge, even if the answer shows a weakness in security.
7. **Question:** Passwords can be written down, but it should not be possible to guess where they are supposed to be used. This and the next two questions tried to discover what the users thought were acceptable places and circumstances to store passwords. Viewed together they should be able to give an indication off the users attitude about it, that again could be used as an indication on what they were most likely to do.
  - **Possible answer:**Strongly agree, Agree, disagree, strongly disagree
    Because of how the question was asked, the answer that can be considered best may be "disagree". The reason is that a password that one don't know where should be used (this argumentation depends on the knowledge that the combination found is a password), it can simply be a trial and error to see if it fits some public places.
8. **Question:** Passwords should only be remembered. The argumentation was the same as the previous question.
  - **Possible answer:**Strongly agree, Agree, disagree, strongly disagree
    This may be considered one of the best locations to store a password, since it cannot be stolen. The problem is if there are many passwords, then it may be easy to forget one, or to mix two passwords. In light of this the answer that may be considered the best was determined to be "agree".
9. **Question:** Passwords and where they are used can be written down and stored at a

secure location.
The argumentation was the same as the previous two questions.
- **Possible answer:**Strongly agree, Agree, disagree, strongly disagree
  This is best done by the use of dedicated programs that can store the passwords in a secure way. This makes it possible to have many different passwords that are difficult to guess. The downside is that if the password to the program is forgotten, all the passwords are lost. So the best answer here was determined to be "agree".

10. **Question:** *Consider this scenario: One of your friends has forgotten her password and can't access Fronter to get some files, and you can't send the files to her. Would you have lent her your password?*
    This question sought to establish if the users were likely to, under right circumstances, disclose the password to somebody they knew. While a password should newer be given to anybody, some cases are better than others, an example is if the person are known, and it is possible to guarantee 100% that it is the correct person. While it is a better scenario, it is still a violation of the rules.
    - **Possible answer:**Yes, No
      The correct answer here should be "No" since one can newer be 100% sure that it actually is somebody you now that you are talking to if you can't see them.

- **Use of Internet**

11. **Question:** *Do you know your browsers current security level?*
    Together with question 12 this question aimed at giving an indication of the users knowledge about how to use Internet in a secure manner. And since it is easier to get malicious software while using a browser that is not configured properly, compared to one that has the correct security settings, knowing how strong they are indicates that the user have knowledge about, and are interested in, the security of the browser.
    - **Possible answer:** Yes, No, Don't know.
      The best answer will be yes, while the worst will be "Don't know", this since the last alternative demonstrates a lack of knowledge.
12. **Question:** Consider this statement: You cannot get a virus if you only visit a web page.
    Here an answer was given to the question if the users are aware of the dangers of using the Internet. While it can be argued that this may not be considered common knowledge, the potential dangers of visiting unknown Web sites should be known.
    - **Possible answer:** True, False, Don't know.
      Of the answer alternatives above it was the second one; "false"; that was the correct answer. (Provos et al., 2007) But the other two alternatives gives an indication either don't know or don't think that it is possible to be infected just by visiting a webpage.
13. **Question:** When you get to a webpage that asks you if you want to run script on the page, do you answer yes?
    This question gave an indication of the users Internet behaviour, but it did not an-

swer the question if it was a lack of knowledge or a bad attitude that caused the answers. It is important since the running off script, or anything else, should not be run on pages that one don't know, since it may be malicious software.

- **Possible answer:** No/Yes, but only if I know that the page is safe/Sometimes I do, sometimes I don't.
  The answer alternatives were worded so that they tried to give an indication on the behaviour of the user, while at the same time trying to distinguish between if it is a conscious choices on their part. This was done with the last to alternatives where the first of those indicates that the user tries to establish if the page can be trusted. The last alternative indicates that the user may not always be conscious about it.

- **Physical security**

14. **Question:** Do you usually secure your computer?
    This question, together with question 18, tried to establish how the user treated their computers. An example is if they leave it unguarded in a room. Also, following the argumentation from chapter 3.3.2; What to measure and why, subchapter "Development of questions", under the point "sources of errors", the questions (14 and 18), will try to discover users that "always agrees" to questions.
    - **Possible answer:** Yes/No]
      The correct answer is yes.
15. **Question:** *Do you store sensitive information unencrypted on your laptop (if you have one), or another portable device?*
    This question was not of immediate importance, but it was interesting since sensitive information, in this case that is most probably personal information, should not be stored on an unencrypted device, especially not on a device that is often moved from place to place.
    - **Possible answer:** Yes/No/Don't know.
      The correct answer here should be "NO", while the worst answer is "Don't now".
16. **Question:** *Are your hard disk encrypted?*
    The argumentation was the same as the one from the previous question.
    - **Possible answer:** Yes/No/Don't know.
      The correct answer here should be "Yes", while the worst answer is "Don't now" since it denotes a lack of knowledge.
17. **Question:** *Do you lock the computer when you leave it?*
    This question could be viewed together with question 6 in that the previous one asked if the computer was password protected while this question asks if it is used. The importance here was simply that for it to be a point in the computer to be password protected is had to be used.
    - **Possible answer:** Yes/No
      The correct answer here is Yes.
18. **Question:** *When throwing printouts, do you then ensure that they don't contain critical data? An example can be private information.*

The treatment of information is an important aspect of security, and it is assumed that almost everybody and especially students, handles, if not regularly, printouts containing critical data.
  - **Possible answer:** Yes/No
    The correct answer here was Yes.

19. **Question:** *Do you often leave the computer unattended?*
    See argumentation from question 14.
  - **Possible answer:** Yes/No
    The correct answer is "no".

- **General computer usage**

20. **Question:** *Do you update your computer regularly?*
    This was important since a computer that is not regularly updated can be susceptible to malicious software.
  - **Possible answer:** Yes/No/Don't know.
    The best answer here is "yes". In addition the last alternative might be considered the worst since if the user answers "No", at least she is aware of the fact.

21. **Question:** *If you have an anti virus program, do you know if it is updated?*
    The importance is that for an anti virus program to be effective it has to be updated regularly. In addition all users should have an anti virus software on the computer, since it is an important part of the overall security.
  - **Possible answer:** Yes/No/I don't have an anti virus program.
    Of the answer alternatives, "yes" is the best, although it does not tell if the software is updated, just the users knowledge it exists. "No" might be considered somewhat better than the last one since an anti virus program that may or may not be updated is better than no anti virus program at all.

22. **Question:** *Are your computer password protected?*
    Password protection can probably be said to be on of the easiest methods to secure a computer. And as such there is no reason not to have it in place. In addition it is often the only method of securing the computer, excluding other external methods, like securing the room.
  - **Possible answer:** Yes/No/Don't know
    The best answer here is yes, while the rest might be considered equally bad.

23. **Question:** *Does your regular user have admin rights at your computer?*
    This question is important since if a user regularly uses an account with administrator privileges makes the system more vulnerable, an example is that it makes it easier for viruses or other malware to damage the system since they have access to more.
  - **Possible answer:** Yes/No/Don't know
    The best answer here is yes, while the worst might be considered "Don't know" since such an answer demonstrates a lack of knowledge.

24. **Question:** *Consider this statement. You don't have a program that can be used to update all the programs on the computer for you, and Microsoft released such a*

program, would you use it? There exists programs that can be used to update the computer for a user, and while this may make things easier for people, it can be considered a security risk to allow one program access to everything. This question then tries to determine if the users would trust such a program if it was released by Microsoft.

- **Possible answer:** Yes/No
  Considering that Microsoft is a well respected and trusted company, using programs from them can be considered safe in terms of it containing malicious code. So the answer in this case is determined to be "Yes"

25. **Question:** *Consider this statement. You don't have a program that can be used to update all the programs on the computer for you, so a person you trust recommends one for you? Would you have tested it?*
    See argumentation from the previous question.
    - **Possible answer:** Yes/No
      Even though the program came from a trusted person, one can newer be sure that the program is safe if it is not from a known distributor. So the answer that may be considered the best in terms of security is in this scenario "no".

- **Backup**

26. **Question:** *Do you know if there exists backup off data that is important for you?*
    The importance here is to discover if the user know of the existence of backup systems. While the question does not distinguish between the school or elsewhere, it can be used as an indication of the users awareness about backup.
    - **Possible answer:** Yes/No
      The correct answer is "yes".
27. **Question:** *If you answer 'no' to the question above: Why not?*
    This question is important since it tries to establish the reason for the answer "no" from the previous question.
    - **Possible answer:** Newer thought of it/It is not my responsibility/Don't need it/I havent done it, yet...
      The answer alternatives tries to establish the reasons for why the users don't have backup. "Don't need it" was considered to be slightly better than "I havent done it, yet...", while the two first alternatives were considered the worst answers. In that the first displays a lack of knowledge, while the second displays a lack of responsibility.
28. **Question:** *Consider this scenario: You work at home on school work, do you then copy this to your account at school in order to have a backup of the work?*
    This question can be said to test the same as the two previous ones; if they perform backup and if they are aware of the existence of backup. In addition to this it determines if they use the school as a off-site backup location.
    - **Possible answer:** Yes/No/I use only the computers at school/I perform backup myself.
      The alternatives were worded so that they answered the question directly, and in addition gave alternatives that provided additional reasons.

"No" is the worst answer here, with the last alternative considered to be slightly worse than the two alternatives, following the reasoning that the backup may not be stored at an secure external location.

29. **Question:** *Where would you store your backups?*
    This question is important in that it determines the students knowledge in where they should store their backup.
    - **Possible answer:** USB stick, DVD, etc./External secure location./Another disk in the PC.
      The alternatives tried to cover the common places that the students can store backups, while at the same time dividing them in categories.
      The best answer would be an external secure location since it is usually not affected is something happens at the main location. This followed by "USB stick, DVD, etc." and lastly "Another disk in the PC".
30. **Question:** *Do you feel that you have a responsibility in ensuring that the data you use have a backup?*
    The importance of this question is in the knowledge of the users feelings of responsibility in ensuring that they have a functioning backup.
    - **Possible answer:** Yes/No
      The correct answer in this case is "yes".

- **E-mail**
  31. **Question:** *Consider this scenario: You are not expecting any email and receive one from an unknown sender, what would you most likely do?*
      This question together with question 35, tried to establish what the users were most likely to do if they received an unknown e-mail. The difference between the two questions is that the first question establish that you are not expecting an e-mail while the second do not. The reasoning behind this was to see if the users would delete an email without reading it first if it was from a completely unknown sender.
      - **Possible answer:** Read it/Delete it without opening it.
        Continuing the argument above, the recommended answer here would be to delete it without opening it. While this was not stated in the question, an E-mail can be considerd "known" if it, as an example, comes from an institution that you know, e.g. a mail that clearly comes from UiA.
  32. **Question:** *Do you know if your mail is stored at your local computer or at the server?*
      As long as the mail is stored at the server it can be considered safe, but if it is downloaded to the local machine it can be a problem, since then it becomes important that there exists backup off it. Another important aspect is if the mail is read at a public computer, then it is imperative to know if the mail are downloaded or not.
      - **Possible answer:** Yes/No
        This question needs only a simple yes or No, where the correct answer would be "yes".
  33. **Question:** *Do you have automatic filtering of mail active?* This question together with the next one discovered if the user have automatic filtering of e-mail active,

and if so was the case, check if they inspect if important mail is discarded.
Automatic filtering of mail is important since it removes unwanted email, that again can result in fewer chances that malicious email is opened. In addition, automatic filtering of mail can make the use of email more efficient if the unwanted mail is already deleted.
  - **Possible answer:** Yes/No/Don't/know.
    The correct answer is "yes", while the worst is "Don't know" since the last answer indicates a lack of knowledge, while "No" at least indicates that they are aware of the current state.

34. **Question:** *If you answered 'yes' to the question above, do you check regularly to see if important mail is discarded?* This question was a continuation of the previous one, and is important since it is possible that e-mail that should not be discarded is sorted as junk mail.
  - **Possible answer:** Yes/No
    The correct answer should be "Yes".
35. **Question:** *Do you usually delete unknown email without opening it?*
See argumentation from question 31.
  - **Possible answer:** Yes/No
    See argumentation from question 31.

- **Rules**

36. **Question:** *Have you read the schools rules regarding the use of computers?*
This question would determine if the students have read the rules. The answer to this gives an indication about their knowledge and attitude about rules.
  - **Possible answer:** Yes/No
    The answer that may be considered the correct one is "yes", since the student then have demonstrated with their actions that
37. **Question:** *Have you downloaded illegal software when at school?*
It was chosen since the answer indicates how the students adhere to the schools rules. In addition the school may get into problems when the students download illegal software .
  - **Possible answer:** Yes/No
    The correct answer here is "no", since doing otherwise is a violation of the rules from the university, in addition to that it may also be against the law.

- **Personal information**

38. **Question:** *Please specify you gender.*
This question would make it possible to see from the result if there was any differences between the genders.
39. **Question:** *Please specify your line of study.*
This question would make it possible to see from the result if there were any differences between the different lines of study.

- **Additional questions**

40. **Question:** *How many minutes did you use on the test?*

The intention with this question was to measure how much time the students used on the survey.
  - **Possible answer:** Less than five/Between five and ten/More than ten.

41. **Question:** *Length of the test? This test consisted of 37 questions, how do you consider this length?*
    The intention was to measure the students taught about the length of the survey.
    - **Possible answer:** The number of questions were OK. It felt a bit long. Definitely too long.
42. **Question:** *Please specify difficult questions.*

3.3.3 How to measure it?

As stated in chapter 3.2.1, the method that was to be used to measure security awareness was multiple choice. This had positive and negative aspects, some of which are listed below:

- Positive aspects
  - Quick for the respondents to complete.
  - The result is not difficult to evaluate, the answers need not be interpreted in any way.
- Negative aspects
  - Developing a multiple choice survey can be time consuming.
  - The validity of the result is limited to how the questions are made.

A more detailed view of the aspects mentioned above was that for the positive parts part the respondents needed only to mark the preferred answer. This is true for a pure multiple choice test, but it is also possible to have the option that some of the questions demands that the respondent write the answer. This leads directly to the reasoning for the second point in that once the method for evaluating the results is in place, doing so is simply a process of adding up the answers and calculating the result.

An explanation of the negative aspects is that the combination of the question and answer-alternatives should provide a good picture of the respondents understanding of security awareness, for example password, the questions need to cover all aspects of it, the users understanding of what is a good password, how passwords should be treated, and how they feel about the passwords, rules, use of them and so on. If the questions do not cover enough aspects of the topic, then using the result to make a conclusion may be difficult.

The platform that was used in the survey was the one used by the school; fronter. Since Fronter was web based there where no additional work concerning the actual execution of the survey. In addition, the ability to Fronter to export the results afterwards made the post survey work easier since it would not be necessary to transcribe papers.

calculation of result

The result was calculated using the same principle as the one used in the preliminary survey:

1. The options to each questions where assigned a value between one and three, based on how correct the alternative was determined to be.
2. The total sum for each option was then calculated.
3. The combined sum for each option was then added together and used as a score for each question.
4. The sum for each question was then used to calculate the score for each category.
5. The value for each category was added together to make a total score.

The difference between the survey done by Kruger and Kearney, and the one done by this study was that an importance weighting between the questions was not performed. The main reason for this was the lack of experience and the amount of time available for the project.
The only adjustment that was done was to ensure that each of the three categories was of equal importance when it came to the calcualtion of the result. This was done by using a multiplier on each based on the maximum number of points that it was possible to achieve.

3.3.4 How to evaluate the result.

The evaluation of the test was performed in two stages, one where the actual result from the survey about awareness was analyzed, and one where the participants response to the questions about the test were analyzed.

The result from the awareness survey will be compared to a set of hypothesizes:

- The number of respondents
  - The total number of respondents.
  - The number of respondents.
- The result.
  - The total result from all the students
  - The result based on different hypothesis.

Evaluation of the users feedback to the survey

This part of the evaluation was planned based on feedback gained from the questions requesting that in the study, those were about the length of the survey, time used and difficult questions

Length of the test

Here the respondents were given three statements about the length of the survey, and were asked to mark the one they felt best described what they felt about the length. The choices available as described in chapter 3.3.2, were:

- The number of questions were OK.
- It felt a bit long.
- Definitely too long.

Time used

In the introduction to the test it was stated that the estimated time to complete the survey was a maximum of 10 minutes. In order to see if the actual time the users spent on the survey was within this time frame, the survey included a question about the length of the time used. Here the users were asked to mark what description best fitted their time used:

- Less than five.
- Between five and ten.
- More than ten.

Evaluation of the questions

The evaluation of the questions used information gained from the feeback the users where able to place on the page. In addition to this, a new understanding of the questions was also used in the evaluation.

Evaluation of the awareness survey

This part of the evaluation of the survey was planned according to the expected number of answers. Since if it was to few, the survey would only give an indication that the proposed theories was correct.

The total level of security awareness.

When evaluating the level of security awareness, the scale from Kruger and Kearney will be used:

- *Good (80% - 100%) Satisfactory no need for action*
- *Average (79% - 60%) Monitor action potentially required*
- *Poor (59% and less) Unsatisfactory action required*

The result was, without any preexisting knowledge, estimated to be in the average range, and then closer to 60% than 80% percent. The reason for this estimation was that, as students at a university, the expectation were that they had a general understanding of security.

The total number of respondents.

The number of respondents can be estimated on the bases on earlier results from surveys performed by the school. Those where between 5 and 8 %, so it was not likely that the degree of completion on this survey would be higher. Also, since those surveys were evaluation of the studies, they may have been considered somewhat important, and thus the total number or respondents were likely be lower on this survey since it will probably be considered to be less important.
So an estimation of the percentage of respondents was less than five percent, more specifically around two or three.

The result from security and programming vs rest.

Since the expected number of respondents were low, it was difficult to make detailed predictions about the level of security awareness between different factions.

Because of this, the only prediction was that the result from the security and programming, both on the master and bachelor, would be somewhat higher than the rest of the school. The reason for this assumption was that the number of students that had a high knowledge of computers, and probably also security, could be expected to be higher among them then the rest of the school.

It should be noted that security aware students, both in terms of knowledge and behaviour, can also be found at the other courses, not only on the computer technical ones.

3.3.5 Execution and evaluation of the field survey

Evaluation of the survey

This part of the evaluation was done based on feedback gained from the questions requesting that in the study, and additional feedback gained from other sources. Those was from some students who took contact directly and through discussions with some of the respondents.

The last questions in the survey were about the test itself, more specifically they were about the length of the survey, time used and questions that were determined to be difficult.

Length of the survey

One question, as mentioned above, was about the respondents thoughts about the length of the survey. Here the respondents were given three statements about the length of the survey, and were asked to mark the one they felt best described what they felt about the length. The choices available were:

- The number of questions was OK.
- It felt a bit long.
- Definitely too long.

The result from this can be seen in the diagram below:

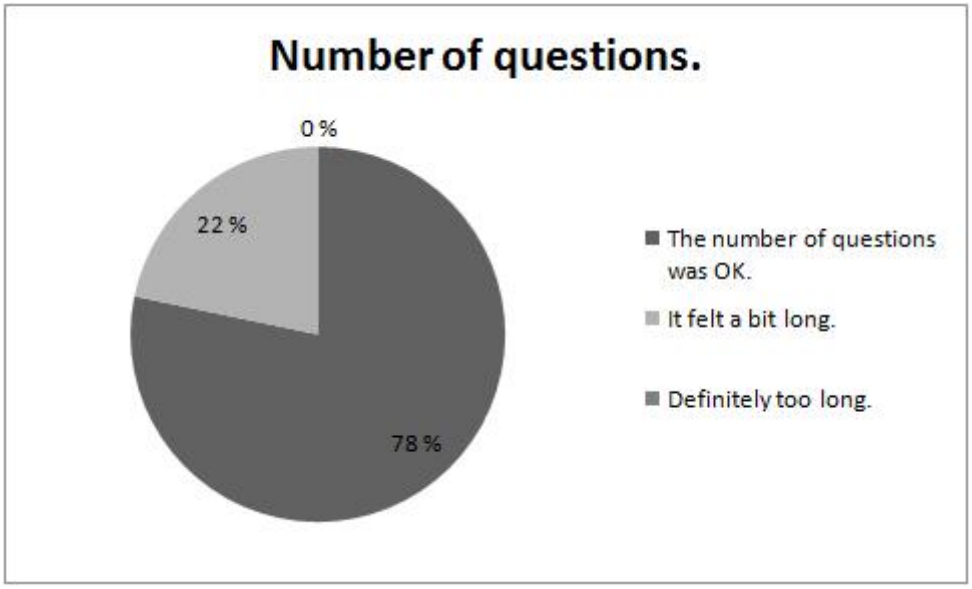

Figure 3: Length of the survey.

As the figure above demonstrates, the majority of the students that answered the test felt that it was of an acceptable length, while only a few felt that it was a bit to long. Even though it may seem as this shows that a survey of about 40 questions were an OK length. One problem with the result was that it told nothing about the potential number of students that did not participate because of the length.

Time used

In the introduction to the survey it was stated that the estimated time to complete the survey was a maximum of 10 minutes. In order to see if the actual time the users spent on the survey was within this time frame, the survey included a question about the length of the time used. Here the users were asked to mark what time frame best fitted their time used:

- Less than five.
- Between five and ten.
- More than ten.

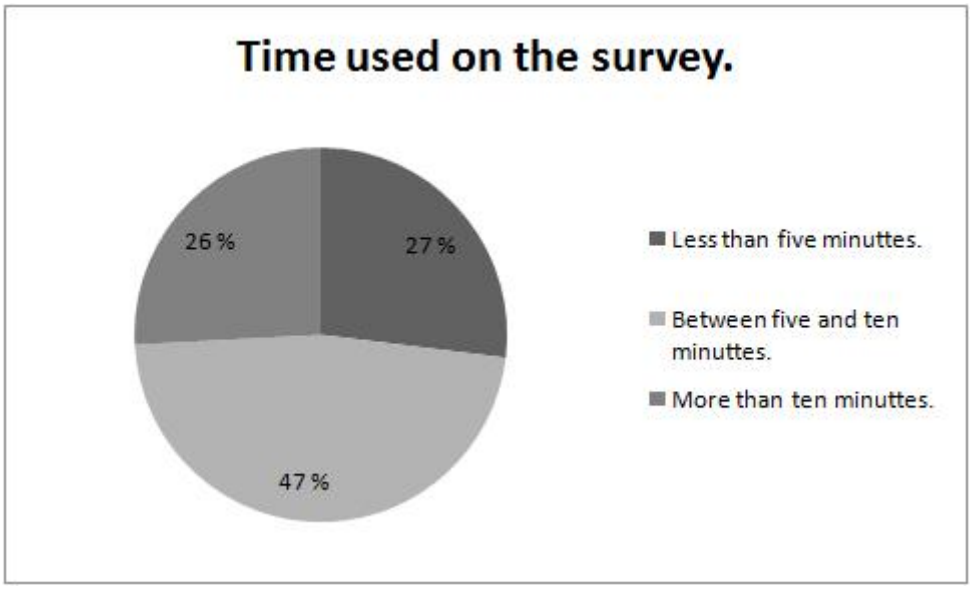

Figure 4: Time used on the survey.

As can be seen in the figure above, of the students that answered the survey, the majority answered between five and ten minutes, so the estimated time can be considered to be good when half of those answering survey used around that timeframe, and the rest was almost equally divided over and under that time..

Evaluation of the questions

The evaluation of the questions followed the plan from chapter 3.3.4. In addition to this feedback gained through informal discussions with some of the students that performed the survey.

The numbers to the questions used below are the same as those found in the survey.

- **Physical security**
  14. **Question:** Do you usually secure your computer?
      - **Possible answer:** Yes, No
        The intention with this question was, as discussed in chapter 3.3.2; subchapter "Development of questions", to determine if the person taking the survey always agrees with the question at hand.
        This was dropped since the feedback showed that several students did not see this question as to physically secure the computer. Therefore it can't be used to determine this with a high degree of certainty.
        The questions should have been better worded and there should probably have been more that one sett.
  15. **Question:** *Do you store sensitive information unencrypted on your laptop (if you have one), or another portable device?*
      - **Possible answer:** Yes, No, Don't know.
        The intention with the question, to discover if the users are conscious about their use of portable devices is sound, but the wording of this question may cause people that are conscious about it to register as if they aren't.
        A better wording may have been to ask if the users store sensitive information on such a device.
        A second alternative would be to have it as a follow up question to one that asks is sensitive information is stored at a device in the first place.
  16. **Question:** *Are your hard disk encrypted?*
      - **Possible answer:** Yes, No, Don't know.
        The evaluation showed that this question may not be that relevant when measuring students security awareness. The explanation is that most student don't have data that is so important that they need to encrypt it. This sentiment was echoed by the students feeling that they simply did not need to do it.
        A possible change to this question would be to replace it with a more relevant question, or to add the option to select that they do not need it.
  19. **Question:** *Do you often leave the computer unattended?*
      - **Possible answer:** Yes, No
        See the discussion on question 14.
- **General computer usage**
  20. **Question:** *If you have an anti virus program, do you know if it is updated?*
      - **Possible answer:** Yes, No, I don't have an antivirus program.
        The problem with this question is that it does not take into acount that not all students use Windows.

22. **Question:** *Consider this statement. You don't have a program that can be used to update all the programs on the computer for you, and Microsoft released such a program, would you use it?*
    - **Possible answer:** Yes, No
      See the discussion on question 20
23. **Question:** *Consider this statement. You don't have a program that can be used to update all the programs on the computer for you, so a person you trust recommends one for you? Would you have tested it?* Se the previous question.
    - **Possible answer:** Yes, No
      See the discussion on question 20

- **Backup**
  24. **Question:** *Do you know if there exists backup off data that is important for you?*
      - **Possible answer:** Yes, No
        See the discussion on the next question.
  25. **Question:** *If you answer 'no' to the question above: Why not?*
      - **Possible answer:** Newer thought of it. It is not my responsibility. Don't need it. I havent done it, yet...
        The problem with this and the previous question, is that it is not guaranteed that the students answers correctly. This means that it is possible to answer "Yes" to the previous question and still give an answer to this question. On the other hand, it is not guaranteed that this is a mistake, in that "yes" was marked but the intention was "no", or that the question was misunderstood. This result in that the answer from a student that uses the wrong combinations can't simply be deleted.
        In addition, it was discovered late in the project that an answer here would make it possible to get a higher score even though the person had a low security awareness. This was possible since answering "no" to the previous question gave one point, while the best answer here would add three points to this. The result of this would be that one person could get three points by answering yes to the previous one, while another could get a total of four.
        This problem was solved by simply not including the question when calculating the result.

- **E-mail**
  33. **Question:** *Do you have automatic filtering of mail active?*
      - **Possible answer:** Yes, No, Don't know.
        No problems with this question, but it is included because of the next question.
  34. **Question:** *If you answered 'yes' to the question above, do you check regularly to see if important mail is discarded?*
      - **Possible answer:** Yes, No
        The argumentation is the same as for question 25.
  35. **Question:** *Do you usually delete unknown email without opening it?*

- **Rules**

37. **Question:** *Have you downloaded illegal software when at school?*
    - **Possible answer:** Yes, No
      Some of the feedback suggested that this question was somewhat unclear, and would have been improved by a better explanation.
      This could have been done by stating that by illegal software the intention was any kind of software that the student did not have the right to download, an example being programs that the student did not own.

- **Personal information**

38. **Question:** *Please specify your line of study.*
    The problem with this question was that it relied on the student to write the relevant line of study. This resulted in instances where some students did not write the correct study, or instances where it was difficult to be certain what the student meant.
    The best here would have been to have listed the different studies and let the student choose the correct one.

- **Additional questions**

Summary

Following the discussion on the questions above, it is clear that there were several issues with the survey. The problems ranged from questions that may have been easy to misunderstand, to questions that made it possible to answer wrongly, as seen with the questions that required a follow up answer.
It was discovered late in the process the follow up questions discussed in the section above made it possible for a person that answered
Also, some of the questions may not be necessary or they may be wrong, in that they don't contribute towards the end goal of measuring awareness among students.
The end result of this evaluation is that it the survey is, at most, good enough to be used as an indication on the level of security awareness.

Evaluation of result to the awareness survey

The total level of security awareness.

It was stated in chapter 3.3.4; Evaluation of the result, that the awareness level of the students would be in the lower average, as defined by Kruger and Kearney. The result can be seen in the diagram below:

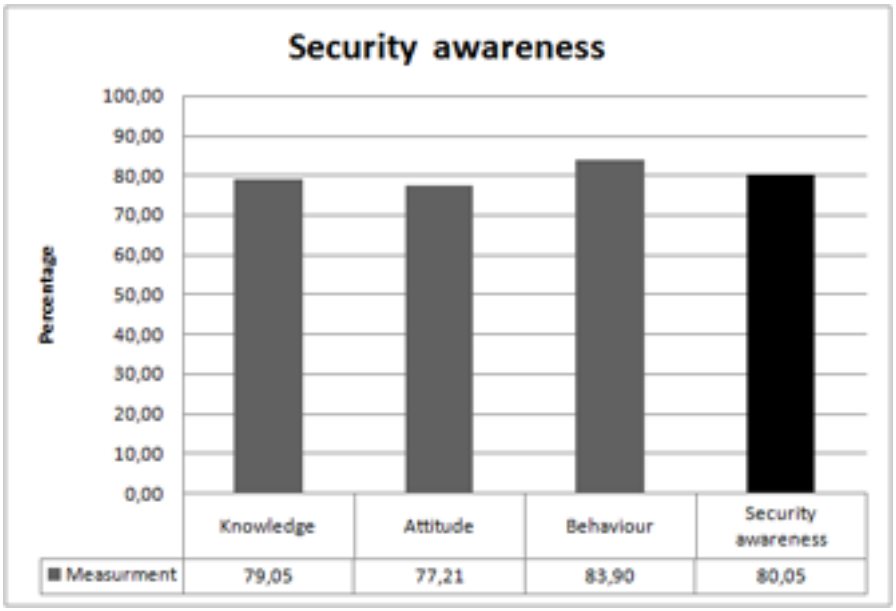

Figure 5: Security awareness.

Compared to what was estimated, the result was about 20% higher. But it should be noted that following the result from the evaluation of the survey, this result could at best be used as an indication of the level awareness.

The total number of respondents.

From the discussion in chapter 3.3.4; Evaluation of the result, it was estimated that the result of the survey would be at 2 - 3%.

The actual result was 4,1%, and was higher than the estimated result.

Comparison of computer classes vs non-computer classes

Following the discussion from 3.3.4; Evaluation of the result, it was stated that the computer courses, on average, probably had a higher degree of security awareness than the rest of the students.

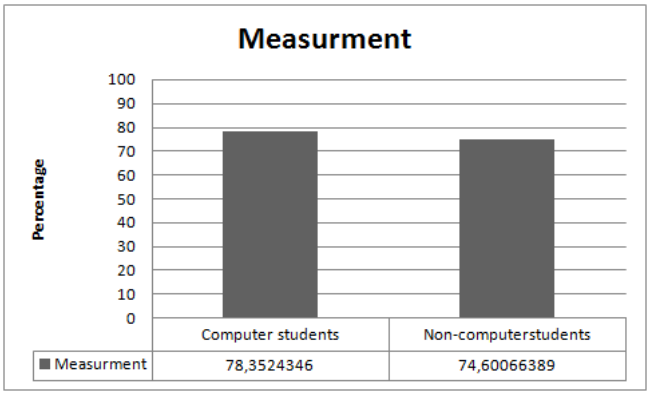

Figure 6: Comparison of computer classes vs non-computer classes.

As can be seen on figure 6; the survey gives an indication that the assumption may have been correct. But it should be noted that the same problems existed here as with the result discussed in the previous section, so the result can at best be used as an indication.

4 Discussion

4.1 The search for literature

The search for literature was not as good as it should have been. The reason was partly that it at first was not done with a good enough plan; so that the search had to be repeated, but also since it was done on only a few databases, so it was not guaranteed that it covered all relevant papers.

In addition, more work should have been spent on reviewing the documents in order to verify that they are of a certain standard so that they could be used in the thesis.

4.2 Comparison of definitions of security awareness

The comparison of the different definitions was done based on the criteria that was stated in the start of the chapter, except for the discussion on the definition in relation to the feasibility of measuring awareness as this part of the discussion was done in general at the beginning of the chapter.

The conclusion following the comparison of the definitions was shallow and should have been more elaborate. This would have ensured that the result had been more accurate and believable.

4.3 Comparison of methods for measuring of security awareness

The comparison of methods was not done with a specified set of criteria, so had there been more methods, the procedure used now would likely not have resulted in a good comparison.

4.4 Method for measuring awareness

4.4.1 The work

From the evaluation of the survey it was clear that more work should have been done in developing the questions since some of them were unclear and could be misunderstood. In addition it was a major fault to not take in consideration in the development of the questions that not everyone use Windows. This could have been avoided by a more diverse group of test subjects.

4.4.2 The method

The method found and used in this thesis measures security awareness in three different levels; knowledge, attitude and behaviour, this, together with a defined and constructed questions and areas to be measured, makes it possible to easily make a comparison of the different levels. Also, as can be seen in the work from Kruger and Kearney, the method should have no problem with bigger organizations.

The drawback is that, according to Kruger and Kearney, the calculation of the importance weighting that should be given to each question is time consuming.

Despite the drawback, this indicates that the method is well suited to be used in measuring security awareness.

4.5 Testing of method for measuring awareness

More time should have been spent on the process of calculating the result, since now there are factors that can potentially affect the result. The problem was twofold; the selection of the questions, and the wording of the questions. This result in that the result from the measurement may not be accurate enough, and that the result can, at most, be used as an indication of the total level of security awareness.

4.6 General discussion

The result from the work on this thesis was not as good as it could have been, and this can be explained by several factors, some of those are:

- The work process was not as effective as it should.
- The motivation to work harder was not always present.
- The planning was in many cases not good enough.

5 Conclusion and further work

5.1 Goals

The four goals of this thesis started with discussing the existing definitions of security awareness and a comparison of existing methods for measuring security awareness. This was to be followed by possible improvements in the measuring method and concluded by the performance of a survey to test the method.

5.2 Solution

The solution was to start with a search of the existing literature in order to be able to solve the two first goals mentioned above. This was then followed by a discussion on the definitions of security awareness in relation to the feasibility of measuring awareness.

Continuing the solution, it was determined that the method found was not in need of changes beyond a clarification off how to calculate the result. The last part of the solution was solved by first performing a preliminary survey and the construction of a method for evaluating the result, and then the solution was concluded by the main survey of the security awareness level to students at UiA.

5.3 Result

The result from the thesis was threefold:

- The first was definitions of security awareness in relation to the feasibility of measuring awareness.
- The second was a method for measuring of security awareness and the realization that there exist few methods that do this.
- And the third, was the result from the survey that gave an indication that the security awareness level at the University of Agder may be considered as good.

5.4 Further work

Defining questions within the different aspects

The questions within on topic, like password, should be made so that they measure all of the three aspects: *"attitude", "knowledge" and behaviour"*. Following this a method for how to word the questions within the different categories should be made. This method will ensure

This will ensure that the likelihood of a question within a given category give an answer that fits within said category.

Defining what questions to ask

Following the advise from Kruger and Kearney, a definition should be made that tells what type of questions that are relevant to ask.

The reason for this is that otherwise it is easy to develop questions that may give an answer to e.g. the knowledge about passwords, but that may not be most appropriate or best question to ask.
This differs from the previous section in that it defined *how* to ask questions *within different* categories, while this section concern itself with *what type* of questions it is *relevant* to ask.

Changes in method

A method should be developed that can be used to measure security awareness with a higher degree of certainty so that it is not possible for the the person that is participating in the survey to make mistakes.

6 References

Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4):276–289, 2007.

A. Da Veiga and J. H. P. Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010. doi: DOI: 10.1016/j.cose.2009.09.002.

D'Aubeterre Fergle, S. Iyer Lakshmi, and Singh Rahul. An empirical evaluation of information security awareness levels in designing secure business processes, 2009. 15556411-11.

S. Hansche. Designing a security awareness program: Part i. *Information Systems Security*, 9 (6):14–23, 2001.

Sokratis K. Katsikas. Health care management and information systems security: awareness, training or education? *International Journal of Medical Informatics*, 60(2):129–135, 2000. doi: DOI: 10.1016/S1386-5056(00)00112-X.

E. Kritzinger and E. Smith. Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, 27(5-6):224–231, 2008. doi: DOI: 10.1016/j.cose.2008.05.006.

H.A. Kruger and W.D. Kearney. A prototype for assessing information security awareness. *Computers & Security*, 25(4):289–296, 2006. doi: DOI: 10.1016/j.cose.2006.02.008.

A. Marks and Y. Rezgui. A comparative study of information security awareness in higher education based on the concept of design theorizing. In *Management and Service Science, 2009. MASS '09. International Conference on*, pages 1–7, 2009.

A. Martins and Jan H. P. Eloff. Information security culture, 2002. 719826 203-214.

Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, and Nagendra Modadugu. The ghost in the browser: Analysis of web-based malware., 2007. In Usenix Hotbots.

Petri Puhakainen. *A design theory for information security awareness*. PhD thesis, UNIVERSITY OF OULU, 2006.

MikkoT. Siponen. Five dimensions of information security awareness. *SIGCAS Comput. Soc.*, 31(2):24–29, 2001. 503348.

Frode Svartdal. *Pskologiens forskningsmetoder*. Fagbokforlaget, Bergen, 2009.

A. Al-Hamdani Wasim. Assessment of need and method of delivery for information security awareness program, 2006. 1231069 102-108.

Mark Wilson and Joan Hash. Building an information technology security awareness and training program, 02.02.10 2003. http://csrc.nist.gov/publications/PubsSPs.html.

7 Appendix

7.1 Appendix A

General security

Questions	Answers
Do you update your computer regularly?	☐ Yes ☐ No
Assuming one of your computers is not important for you in any way, should you care if it gets infected by a virus?	☐ Yes ☐ No
In you regular computer use, are you then using an account that has full access to you computer? This is an account that has more rights than a normal user, usually an administrator account.	☐ Yes ☐ No ☐ Don't know.
Would you consider using a program to ensure that your computer and the programs that is installed on it is up to date?	☐ Yes ☐ No

Internet

Questions	Answers
When you get to a web page that you don't know, and it asks you if you want to run a script on the page, do you answer yes?	☐ Yes ☐ No
Do you, or have you placed information on the Internet that tells when you will leave for a vacation?	☐ Yes ☐ No
Are you conscious about what private information you share on the Internet?	☐ Yes ☐ No
Do you use Facebook?	☐ Yes ☐ No
If you answered yes to the question above, did you know that, while a picture exists on Facebook, that you grant Facebook a licence for it?	☐ Yes ☐ No

Backup

Questions	Answers
Do you have backup off data that is important for you?	☐ Yes ☐ No
If you answered 'no' to the question above : Why not?	☐ I don't need to do it. ☐ I have not considered it. ☐ I haven't done it, yet...
Were would you store your backups?	☐ Another disk in the PC. ☐ USB stick, DVD, etc. ☐ External secure location.

Physical security

Questions	Answers
Have you left your computer in an unlocked room?	☐ Yes ☐ No
Do you lock the computer when you leave it?	☐ Yes ☐ No

Password

Questions	Answers
Are you conscious about your use of passwords. That is, do you distinguish between critical and non-critical use?	☐ Yes ☐ No
Is your computer password protected?	☐ Yes ☐ No
Passwords and were they are used, can be written down and stored at a secure location.	☐ Strongly agree ☐ Agree ☐ Disagree ☐ Strongly disagree ☐ No opinion.
Passwords should only be remembered.	☐ Strongly agree ☐ Agree ☐ Disagree ☐ Strongly disagree ☐ No opinion
Passwords can be written down, but it should not be possible to guess were they are supposed to be used.	☐ Strongly agree ☐ Agree ☐ Disagree ☐ Strongly disagree ☐ No opinion.
One of your friends can't access Fronter to get some files, and you can't send them to her. Is it OK do lend her your password?	☐ Agree ☐ Disagree

Questions	Answers
How strong do you consider the following password? Kyfdsh2gv	☐ Very strong. ☐ Strong ☐ Ok ☐ Weak ☐ Very weak
How strong do you consider the following password? #Oyhfpyggyope	☐ Very strong. ☐ Strong ☐ Ok ☐ Weak ☐ Very weak
How strong do you consider the following password? Mvdyqp_amrf	☐ Very strong. ☐ Strong ☐ Ok ☐ Weak ☐ Very weak