Master Thesis

Building a Successful Information Security Awareness Programme for NLI

Peng Xiong

Peng.xiong@hig.no

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

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

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

Abstract

NLI is a Norwegian industrial company. Information security, which is crucial for their business success, has gained more and more attention from NLI's top management and IT department. Currently the technical side of security in NLI is better developed than the human and organizational side. More needs to be done are that building a progamme to increase information security awareness for each employee and making every employee in NLI realize the importance and necessity of information security and then acts accordingly.

This thesis defined three research questions in order to building a successful information security awareness programme for NLI:

1) What should the curriculum of an information security awareness programme for NLI be?
2) How should the information security programme be organized to effectively deliver the necessary information to NLI employees?
3) How should the effectiveness of the information security awareness programme be measured in NLI?

Solving these three research questions, I have done an interview in NLI and then understood their management organization, work processes and information system in use. Based on results of interview combined with some literature study, I analyzed and then provided proposed training curriculums of an information security awareness programme for NLI. Computer based training which include both web-based and no web-based training combined with an annual web-based mandatory information security exam is the best delivery methods that I proposed for NLI compared with others. In order to measure the effectiveness of the information security awareness programme, I have identified and defined a set of security awareness metrics for NLI. The set is not meant to be a complete set of awareness metrics for NLI, but hopefully they may serve as examples and give inspiration to other metric definitions. The metrics are defined according to available templates, and they are presented in Appendix C at the end of this report.

It is important that the proposed information security awareness programme can be used in practical work in NLI. A practical test of this programme is therefore very important. This is however not being described in this report. But it is considered a natural follow-up to this report.

Acknowledgements

First of all, I wish to express my sincere gratitude to my two supervisors, Professor Jose J. Gonzalez and Finn Olav Sveen for all the help in connection with the project. They have provided invaluable technical and methodological assistance and support throughout the project period. Without their excellent guidance, this work could not have reached completion.

Secondly, I wish to extend special thanks to IT Manager Hilde Gjevestad Hellenes and Managing Director Anders Jensen in NLI. Many thanks they give me this project and also give me lots of support and help to hand this project. The interview-based method used in the research is totally dependent on cooperative employees. Many thanks Hilde Gjevestad Hellenes find all key persons to participate in the interviews, and also help in motivating them to participate in the interview. Without such help, completing the interview would be much harder.

Thirdly, I would also like to give a big thanks to these NLI employees, who with great good will have contributed their views during interviews, and offered this time in a hectic schedule.

Last, I also owe my special thanks to my family for their love during my master studies. They really have made this world a better place to live.

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Topic covered by the project

In the recent years, information security has become a more important issue for most companies around the world. However, when implementing their information security solutions, most of companies have typically focused on technical and procedural security measures (such as installing security hardware device like a firewall or an intrusion detection system) [1] [2]. From the information security point of view, this is not good enough since not all information security challenges can be achieved only by technical controls. Effective information security in an organization requires the commitment of employees at all levels. Without full employee commitment, security mechanisms may be diminished or bypassed entirely [3] [4] [5]. The attitudes and awareness of the employees are very important for the information security in a company today. Mr. Gullik Wold points out the importance of awareness in his MSc Thesis "Key factors in making ICT Security Policies effective" [6]. His survey shows "organizations that do not promote information security awareness are more likely to experience a major security incident than those that do promote awareness." As for the definition of security awareness, NIST (National Institute of Standards and Technology) [14] defines it as follows:

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

The Information Security Forum [7] defines information security awareness as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly.

The contents of those definitions are quite similar as they both define information security awareness as the level of knowledge and attitude, regarding the importance and understanding of information security, and the willingness to act and behave accordingly.

Nevertheless, it is very difficult to improve the employee's security awareness and change their attitude and behavior for an organization [8]. Many organizations have developed and implemented different programmes in order to improve their employees' information security awareness. The results for most organizations are ineffective programmes that do not improve information security practices [9].

In this project, I intended to build an efficient information security awareness programme for NLI. Based on what is done by some researchers or companies in this field combined with some practical interviews with NLI employees and managements, I will analysis the data and finally propose recommendations for NLI. Such recommendation will hopefully make it easier for NLI or other similar companies to build their information security awareness programmes.

1.2 Problem description

NLI is a Norwegian industrial company supplying engineering and fabrication services, technology products and process solutions to the following market areas: oil & gas, industrial plants, maritime industry as well as bridges and buildings/infrastructure.

Information security, which is crucial for the business success of NLI, has gained more and more attention from NLI's top management and IT department. Technical security measures such as firewalls and access control have been implemented already. An IT security policy was established in October 2008 to clarify routines for correctly handling confidential information and information resources. The policy is required to be carefully read by every employee in NLI and an agreement to follow it must be signed afterwards. Nevertheless the policy is frequently violated [10].

Even though some executive managers declare that they usually do pay good attention to the information security and believe it is very important for NLI, they still complain about lacking enough time and resources to invest in corresponding tasks. In other words, they believe that the technical measures and the IT security policy are sufficient for protecting information.

However, many respondents in the UK DTI information security breaches survey (2007) believe policies, handbooks and guidalines alone are not an effective way to deliver the necessary information to employees [20]. European Network and Information Security Agency [11] showed that it is simply unrealistic to expect most staff to read and absorb all the information they are bombarded with. These techniques serve a useful role in underpinning and reinforcing other awareness raising activities. However, alone they are not effective ways to deliver the necessary information to employees. As stated in [12], "policies alone do not constitute a sufficient awareness effort".

Currently the technical side of security in NLI is better developed than the human and organizational side. More needs to be done to increase in compliance with the IT security policy. Only having it in place is not sufficient, awareness must be raised among the employees of the needs for the policy and why it is important to follow it [12]. Without good security awareness from each employee, the validity and function of the implemented technical measures and published security policy decreases dramatically [3] [4] [5].

Therefore, the aim of the project is to build an efficient programme to raise information security awareness of NLI employees, improve their knowledge, and

change their attitude and behaviour so that the already established IT security policy is followed and the installed technical security measures are not circumvented and remain effective.

1.3 Justification, motivation and benefits

Most large companies including NLI have good technical security measures and solutions to take care of the information security today [13]. The weakest link in the security chain is therefore the employee, if employees are not aware of and thus not follow the available security measures as described in their organizations' information security policies and instructions, the validity of the security measures is lost [13]. The attitude and behavior of employees play an important role to an organization’s information security. Security measures and policies can be better implemented by executing a good information security awareness programme [14].

Stakeholders for such knowledge would typically be NLI’s security managers. It will also benefit to the security managers, or other people responsible for information security, in both small and large companies.

1.4 Research questions

Hansche (2001) [15] has successfully reported such work as developing and implementing an organizational IS security awareness program. According to Hansche (2001) [15], there are five important stages of an information security awareness programme: (1) setting the goal for the program, (2) deciding on the content of the program, (3) selecting delivery options, (4) implementation (as well as overcoming obstacles), and (5) evaluation of the program.

Mark Wilson and Joan Hash from NIST also proposed four steps to build a functional awareness program: design the program, develop or purchase awareness materials, implement the program, and post-implementation activities, which is shown in Figure 1 [14].

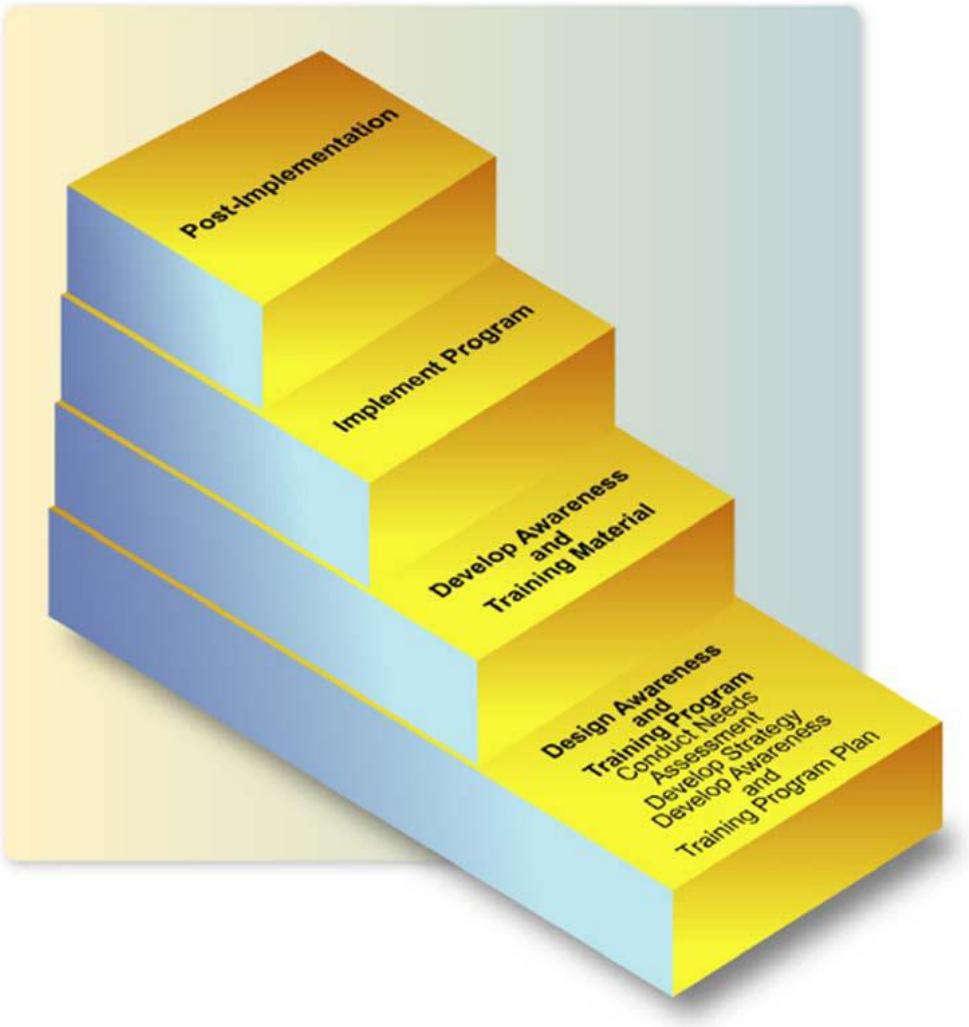

Figure 1 - Steps in the Creation of a Security Awareness Program [14]

- Awareness and training program design. This step includes activities like structuring the awareness and training activity, developing a plan, establishing priorities and funding the program.

- Awareness and training material development includes selecting the topics and curriculum for the campaign.

- Program implementation includes the activities of communicating the plan and delivering the awareness and training material.

- Post-implementation. This last step includes monitoring the effectiveness of the program. Formal evaluation and feedback mechanisms are pointed out as critical components of any security awareness, training, and education program. The feedback can be used to update the awareness and training program plan.

According to these two literatures, the content, delivery method and evaluation seem very important for an information security awareness programme. In order to build

efficient information security awareness programme for NLI, I defined three research questions:

1) What should the curriculum of an information security awareness programme for NLI be?

   The motivation of answering this question is to make sure the curriculums built in the information awareness grogramme are really needs for NLI employees. The content of an information security awareness programme is very important. We cannot randomly choose some curriculums. If some untargeted curriculums are set on the programme, the effectiveness of programme is lost. Getting answer for this question is a prerequisite when we start to design and develop an information security awareness programme.

2) How should the information security awareness programme be organized to effectively deliver the necessary information to NLI employees?

   The motivation of answering this question is to make sure all NLI employees can receive the necessary information efficiently. Appropriately organize the information and choosing efficient delivery materials are also important. No matter how completed the curriculum and content the programme have, if people cannot get it, the usefulness of progrmme also lost.

3) How should the effectiveness of the information security awareness programme be measured in NLI?

   Measuring the effectiveness of the information security awareness is a post-implementation step of an information security awareness programme, which is very important. The feedback can be used to update the awareness and training program plan. However, measuring is a very difficult task. An insufficiently measuring method cannot give reliable feedback.

To answer these questions I will first take a closer look at what has already been done by research in this area and then analysis what should be done in NLI.

1.5 Thesis structure

The overall method for the thesis structure is called P'HAPI method which is described in Moxnes 2009 [16]. The letters are short title for Problem, Hypothesis, Analysis, Policy and Implementation.

Chapter 1 introduction includes problem description, which is P in P'HAPI. The report set on section 1.2. Based on thorough study of literature formulate Hypothesis, this is H in P'HAPI which is worked as research question for this project. The report

set on section 1.4. The second chapter presents an overview of existing research focus on three research questions which I defined. The third chapter describes the research methods that I used to answer the research questions. The analysis section begins with chapter 4 Interview result and concludes in chapter 5 where results and analysis of the research work are presented. Policy in P'HAPI set on Chapter 6. It deals with what the results of the work means and provides recommendations or policy to NLI along with guidance for the Implementation (I in P'HAPI). The seventh chapter summarizes the research work and project. Chapter 8 is the last chapter which describes the future works for this research.

1.6 Keywords

Information security, Security awareness, Organizations, Employees

2. Review of state of the art

2.1 The curriculum of information security awareness programme

What kind of information security awareness curriculums have been used in different organizations?

In order to improve employee's information security awareness, Department of Child Support Services (works with parents and guardians to ensure children and families receive court-ordered financial and medical support) [17] have implemented an annual security awareness training programme. The goal of this programme is to enhance awareness and understanding of:

- Information Security Requirements
- Challenges and Vulnerabilities
- Responsibilities in accessing Child Support Service information
- Security Practices

This security awareness training programme includes the following training curriculum [17]:

Introduction of Information Security
This includes the definition of information security and the importance of information security.

Information and Assets
This includes information and assets classification, which will teach people what is public information and what is confidential information. This part also includes the introduction of basic laws and regulations.

Information Security Policies and Practices
This curriculum include how to protect confidential information and preventing unauthorized access, E-mail acceptable using rule, internet acceptable use policy, security management of user accounts and passwords, appropriate software Use, physical security, Remote Access and so on.

Information Security Incident Reporting
This includes how to recognize some basic and common risk and incident and how to immediately report it to related department and people.

The information security awareness programme can also set some curriculums modules which not focus solely on the information security, but information security are included in these modules.

The Wilh.Wilhelmsen (WW) Group, a Norwegian leading maritime industry group that delivers logistics solutions and maritime services worldwide, which similar as NLI's services. To raise individual awareness, in March 2008, the WW Group's own academy launched web-based security awareness training programme, named Individual Security Awareness (ISA). ISA consists of six modules, which include the following aspects of security curriculum [18]:

- Module 1: introduction. This module introduces various security and risk issues, defines the risks, and describes the security organization and security responsibilities.
- Module 2: information security. This module focuses solely on information security. It defines information security as confidentiality, integrity, and availability, explains the threats that may exist to information security, and shows how employees should handle different classes of information.
- Module 3: travel security. This module explains how to deal with the risks that may occur while traveling, such as mugging, street robbery, kidnapping, hotel fires, diseases, accidents, etc.
- Module 4: personal security. This module is about being able to take care of yourself, your colleagues, and your family, and discusses ways to deal with risks such as fire, burglary, kidnapping, loss of sensitive information, etc.
- Module 5: security of facilities. This module is concerned with the workplace. It is about protecting premises and detecting and preventing unauthorized entry to the premises.
- Module 6: internal/external communication. This module is about being aware of what and how you communicate, both internally and externally.

Even though only one module focuses solely on information security, information security is included in the other modules, too.

ISA gives an overall introduction to security and information security, but does not teach the details on how to for instance separate lure web pages from real web pages, or how to encrypt e-mail, or detect social engineering attacks. It only teaches the employees about the risks connected to these issues and other issues.

Mark Wilson and Joan Hash in his article "Building information technology security awareness and training program" proposed a significant number of topics can be mentioned and briefly discussed in any awareness session or campaign [14]. Topics include:

- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance

- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage – centralized or decentralized approach
- Social engineering
- Incident response – contact whom? "What do I do?"
- Shoulder surfing
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
- Timely application of system patches – part of configuration management
- Software license restriction issues – address when copies are allowed and not allowed
- Supported/allowed software on organization systems – part of configuration management
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain

Above are general topics and curriculums which an information security awareness programme should have, however, different topics and curriculums should be set different employee groupings. In the paper "Making information security awareness and training more effective" [19], Mark Thomson examines the importance of information security awareness programs in modern organizations. An expanded program is suggested to cater for more employee groupings in the organization. Security awareness and training programs should be aimed at three diverse employee groupings: top management, IT personnel and end-users.

- Top management has responsibility to provide the lead and impetus for the awareness program. In order to provide the necessary backing needed to make the program a success, they must believe in the need for information security first. Therefore, terminology and definitions, business continuity and legal issues are

among the topics are necessary to covered in this phase of the program.

- IT personnel are responsible for information system security which include identification, implementation and management of controls and also need ensure that the information security policy is adhered to. It therefore follows that this part of the program will be at a lower level and be more technical in nature. Some of the curriculum in this part of the program should include assignment of responsibilities, selection of risk analysis strategies and making security recommendations and so on.

- The end-users need information about the information security policy, guidelines and controls so that they can follow them in their work processes in order to ensure the work processes stay in security level. Possible threats, passwords, viruses and ethics are topics that should be covered in this part of the program.

2.2 Delivering of information security awareness

How should the information security awareness programme be organized to effectively deliver the necessary information to the employees?

The UK DTI information security breaches survey (2007) indicates several different techniques have used to make staff aware of information security issues and their obligation, which show in Figure 2:

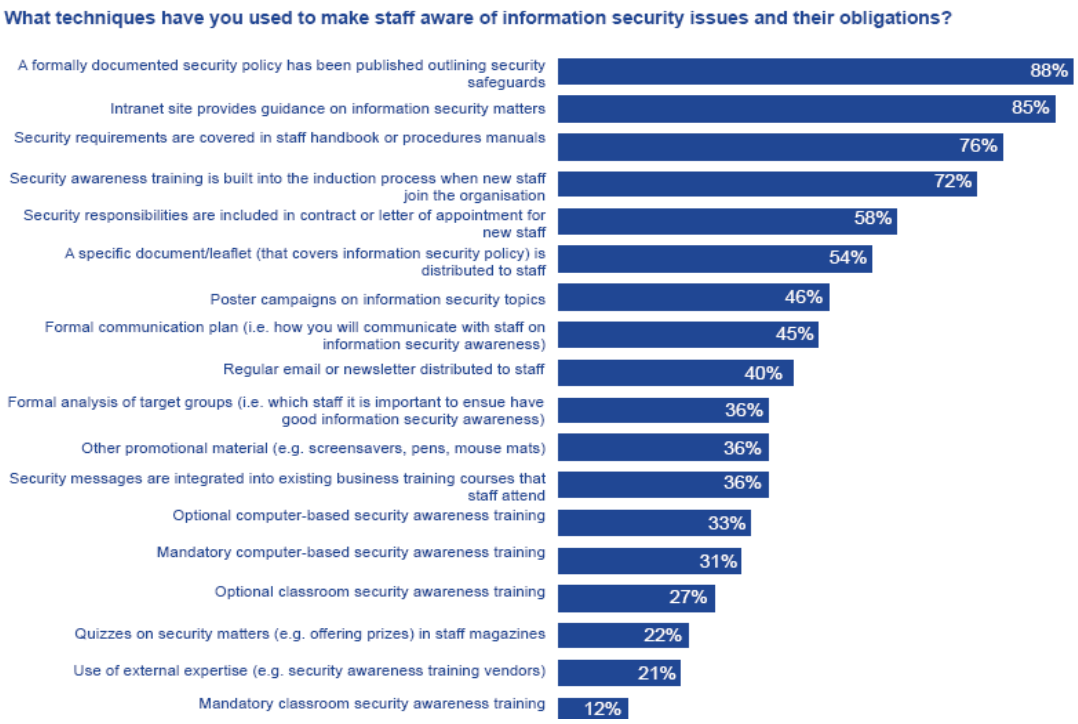

Figure 2 - Techniques to make staff aware of information security issues and their obligations [20]

Each of techniques shown in Fig. 2 has advantages and disadvantages. According to the Fig. 2, almost every respondent has defined their security policies, 85% of respondents have set up an intranet site that provides guidance to staff on information security matters. These techniques are low cost and so there is no reason not to use them. However, many respondents in the UK DTI information security breaches survey (2007) believe policies, handbooks and guidance alone are not an effective way to deliver the necessary information to employees [20]. European Network and Information Security Agency [11] showed that it is simply unrealistic to expect most staff to read and absorb all the information they are bombarded with. These techniques serve a useful role in underpinning and reinforcing other awareness raising activities. However, alone they are not effective ways to deliver the necessary information to employees. As stated in [12], "policies alone do not constitute a sufficient awareness effort". Charles Wood claims over 50 awareness-raising methods in his article. Some methods that are mentioned are:

- Stage vulnerability demonstrations (e.g. tiger-team attacks or penetration attacks).
- Give small prizes like free lunches to exemplary staff.
- Distribute relevant clippings from newspapers and technical magazines.
- Issue pamphlets or brochures to end users describing a code of conduct.
- Hang posters and signs to remind people (some also use stickers).

This list may be valuable to any company wanting to raise the awareness among its employees. One important document to distribute is the organization's IT security manual. One commonly used method is to put parts or all of the policy manuals on the Web. An experiment carried out in Sweden showed however that putting those documents on the Web not necessarily has a good effect [21]. The results from the study showed that the employees reading the security information on web appeared to have gotten better attitudes to IT security policy than the ones reading the information on paper. But in contrast, the self-reporting security behavior of the Web group was worse than the paper group. This was a relatively small experiment with only 28 persons answering two sets of questionnaires.

72% of respondents find the security awareness training is the most effective technique to deliver the necessary information to employees in the UK DTI information security breaches survey (2007), especially the classroom training also says an instructor-led training or face-to-face training. Though training and education are generally considered more effective than more formalistic measures such as procedures and controls [22], studies show that many organizations neglect to provide adequate training [23].

How to organize the training is also important. Common for most of training is one-way communication directed at a large population from authorities to single individuals by use of expert knowledge. On the other hand, several organizational researchers argue that bringing in local knowledge through processes that involve

employees is both necessary and efficient in order to attain all kinds of organizational change[24] [25] [26] [27]. It emphasizes the importance of employee participation, plenary reflections and group for improving employees' information security awareness and behavior. Eirik Albrechtsen and Jan Hovden [28] have experimented and evaluated this kind of work process which used in an information security awareness training programme. They conduct the intervention study which includes six workshops, involving a total of some 100 employees (15–20 participants per workshop) in Brønnøysund Register Centre. Figure 3 illustrates the contents and processes of a single workshop.

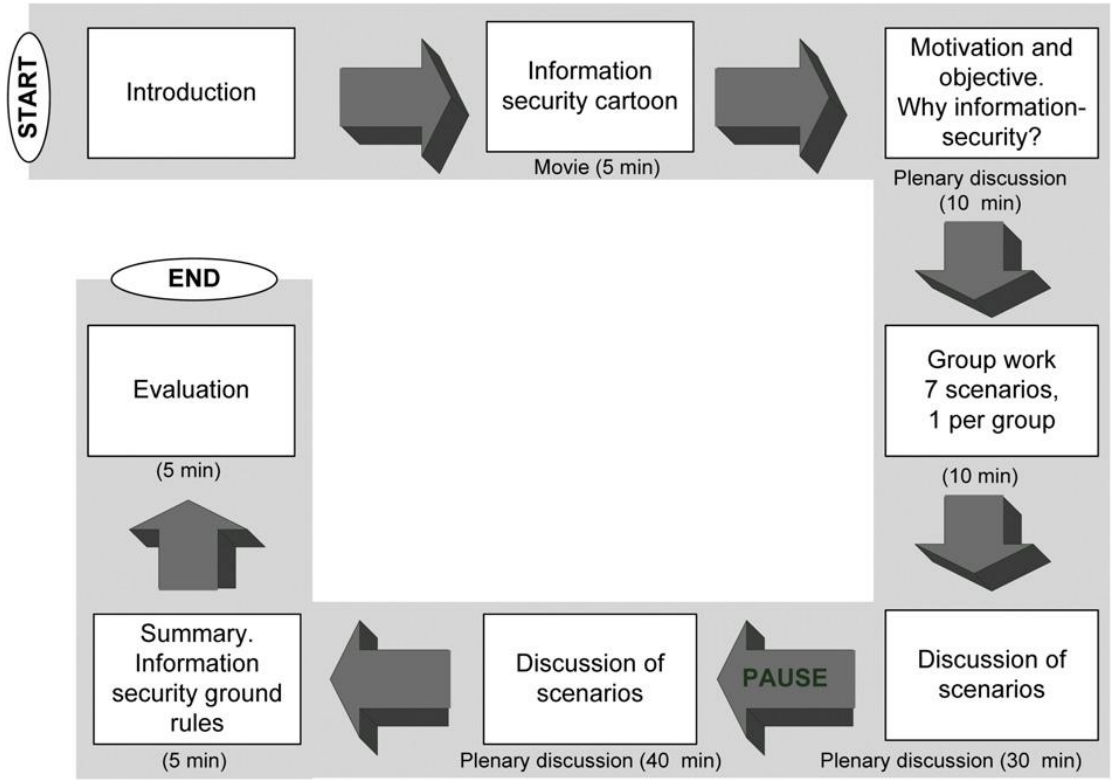

Figure 3 - Content and processes of an information security workshop [28]

Through the intervention study, they found that this kind of training processes produce significant information security awareness and behavior changes in short-term among users.

However, arranging and running these courses are difficult and high cost. On the other hand, getting sufficient time to take the training is also difficult for those busy business people in their work time today. Instead, some web-based training or non-web, computer-based training and e-learning seem more attractive to the organization. A European Network and Information Security Agency (ENISA) report gives an overview of training practices in 69 companies in nine European countries. Approximately, 50 percent of the companies used computer-based training [11]. Janne Merete Hagen and Eirik Albrechtsen through their survey found the significant short-time improvements in security knowledge, awareness, and behavior of members

by E-learning [18]. E-learning system normally includes some important information security curriculums which based on the company work processes, through a vocal introduction, uses pictures, music, and texts to illustrate different security risks, and then provides exercises that motivate reflection. There are also multiple-choice tests with immediate feedback, including the correct answers.

Computer based training is cost-effective, which have no limitation with time arranging, employees can arrange the time to take this training by their selves [11]. While there is an investment cost in setting up computer base training, once it is running, the delivery costs are very low [11]. It, therefore, lends itself well to ongoing training to a large population of existing users [11]. Consistency of delivery is usually better than with large classroom training programmes [11]. Building tests into the computer based training also allows some measurement of how well recipients have absorbed the training [11].

Mark Wilson and Joan Hash [14] proposed an Interactive video training (IVT), which is one of several distance-learning techniques available for delivering training material. This also is one kind of computer based training, which supports two-way interactive audio and video instruction. The interactive feature makes the technique more effective than non-interactive techniques, but it is more expensive and same as classroom training, the time arranging for employees also is the problem.

Mark Wilson and Joan Hash [14] also said that blending various training delivery techniques in one session can be an effective way to present material and hold an audience's attention. For example, showing videos during an instructor-led session allows the audience to focus on a different source of information. The video can also reinforce what the instructor has been presenting. IVT, web-based training, and non-web, computer-based training can also be used as part of an instructor-led training session. R.S. Shaw, et al. through their survey found that learners with multimedia material perform better at the comprehension level and projection level of information security issues than those single-media material [29].

According to the Fig. 1, Tips such as poster campaigns, promotional materials (such as pens, mouse pats, coffee cups) and blanket emails are each used by a significant number of respondents. Chapter 29 in the Computer Security Handbook [30] described the tips which used to delivery important information to employee in order to raise employee's security awareness. It proposed that posters should be colorful and should present a single message or idea", "Posters should be larger than standard letter size to stand out and gain attention", and "Posters should be changed or rotated regularly and placed at eye-level in many locations". Some other hints, like designing a security logo or mascot, are also described. Appendix A in this thesis contains examples of posters found on the Internet. Some of the posters must be bought while others are free to use.

Johnny Mathisen [31] in their master thesis found that most of Norwegian companies use different Poster to deliver awareness material to their employees with respect to information security. However, this method has a relatively short shelf-life and can be expensive to distribute across the organization. There is also a limit to how much information they can convey to the reader, and many people simply ignore them completely [31].

There is a special method called mandatory Information Security (InfoSec) exam, which has been used in a United States company—Aetna [9]. This method effectively delivered the necessary information to their employee and successfully improved their employee's information security awareness. This exam is updated annually to incorporate security topics that are relevant to Aetna's environment. Each exam builds on the strengths of the previous exam and attempts to correct obvious weaknesses. Each exam has a different focus and each module addresses a different security topic [9]. All employees must complete this exam every year. This method not only can force employee to remember their obligations and aware the information security issues but also cost low. The questions designing which can deliver the organization's really security needs on this exam is the challenge for this method.

Since the purpose of an information security awareness programme is that making users understanding the importance of information security and then behave accordingly [32]. The behavior of the employees is very important as it is what they really do that matters, and not what they know they should do. The most of delivery methods which I describe in above can improve employee's security knowledge, the more security knowledge the employee have the better security behavior employee may have. In order to more efficient improve employee's behavior some factors from social psychology can be applied in an awareness program [31]:

- Instrumental learning. If the attendees carry out the required actions specified in a previous session, then they are rewarded with a small "token". This would be applied by having the attendees evaluated after each session.
- Social learning. This refers to the observation of someone else and how they are rewarded for the correct behavior.
- Conformity. There will be groups of employees attending the awareness sessions, and group pressure can play a role in changing difficult individual's attitudes and behavior.
- Reciprocity. This refers to the returning of a favor. If the attendees feel that the presenter has done them a favor, they will be more likely to carry out the tasks.
- Commitment. A rule of society is that a person must stand by a commitment. By making attendees give a firm commitment to carry out the tasks specified, the likelihood is far greater that they will in fact do so.
- Self-persuasion. Forcing a person into a role-playing exercise where they are required to play a role that is in support of information security will often be more effective than the presenter trying to persuade them.

- The importance of the presenter. The importance of the person who presents the awareness program cannot be underestimated.

Skinner (1991) [33] also point when a behavior is followed by a reward, that behavior is more likely to be repeated by the same individual in the future under similar circumstances. Moreover, when a behavior is punished it is less likely to be repeated in the future. Hence, appropriately organize the delivery form social psychology or using some reward and punishment which combined with different delivery techniques is a good method to deliver the necessary information to the employees and change their behavior. However, design appropriate forms of reinforcement – reward and punishment are very important. Festinger and Carlsmith (1959) reported empirical evidence that significant rewards do not necessarily produce significant attitudinal change. This result is explained by the fact that large rewards can provide a justification for taking a position contrary to one's prior attitude. Therefore, a certain behavior reinforced with large rewards does not create dissonance between the recipient's attitudes and behavior, even though his behavior is not in line with his attitudes [34]. Instead, small rewards are worth considering when persistent behavioral changes are sought through rewarding [34].

On the other hand, albeit punishment is proven to be efficient in the context of information security [35], the impact of the possible negative side effects should also be considered. Driscoll 1997 found that the effectiveness of punishment seems to be short-lived [36]. In addition, punishment has side effects, which have been presented by [37], [38], [39], [40] including, e.g., fear of the punishing manager, reduced communication with the manager, escape behavior (e.g., avoidance of risk), aggressive behavior, anger, and learned helplessness.

In addition, it should also be remembered that effective forms of reinforcement – reward and punishment are personal. What reinforces someone may not work for someone else. Hence, successful outcomes depend on employees' preferences [40] [41] [42] [43] and managers need a basic understanding of how specific consequences might influence specific individuals. Effective use of reinforcement requires that this information is gathered from the employees [40].

2.3 Measuring information security awareness

How should the effectiveness of the information security awareness programme be measured?

In order to make a security awareness program add value to an organization and at the same time make a contribution to the field of information security, it is necessary to have a set of methods to study and measure its effect. Luc Pelfini presents the goal of information security awareness is to influence all employees and the whole organization towards security aware behavior of people, knowledge of techniques,

processes and attitude of organization, which is shown in Figure 4:

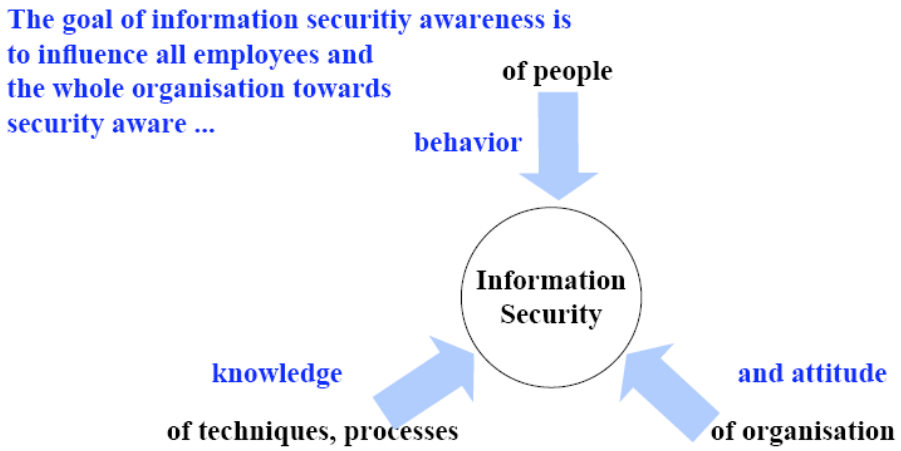

Figure 4 - The goal of information security awareness [44]

Therefore, when we intend to measure the effectiveness of an information security awareness programme, we are actually trying to measure and compare the corresponding changes in human knowledge, attitude and behavior and its impact on the organization's ability to reach its goal before and after implement this security awareness programme. Changing people's behaviors is the ultimately goal for an information security awareness programme. This is always hard to measure and thus it is a really challenging area for most organizations.

Different organizations adopt different methods of assessing the effectiveness of information security awareness activities. These include both quantitative and qualitative approaches. ENISA (European Network and Information Security Agency) [11] proposed four main approaches in general, each with different performance indicators:

1) Process improvement

This approach assesses the effectiveness of the programme by looking at its activities. In other words, these measures are around the effort put into the programme; they do not directly measure whether the end result has improved security. Possible performance indicators include: The extent of development of security guidelines, the extent to which the guidance is disseminated, the efficiency of the awareness process, the relevance of the awareness material, the effectiveness of the deployment of the security guidelines and so on.

The advantage of process improvement measures is that they are easy to define and to gather. The disadvantage is that they provide only indirect comfort as to whether the programme is making the organization any more secure.

2) Attack resistance

This approach focuses on measuring how resistant staffs are to a potential attack. Possible performance indicators include: The extent to which staff recognize attacks, the extent to which staff fall prey to attacks and so on.

The advantage of attack resistance measures is that they provide some direct evidence of the actual state of staff awareness. They tend to be good for impressing senior management on the need for investment in security awareness. The main disadvantage is that there are potentially many attack scenarios; any individual measure will be quite specific to the scenario it is testing. Simulated tests can also be relatively expensive to set up. A risk-based approach can help overcome these issues.

3) Efficiency and effectiveness

This approach focuses on the actual experience of security incidents within the organization. Possible performance indicators include: The extent of security incidents arising from human behavior, the extent of downtime arising from human behavior, the extent to which human behavior caused the organization's most severe incidents and so on.

The advantage of these metrics is twofold: firstly, the data can be gathered through the overall security incident monitoring that most information security groups do anyway; secondly, these statistics are usually of great interest to senior management. The disadvantage is that they do not necessarily give a true reflection of security awareness. It is not just security awareness that determines whether incidents occur; the extent to which attacks actually occur is the main factor. In the long term, the trend can be a good indicator of awareness. In practice, however, people often take action based on individual incidents; this may not be the most effective approach.

4) Internal Protections

This category is concerned with how well an individual is protected against potential threats. In other words, has the individual's awareness resulted in secure behavior?

Possible performance indicators include: The extent to which individuals incorporate security into the development and acquisition of systems, the extent to which individuals protect their data files, the extent to which individuals have allowed their systems to be infected by viruses or other malicious software, the extent to which individuals have allowed their systems to harbor inappropriate (e.g. pornographic) material or unauthorized (e.g. pirated) software and so on.

The advantage of these measures is that they provide direct evidence of staff behaviors. They assess whether awareness is making the organization more secure and avoid hypotheses or extrapolation. In addition, existing audits (by internal or

external auditors) may provide feedback here, effectively for free. The disadvantage is that any individual measure is quite specific to the behavior it is measuring. Often, an awareness programme aims to change many behaviors. This can result in many potential metrics. Each, in turn, may require investment in scanning tools or audits. A risk-based or rotational approach can help reduce the ongoing cost.

Most organizations use a combination of several approaches out of the above four. Blending different metrics enables them to build a well balanced scorecard for their awareness programme. Decisions are based on the overall picture, rather than on any single measure.

Overall, there was a good correlation between the metrics that were highlighted as most effective and the most popular metrics in actual use. Figure 5 bar graph shows the metrics which have been proved effectively at measuring the success of information security awareness activities found by ENISA through their survey in many different organizations. Blue bar represents the most effective and red bar represents the least effective. The result showed that five most popular metrics used by respondents are:

1) Number of security incidents due to human behavior. It can quickly show trends and deviations in behavior and can help understand root causes and estimate costs to the business. However it may not enough incidents to draw meaningful results and other factors may affect the incidents.
2) Audit findings. This metric generally conducted by independent and knowledgeable people who can provide third party assurance on behaviors. However, some significant areas of awareness may not be reviewed.
3) Results of staff surveys. If used before and after specific training, can be used to gauge the effectiveness of campaigns. If sufficiently large, can provide statistical conclusions on staff behaviors. However, need to be targeted at verifying key messages and have to be carefully designed since staff may respond with "expected" answers and not true behaviors.
4) Tests of whether staffs follow correct procedures. This is a very good way of actually measuring behavior and highlighting changes after training. However, we have to be carefully planned and carried out since could be breaches of employment and data protection laws and in order to get meaningful results, large of samples are needed.
5) Number of staff completing training. This need to decide what combination of classroom and computer-based training to use and consider what training to make mandatory. On the other hand, it may need to be tailored for different areas or regions and some regular, potentially costly updates also may needed.

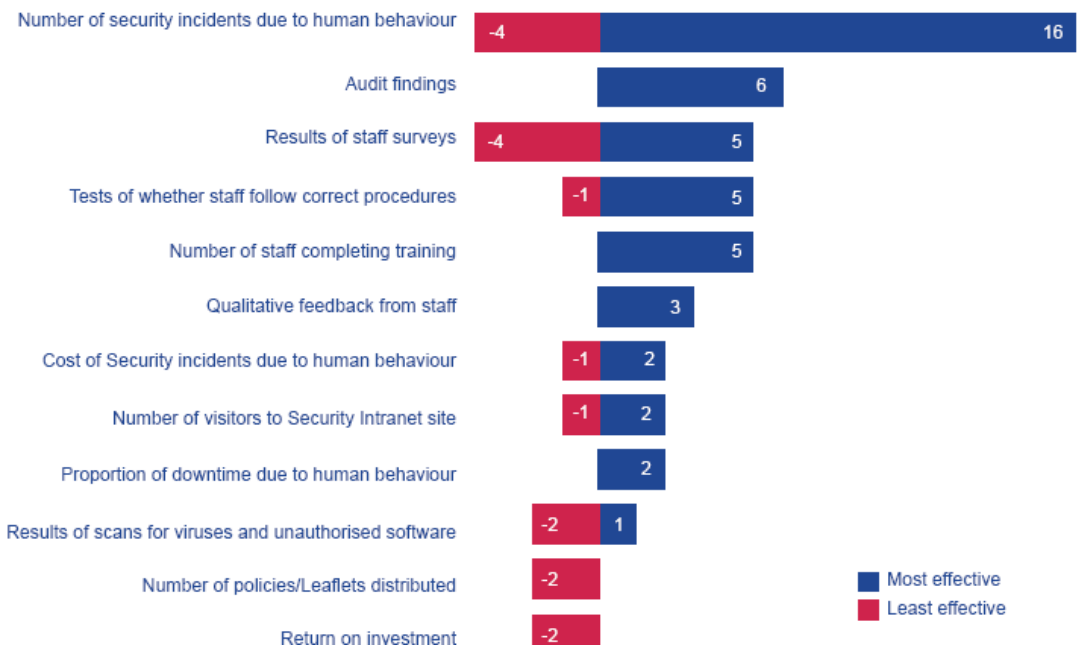

Figure 5 - The metrics have proved effective at measuring the success of information security awareness activities [11]

Johnny Mathisen has identified and defined nine security awareness metrics in his master thesis "Measuring information security awareness" through his survey which set in several Norwegian companies. These awareness metrics include [31]:

A-1. Percentage of employees having finished the necessary security training
A-2. Number of reported security incidents
A-3. Percentage of employees leaving their desk clean at the end of the day
A-4. Percentage of paper waste being shredded
A-5. Percentage of illegal traffic on the internal computer network
A-6. Percentage of weak user passwords
A-7. Number of hits to security web pages
A-8. Number of requests to security department
A-9. Customer satisfaction

The detailed definition and description are presented in Appendix B. Some of them has been successfully used in practical work already, such as A-1, Percentage of employees having finished the necessary security training, which can be found in the ENISA in their UK DTI information security breaches survey (2007) [20]. It was listed as one of the top five effective metrics and is showed in Fig. 5.

The NTNU/NSM survey [36] contains the example tool which is used to measure the human's behavior and attitudes. The tool was used in three different organizations in 2003. The questionnaire starts with questions about age, sex, and education etc. The participants are also asked if they have ever violated the security rules and if this was

detected. One important question about behavior is "If you found out that a colleague did something illegal (for instance theft or fraud) would you report this?" with the possible answers "Yes, always", "It depends on the situation and who it is" and "No". Table 1 show the four questions which used to measure the behavior and their possible answers.

Question	I	II	III	IV	V
Do you think of security when using the Internet?	Seldom think about security. Often give out sensitive information without checking the recipient. Usually click "OK" on questions.	Know there is a risk, but am not particularly careful. Download files and programs and give out personal information relatively uncritical.	Try to be careful. Do not give out personal information uncritical. Trust anti-virus programs.	Generally careful when I am on the Internet. Do not click "OK" without knowing what I am answering on. Check files for viruses.	Take all precautions. Do not give out sensitive information without encryption. Active use of firewall and virus control.
Which e-mail habits do you have?	Often open and forward e-mail with attachments without thinking about security.	Open relatively uncritical. Sometimes send sensitive documents in e-mail.	Have turned on security functions in the e-mail program. Careful when sending sensitive information.	Generally careful. Always critical to e-mail from unknown and control these for viruses. Send sensitive information encrypted.	Take all precautions. Control everything for viruses. Never send sensitive information unless being encrypted.
Are you careful when handling sensitive information?	Seldom think that sensitive information shall be handled with care.	Handling sensitive information is somewhat random. Lock the PC and collect printouts at once when I remember.	Careful when handling information and careful with what I talk about. Lack good system for handling of documents.	Am careful; locks PC and door to office, collect printouts at once and look after that I don't leave any paper.	Take all precautions. Have good control on storing of documents, electronically and on paper. Ensure obligation to maintain secrecy and is careful with what I say.
How do you take care of security when working remotely, for instance working at home or on travel with a portable PC?	Think little on information security. Save my work openly on own PC or on diskettes. Other persons (for instance family) have full access to my PC.	Seldom think that others can capture sensitive information. Save the work unprotected. Use e-mail or diskettes to transfer work.	I am aware that such work increases the danger for leaking information, but do nothing special to protect documents. Try to be careful.	I am extra careful, but could have been more systematic. Protect documents. Use file transfer or e-mail to send documents to work.	Take all precautions and have established good routines. Use encrypted connection to work and store my files at a secure server at work.

Table 1 - Questions about behavior from the NTNU/NSM survey [45]

One problem with such measurement is that the actual behavior may not be measured accurately by questionnaire alone, since there is the discrepancy between what people say and what they do. It is a possibility that some employees won't state the truth about their own attitudes or behavior [46].

The tool also contains three kinds of questionnaire methods. The discussion of the tool in [47] contains experiences from all the three pilot surveys:

Web-based questionnaire

This method can be used in different size of company, especially for those large companies which have many of branches. It is easy to make it possible for all employees to participate in the survey and can use statistical analysis of the results and thereby compare the results from different groups of employees. It is important to notice the danger of representing an abstract phenomenon as awareness as numeric values. The results can though, when used with care, give an indication of the level of awareness.

Paper-based questionnaire
It is better to use in smaller companies or departments. As long as a questionnaire is used the problems with validity will be the same as for the Web-based survey.

Personal interviews and group discussion process
It is possible to go deeper into each question and solve misunderstandings. But it takes longer time to conduct and some of respondents don't answer as honest in an interview as they would on a questionnaire. Same as personal interviews, the group discussion process also takes long time to conduct and it is also difficult to motivate all employees to participate in a rich discussion, since some of them may be busy with other meetings.

H.A. Kruger, W.D. Kearney in 2006 [48] proposed a prototype model for measuring information security awareness. It designed a tree structure to distribute the security problem. First, it classifies information security awareness into three dimensions: knowledge (what you know), attitude (what you think) and behavior (what you do). Each one of these dimensions was then subdivided into the six focus areas. Where appropriate and through consensus the six focus areas were further subdivided into specific factors, for example, the focus area Passwords was broken down into two subcategories Purpose of passwords and Confidentiality of passwords. Confidentiality of passwords was then further broken down into Writing down of passwords and Giving passwords to others. Each of factors was be allocated the different weights, since different regions have different influences on the overall awareness levels, It should contribute unequal proportions to the final awareness level measurement. An illustration of the tree structure developed is shown in Figure 6.

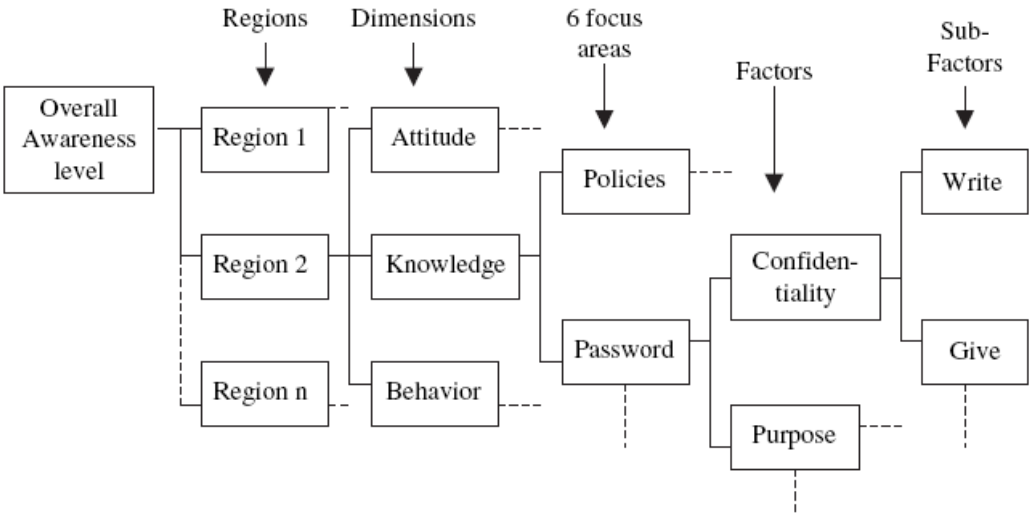

Figure 6 - Tree structure of problem [48]

It used a simple scorecard approach defined as $V(a) = \sum_{i=1}^{n} v_i\,(a) w_i$ to measure the level of awareness. *V(a)* is the overall value of alternative *a*, $v_i(a)$ is the value score reflecting alternative *a's* performance on criterion *i* and w_i, the weight assigned to reflect the importance of criterion *i*. This additive model is one of the most widely used forms of a value function and is described in detail in Belton and Stewart (2002) [49]. The performance, $v_i(a)$, was determined using a questionnaire. Thirty-five questions were designed to test the knowledge, attitude and behavior of respondents pertaining to the six main focus areas and their factors and sub-factors. Some of the questions were answered on a 3-point scale – true, don't know and false, while others only needed a true or false response. Figure 7 shows an example of a question in each of the three dimensions.

Example question to test *knowledge*:
Internet access on the company's systems is a corporate resource and should be used for business purposes only **1. True 2. False 3. Do not know**

Example question to test *attitude*:
Mobile equipment is usually covered with existing insurance cover and there is no special need to include them in security policies **1. True 2. False 3. Do not know**

Example question to test *behaviour*:
I am aware that you should never give your password to somebody else – however, my work is of such a nature that I do give my password from time to time to a colleague (only to those that I trust!) **1. True 2. False**

Figure 7 - Example questions [48]

The importance weightsw_i, was determined using the analytic hierarchy process (AHP). The AHP approach makes use of pair wise comparisons to provide a subjective evaluation of factors based on management's professional judgment and

opinion.

Questionnaire results and importance weights were processed in a spreadsheet application and output was finally presented in the form of graphs and awareness maps. Figure 8 contains one example of a graph showing the overall awareness level (as being average) as measured with the prototype tool. Similar graphs were produced for each dimension as well as for each focus area. The following awareness scale, which was defined in accordance with management's view on awareness performance, was used to explain the level of awareness:

Awareness	Measurement (%)
Good	80–100
Average	60–79
Poor	59 and less

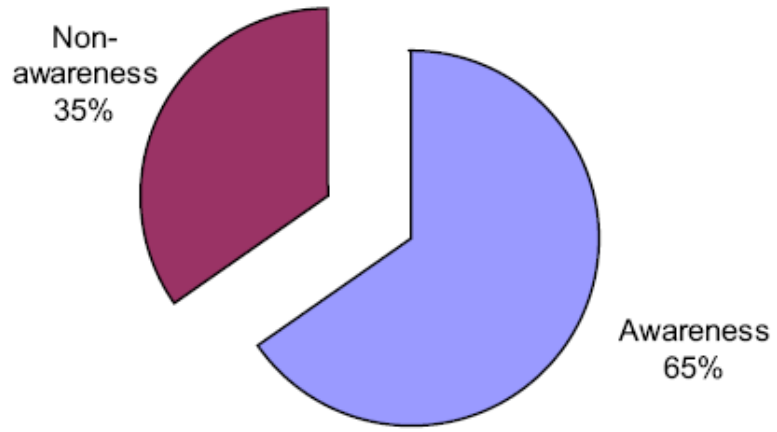

Figure 8 - Overall awareness level [48]

An important problem for this measurement is that the process of putting a number on such an issue as information security awareness. So what does the number mean? Is 70% security awareness good or bad? It could though be useful to compare such numbers with something else as a reference, for instance with the organization's number from last year.

2.4 Summary of literature review and discussion

According to the literature review, there are many different information security curriculums which have been used in different organizations. Such as information security and asset, information security polices, risk recognizing, incident reporting and so on. Some of curriculum modules which not focus solely on information security, but information security are included in these modules, such as travel

security can also be considered to set on the information security awareness programme.

There are also many delivery methods used in different organizations, such as face to face training, computer based training, information security exam, poster campaign, reward and punishment. Each method has its advantages and disadvantages, but currently, the computer based training/ E-learning seems as the most popular delivery method for most of organization. Since it has no limitation with time arranging, the delivery costs are very low once it is running, consistency of delivery and easy to measure its effectiveness.

In order to measure the effectiveness of an information security awareness programme, most organization are simply trying to measure and compare the resulting change in human knowledge, attitude and behavior and its impact on the organization's ability to reach its goal before and after implement this security awareness programme. Choosing and designing appropriate metrics is the important element for this measuring task.

Organizations would not randomly choose the curriculums on their information security awareness programme, and thus their curriculum is based on their specific need. Choosing appropriate form of delivery method also should base on the organization work processes and management system. As Wasim A said entirely using or copying educational curriculum and delivery method from other organization is flawed [50]. Different organizations have different security needs [50]. Making assumptions about our audience without adequate research can be dangerously misleading [50]. We might focus on entirely the wrong messages, distracting as well as irritating our target staff [50]. Therefore, the research should be conducted to understand NLI's specific needs before to decide what kind of curriculums of an information security awareness programme for NLI should be. Understand their work process and management organization through research to analyze what kind of methods are appropriate for NLI to deliver the necessary information to employees effectively.

3. Research methods

3.1 Choice of methods

In this project I intend to improve NLI employee's security awareness, knowledge, change their behavior via an appropriate programme. As Chapter 2 presented that the organizations should never randomly choose the curriculums on their information security awareness programme, their curriculum should be based on what they specific need. Choosing appropriate form of delivery method also should base on the organization work processes and management system. In order to understand NLI's specific needs, work processes and management system I did not use web-based surveys or mail surveys here, although they can offer access to groups or individuals who might be impossible to reach through more traditional forms of survey research [67][68][69] and they can also save time compared with interviews, Response rates also present problems when conducting web surveys. When compared with other survey instruments, web surveys produce lower response rates than interviews [70]. In order to get high response rate and also clearly and correctly understand work processes and information system in use in NLI, interview with their management s and employees is the research method that I selected.

McNamara said that interviews are particularly useful for getting the story behind a participant's experiences and it can pursue in-depth information around the topic [51]. Interviews may be useful as follow-up to certain respondents to questionnaires, e.g., to further investigate their responses [51]. Dapzury Valenzuela and Pallavi Shrivastava also presented the following characteristics about interview [52]:

- Interviews are a far more personal form of research than questionnaires.
- In the personal interview, the interviewer works directly with the respondent.
- Unlike with web-based survey or mail surveys, the interviewer has the opportunity to probe or ask follow up questions.
- Interviews are generally easier for respondent, especially if what are sought are opinions or impressions.

The main disadvantages of using an Interview are:

- The interviewer can affect the data if he/she is not consistent.
- It is very time consuming.
- It is not used for a large number of people.

Since the management are not a big amount employees in NLI, and they are also more clearly know the business work processes and information system in use than the general employees normally. Thus, using an interview for the research method is possible here and their disadvantages will not significant.

As I draw the research conclusions based on answers from interview in NLI, I have

used the qualitative approach which has defined in John W. Creswell's book "Research Design. Qualitative, Quantitative, and Mixed Methods Approaches" [53]:

In a qualitative approach, knowledge claims are primarily based on constructivist (i.e. socially and historically constructed meanings with an intent of developing a theory or pattern) and/ or participatory (i.e. issue- or change-oriented) perspectives. With the primary intent of developing themes from the data, open-ended emerging data are collected.

Qualitative methods are helpful not only in giving rich explanations of complex phenomena, but in creating or evolving theories or conceptual bases, and in proposing hypotheses to clarify the phenomena [54]. Besides, value of the qualitative research consists in validity of the information received; people are minutely interviewed so as the obtained data would be taken as correct and believable reports of their opinions and experiences [54].

Therefore, by interviewing and talking with employees especially their management in NLI combining with qualitative method to draw interview results, we can clearly understand the work processes, information system in use in different department in NLI, and then identify their specific security needs more correctly.

In addition, by literature study, I can find out what kind of information security content and curriculum which has been used in different organizations, what kind of delivery method they have used and how they measure the effectiveness of information security awareness programme. This work can help us get initial knowledge about an information security awareness programme. Integrate literature study and interview results I can then more clearly identify what kind of curriculum or training courses of an information security awareness programme for NLI should be and what kind of methods are appropriate for NLI to deliver the necessary information to employees effectively according to their work process and information system in use. In addition, we can also definite and identify appropriate measurement for NLI conditions.

3.2 Interview

3.2.1 Profile of interview

Three NLI companies are interviewed (NLI business support AS, NLI solution AS and NLI Alfred Andersen AS). NLI business support AS is one service based company, many economic and finance service are provided in this company. Therefore, the interview results from this company are very important for my project. NLI solution AS is one technically oriented company which includes two sub engineer companies. NLI Alfred Andersen A is one production oriented company. Those three companies are the main business parts of whole NLI.

22 key persons in NLI are participated the interview, mainly CEO, project manager, IT technical people, QA and Finance manager and so on. In order to get the contact information from them and motivate them to participate in the interview, I get help from NLI IT manager.

Two phases of interviews are used. First interview I did in the first or second week of March, second interview be implemented in the beginning of April. The reason why divide interviews to two phases is that I intended to find more information and improve the questions after the first interview. Since some additional questions need ask for the people who work on different position in order to get more accurate information. The interviews are recorded by audio recorder to facilitate easier analysis.

3.2.2 Interview questions

According to Stinger (1999) [55], a major problem with interview is that questions are easily influenced by the researcher's perceptions, perspectives, interests, and agendas. To avoid this, I used an approach proposed by Spradley (1979) [56]. This approach suggests that the researcher ask questions that are relatively neutral. This is necessary in order to diminish the extent to which participants' perceptions will be governed by frameworks of meaning unintentionally imposed by the researcher.

Spradley's (1979) [56] approach advises the researcher to start with grand tour questions that are sufficiently global to enable participants to describe their situation in their own terms (e.g., "what kind of information is critical to the business."). When the researcher wants to gain more detailed information about issues already covered, he can present a set of sub questions that focus on concepts already presented (e.g., "How often does this happen? Occasionally or all the time?) In all phases of the interview, the researcher should take a neutral stance and write down or record the responses as accurately as possible.

The first interview is conducted in NLI solutions AS. Six main questions with some sub questions are designed. About 30-40 minutes long interviews for each of people. The questions and purpose of these questions which is shown in as follows:

1) In your opinion, what kind of information is critical to the business?
    a) How is this information used in the business 'work processes? (In other words, why is this information critical to the business?)
    b) How sensitive is this information? (ex, customer data, business plans)

Purpose: Identify the information which is central to performing the business' mission and understand how the business' critical information is used to perform the business' mission.

2) Which information systems is the business using? (ex: what kind of software,

tools are you using to store, publish and process information）

Purpose: To understand how critical information is handled and what kind of systems are used to store and process the information.

3) Are mobile devices used in the business' work processes?
   a) If so, are these devices used to store, send and receive critical information?
   b) What kind of mobile devises are being used?
   c) Is the use of mobile devises increasing, staying the same or declining?

Purpose: Understand how they use mobile devices for work and whether awareness training has to target mobile devices.

4) Do external contractors and/or customers use the business' information systems and networks?
   a) How often does this happen? Occasionally or all the time?
   b) Are there a large amount of external people connecting to the information systems or is it only a few people?

Purpose: Understand to what extent awareness training may be necessary for contractors and customers of NLI businesses.

5) Are there any policies, guidelines or routines regarding information security in the business?
   a) If yes, give some examples
   b) How is information and information systems protected internally?
   c) How is information and information systems protected externally?

Purpose: Understand how protective information security measures are being used throughout the business and in communication with customers.

6) Last, we would like your opinion on how to improve the information security work in NLI. Do you have any suggestions as to how the information security of NLI could be improved both in the technical aspects and management aspects?

Purpose: Get feedback from them, which may helpful for me to get ideas for how to design the information security awareness programme.

7) Additional question, how long have you worked on this position?

Purpose: Get knows the background of interviewers to identify whether they are familiar with the whole work process in NLI. Make sure more accurate of feedback.

The second part of interview is conducted in NLI business support AS and NLI Alfred Andersen AS. According to the first part of interview, we found it is unnecessary to change or add more questions to the second part of interview, since we got everything we want from the interview, the main point to the second part of interview we just want find the answers from people who work on different department and different positions, especially the answers from IT technical people, financial people which are

very important for this interview, since they hold and responsible for lots of critical and sensitive information.

4. Interview results

The first part of interview conducted in NLI solution AS. Seven managers from different departments attended my interview, which include one CEO, four project managers, one document controller and one quality assurance (QA). When I ask the first question about what kind of information is critical to the business, how is this information used in the business' work processes and how sensitive is this information, the answers showed that the business plan and strategies, project plan, contract, price, customer data are the critical information for NLI. Almost all seven managers mentioned about these information, they said these information related to the whole business competitiveness and reputation, especially the business strategies, project contract and customer data which are very sensitive. The CEO described as follows: *the business plan and strategies which covered the whole business direction, goals, and work process. The project part which include the project run process, quality requirement and how can be able to earn money and so on. This will influence the development of the whole business.*

The second part of interview conducted in NLI business support AS and NLI Alfred Andersen AS. Fifteen managers from different part attended my interview, which include IT technical people, financial and purchase people, HR managers, project managers and document controller. The IT technical people said that *"Business critical information would be information such as username and password, contracts or detailed sketches / blueprints related to projects issued to NLI corporations. Since Usernames and password are used to gain access to all NLI data. Contracts and sketches are critical information concerning the business and their partners when making bids on new projects. If this information gets in the hands of the wrong person it could be exploited to gain intelligence on NLI and how they operate. Data could be sold to competitive business and used as industrial espionage."*

The financial people said that project calculation document, salary, payment are the critical information in the business. HR manager said that personal data from employees are the critical information. The project manager said that project contract, price and run processes are the most critical information in their work field. The purchaser said that suppler list and material of project are also very critical information in the business. They said all these information are also sensitive, which related to the whole business competitiveness, development and reputation.

The second question is that ask them which information systems the business is using. For example: what kind of software, tools are you using to store, publish and process information. The answers showed that these three companies and even the whole NLI business use unified information system. They depends mainly on the Microsoft Office portfolio and ERP systems as Microsoft Dynamics Navision. Navision is the most critical software as this system stores everything from bank accounts to social security numbers. Also, payroll software such as Huldt & Lillevik stores critical

information which could be used in identity stealing etc. SharePoint and Citrix are the main servers to share and publish information internally in NLI. They also use email, outlook to delivery, receive information both internally and externally. People with different user right to deal and process different information internally and externally.

The third question is about mobile devices. The mobile devices, mainly Mobile phones and laptop are used for almost every employee in NLI. Almost every employee holds VPN service which can work out of office. They also use these kinds of Mobile devices to store, send and receive critical information internally and externally and also these kinds of devises using are increasing in NLI. All managers think this is necessary trends for NLI. It makes the work more convenient, saved time and improved work efficiency.

The fourth question concerned about the external contractors. There are almost 30 to 40 present of external people connecting to the NLI information systems, mainly are the different consultant who work for NLI different service. They access and use the system everyday almost same as the normal NLI employees but different people have different user right.

The fifth question is asking them whether there have any policies, guidelines or routines regarding information security in the business. The answers showed that except the IT security policy, they don't have any other policies, guidelines or routines regarding information security in the business yet. The IT security policy described the use of IT equipment and guidelines on how to store and use company equipments, email, internet and so on. The policy is required to be read by every employee in NLI and an agreement to follow it must be signed afterwards. People who work on different position have different user right, when they access information system, they need enter their user name and password both in office and out of office. The external contractors also need sign the confidentiality agreement same as the normal employees and also have limited access right when they use the business' information systems and networks.

The last question intended to get some opinions and suggestions about how to improve the information security work in NLI both in the technical aspects and management aspects. The IT technical people said that more information should set on IT policy, doing more tests to check if we need to focus more on the information part. Also, need to update and develop new routines on how inform new personnel on the current policy. The CEO and three project managers and one QA presented that appropriate training courses for information security should be set in NLI. Other two project managers and one financial person suggest that the programme should not too strict, a trader off is very important. Others just said have no idea for this currently, but all of them think that information security is very important in NLI.

5. Analysis

5.1 The curriculum of information security awareness programme

There is a lot of critical information which is related to the whole NLI business competitiveness, development and reputation in NLI according to the answers from interview. In order to protect NLI critical information without disclosure, the employee should first know what public information is and what confidential information is in business or at least in their work position. Therefore, some training curriculums which include information and assets classification should be included in the information security awareness programme for NLI. These curriculums will teach staff and managers to aware and understand what public information is and what confidential information is, how and why they should classify their own data in this manner (Public, sensitive and confidential).

From NLI IT technical people's point of view, username and password are also critical information in business, since usernames and password can be used to gain access to all NLI data, which could be sold to competitive business and used as industrial espionage. Therefore, some curriculums which include password setting, protection are also very important to put on the information security awareness programme for all employees. The similar training curriculums which were also set on the Department of Child Support Services [17] that I have already described on the chapter 2. Mark Wilson and Joan Hash in his article "Building information technology security awareness and training program" also motioned these similar curriculums, which are the basic information security knowledge that all employee should be aware in a company.

Microsoft Dynamics Navision is the main information system the NLI use. Also, payroll software they use Huldt & Lillevik stores critical information. SharePoint and Citrix are the main servers to share and publish information internally. They also use email, outlook to delivery, receive information both internally and externally. In order to better protect those information systems in use, employee should understand how to securely use these systems. Thus, some training curriculums which include basic guidelines or routines for how to securely use Microsoft Office portfolio and Microsoft Dynamics Navision, SharePoint and Citrix server, how to security use email to delivery information internally and externally should also be considered set on NLI information security awareness programme for all employees. On the other hand, some specific training curriculums, such as how to maintain and improve the SharePoint and citrix server and Navisjon database and how to distribute user right for users should also be set on the NLI information security awareness programme for IT technical peoples in order to protect information system without damage from hackers or other fraudulent. In addition, the people who work on financial department then should be extra trained for how to use Huldt & Lillevik payroll system in the security level.

Mobile devices, mainly mobile phones and laptop are used for almost every employee in NLI and also this trend is increasing to make the work more convenient and efficient. However, there are many security risks along with those mobile devices [57]. Thus, some training curriculums which include how to securely use mobile devices, how to securely holds VPN service when work out of office, how to security use mobile devices to store, send and receive critical information internally and externally should be covered in NLI information security awareness programme for all employees. On the other hand, the technical people should be trained how to maintain mobile devices security and how to monitor and fix mobile devices security vulnerabilities.

Since a large amount of external people connect to the NLI information system, it seems necessary to set some training curriculums which include how to set limited user right for external people in the programme for IT technical people.

IT security policy is only one policy that NLI currently has, in order to ensure all employees can follow them in their work processes, some IT security policy and practice curriculums should be covered in their security awareness programme. This will include broad range of topics, such as introduction of security threats, viruses ethics, and incident reporting, how to security use email and internet and so on. Chapter 2 reviewed that almost every organization's information security awareness programme includes these curriculums. On the other hand, since people who work on different department and different position have different access right for some critical information, they are responsible to make sure the confidentiality and integrity of these information without disclosure to other people, therefore, training people who work on different position to clearly know their responsibility are also very important.

5.2 Delivering of information security awareness

Chapter 2 described different ways that information security awareness programme can be organized to effectively deliver the necessary information to employees. We can summarize those methods into four sections: (1) Information security awareness training, (2) Information security awareness tips and poster campaigns, (3) information security exams and (4) punishment and reward. Information security awareness training can also be divided into: class room/face to face training, computer-based training (both web-based and not web-based training).

According to the interview, I found that all NLI companies use a centralized information system, the information resources and decisions regarding their acquisition and control are concentrated in one particular business unit (NLI Business support AS) that provides IT and information security services to the whole firm. Even though NLI have 16 companies, there is no IT department or people who assigned to be responsible for information security in each company. According to

this situation, class room/face to face training seems not appropriate for NLI, although there are 72% of respondents said that face to face training is the most effective technique to deliver the necessary information to employees in the UK DTI information security breaches survey (2007) [20] which described in chapter 2, this could be due to the perceived cost of arranging and running these courses, since 16 NLI companies which are located in different area in Norway, course arranging is a big challenge. Time is a precious commodity to busy business people, getting sufficient time to cover training needs maybe very difficult for NLI.

Instead, some computer based training or e-learning are more appropriate for NLI, since it is cost-effective, and have no limitation with time arranging, employees can arrange the time to take this e-learning by themselves. Compared with face to face training, the computer based training or e-learning can also set a large amount of contents and knowledge through diverse way to deliver employees, which are more attractive. For example: The Wilh.Wilhelmsen (WW) Group, a Norwegian leading maritime industry group that delivers logistics solutions and maritime services worldwide, which similar as NLI's services. To raise individual awareness, in March 2008, the WW Group's own academy launched web-based security awareness training programme, named Individual Security Awareness (ISA). This system includes some important information security curriculums which based on the company work processes, through a vocal introduction, uses pictures, music, and texts to illustrate different security risks, and then provides exercises that motivate reflection. There are also multiple-choice tests with immediate feedback, including the correct answers. Janne Merete Hagen, Eirik Albrechtsen measured the effectiveness of this delivery technique in WW Group, they found the significant improvements in security knowledge, awareness, and behavior of members by this E-learning system [18]. In order to make sure the participation, a web-based exam—mandatory information security exam which can be considered to combine the E-learning to run in NLI. This type of delivery method has been used in a United States company—Aetna and effectively delivered the necessary information to their employee and successfully improved their employee's information security awareness [9]. Chapter 2 described this exam which is updated annually to incorporate security topics that are relevant to Aetna's environment. Each exam builds on the strengths of the previous exam and attempts to correct obvious weaknesses. Each exam has a different focus and each module addresses a different security topic. On-line registration requires each user to participate the web-based information security training and read a condensed version of the company's Information security policy and to electronically agree to comply with that policy before the user can proceed with the exam. All employees must complete this exam every year. The monitoring tools should be set to remind those employees who had not yet completed the annual mandatory information security exam. The main advantage for this exam combined with web-based training is that it not only can force employee to remember their obligations and information security issues, knowledge which learned from training but also deliver consistently, once it is running, the cost is much lower compared with face to face training [11].

Some information security awareness tips and poster campaigns, promotional materials (such as pens, mouse pats) and blanket emails can be also considered to use in NLI, but should not be the main method, just as an adjunct. The advantage of this delivery method is that it uses something popular and useful to attract attention and with simple messages written in the popular or common work place where people can easily see, which can always remind people to take care about security. The UK DTI information security breaches survey (2007) [20] described in chapter 2 showed that these kinds of delivery techniques are used by a significant number of respondents, however, many respondents had used these techniques in the past but have now abandoned or scaled back their use, since they have a relatively short shelf-life and can be expensive to distribute across the whole companies. The cost is also the important part that NLI take care about now, according to the interview from NLI CEO and IT Manager. In addition, this technique also has a limit to how much information they can convey to the reader, many people simply ignore them completely in most of time. Therefore, it is better to just consider this method as an adjunct to combine with other method to run in NLI under the funds permitting.

Reward and punishment are worth to change employee's behavior, which can also be considered and combined with other delivery method to run in NLI. As Skinner's (1991) [33] point, a rewarded user may change his attitude in the direction of greater compliance with IS security policies and instructions. Moreover, a punished user may also change his attitude or behavior from negative side into positive side. However, the impact of the possible negative side effects of punishment should also be considered. Such as fear of the punishing manager, reduced communication with the manager, escape behavior (e.g., avoidance of risk), aggressive behavior, anger, and learned helplessness which presented by [42], [43], [44], [45]. Design appropriate forms of reward and punishment and severity of the sanctions are very important. Effective use of reinforcement requires that this information is gathered from the employees [40]. On the other hand, it is important that make it publicly known that users' information security behavior is monitored and that violators of information security instructions will be punished. This requirement stems from the general deterrence theory [15]. At the same time, Estes (1972) proposed that people must have an expectation of being rewarded in order for reinforcement to work [59]. By this token, it is important to present the existence of the system of rewards and how rewards can be earned. Moreover, to support the general deterrence theory, all punishments – but not necessarily the recipients should be made publicly known. This demonstrates that violators against information security instructions can be caught and will be punished. In addition, an effective system of rewards should not limit the number of rewarded users when the goal is wide-ranging organizational change [60]. Everyone who achieves the targeted goals should be rewarded.

5.3 Measuring information security awareness

As chapter 2 presented: when we intend to measure the effectiveness of an information security awareness programme, we are actually trying to measure and compare the resulting change in human knowledge, attitude and behavior and its impact on the organization's ability to reach its goal before and after implement this security awareness programme [31]. Chapter 2 also described and analyzed advantages and disadvantages of some different approaches which have been used to measure the effectiveness of information security awareness programme in early study and some of organizations. These are very good references and examples for NLI, but not all approaches are appropriate for NLI. Selecting or designing appropriate metrics is the important element for this measuring task. Chapter 2 described advantages and disadvantages of different metrics which defined and used in early study or some organizations. Metrics identifying and designing in NLI should base on the analysis results of the first and second research questions.

From the analysis results of the first and second research questions, the results of quizzes and staff survey and Audit finding approaches can consider to use in NLI condition. Comparing the results before and after computer-based training gives a true reflection of people's understanding and helps gauge the effectiveness of this computer-based training. Quiz responses also often highlight weaknesses in specific areas. This has enabled management to fine-tune training messages or produce targeted sessions to address any weaknesses. It should be noted that target at verifying key messages, this should depends on key messages and have to be carefully designed since staff may respond with 'expected' answers and not true behaviors [46]. Combined with Audit finding by internal or external auditors, the result of measuring will become more precise. Since the result of audit finding shows the real behavior, but some significant areas of awareness may not reviewed if just use this method alone [11].

From the analysis results of the first and second research questions, I can also identify the following three metrics that can be used to measure awareness and behavior in different ways for NLI:

B-1.Percentage of individuals tested on the security policy (passing and failing)
B-2.Percentage of employee recognizing critical information in business
B-3.Percentage of users recognizing a security event scenario

This list is not meant to be a complete set of awareness metrics which can be used in NLI condition, but hopefully they may serve as examples and give inspiration to other metric definitions.

When defining the metrics, I have used the template (see Table 2) defined in [31]. The definitions are shown in Table12 through Table 14 in Appendix C, and they show that

it is possible to measure at least some aspects of awareness and behavior among the employees in NLI.

Metric ID	*The unique number for the metric.*
Name	*Name of the metric (short form).*
Description	*Description of the security metric.*
Metric	*Description of what we are measuring with this metric.*
Formula	*Describes the calculation to be performed that results in a numeric expression of a metric.*
Purpose	*What is the goal of measuring with this metric?*
Frequency	*How often should the measurements be done?*
Indicators	*Information about the meaning of the metric and its performance trend. If possible, the performance target should also be set.*
Cost	*What affects the cost of measuring with this metric?*
Validity	*Evaluation of the possibility that we in fact not measure what is stated in Purpose of the metric.*
Reliability	*Evaluation of the possibility for incidental errors in the measurement with this metric.*

Table 2 - Template for definition of a security metric [31]

6. Proposed information security awareness programme for NLI

After analysis, I summarize and propose an information security awareness programme for NLI, which described in Figure 9:

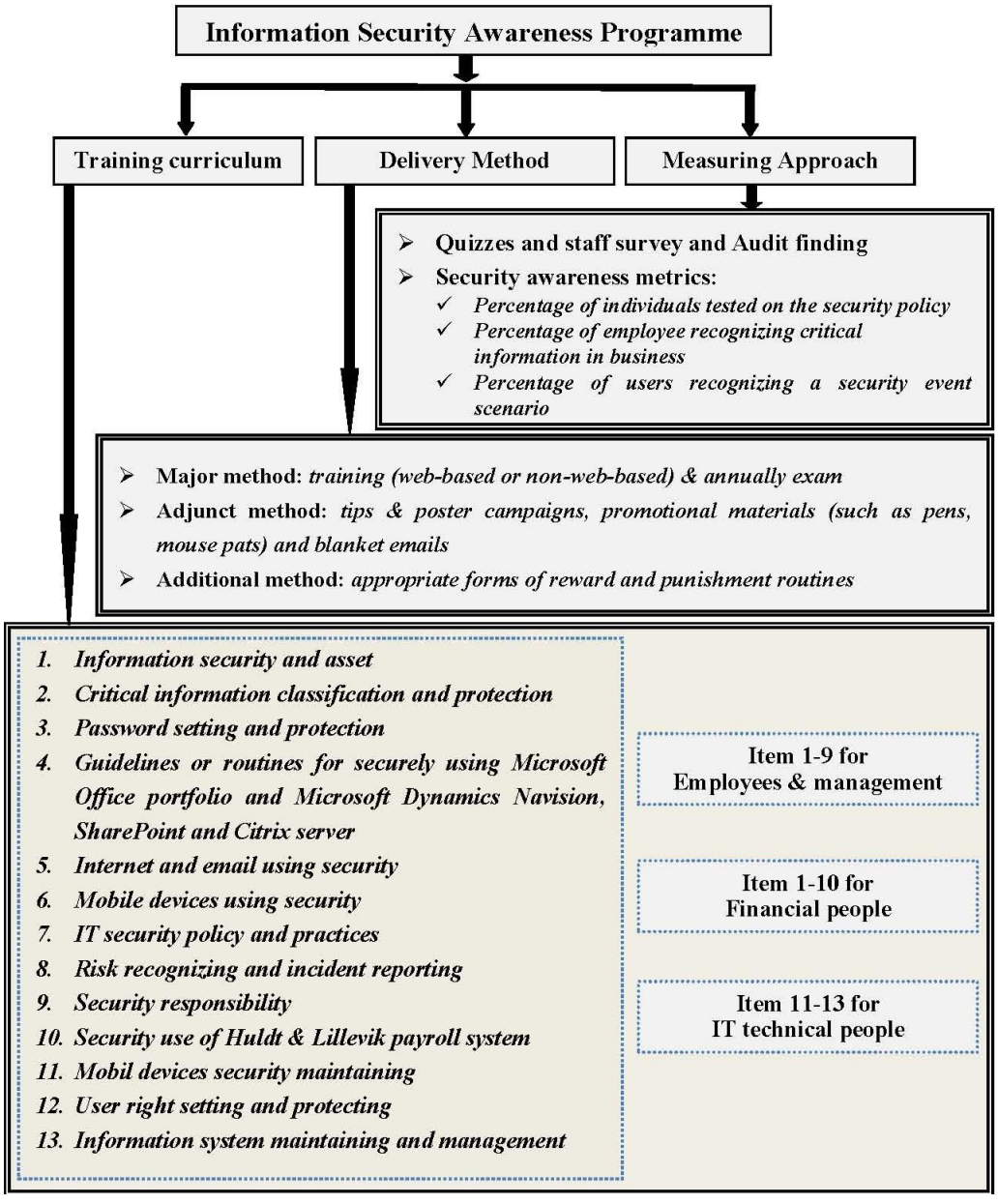

Figure 9 - Information security awareness programme for NLI

6.1 The curriculum of information security awareness programme

6.1.1 Training curriculum for all NLI employees include management

1) Information security and asset
2) Critical information classification and protection

3) Password setting and protection
4) Guidelines or routines for securely using Microsoft Office portfolio and Microsoft Dynamics Navision, SharePoint and Citrix server,
5) Internet and email using security
6) Mobile devices using security
7) IT security policy and practices
8) Risk recognizing and incident reporting
9) Security responsibility

6.1.2 Training curriculums for NLI IT technical people

1) Mobil devices security maintaining
2) User right setting and protecting
3) Information system maintaining and management

6.1.3 Extra training curriculums for financial people

1) Security use of Huldt & Lillevik payroll system

6.2 The delivering methods

Computer based training which include both web-based and non-web-based training combined with an annual web-based mandatory information security exam is a best delivery methods compared with others.

In addition, some of Information security awareness tips and poster campaigns, promotional materials (such as pens, mouse pats) and blanket emails can be also considered to use in NLI, but just considering this method as an adjunct which used to combine with other method to run in NLI under the funds permitting.

Appropriate forms of reward and punishment are also worth to consider combining with other method to run in NLI. But remember to understand employee's preference to design the forms this method, and make it publicly known that users' Information security behavior is monitored and that violators of Information security instructions will be punished. Moreover, not limit the number of rewarded users when the goal is wide-ranging organizational change [60]. Everyone who achieves the set goals should be rewarded.

6.3 Measuring information security awareness

The results of quizzes and staff survey and Audit finding approaches are the best way that NLI can consider to use for measuring effectiveness of information security awareness programme.

Selecting or designing appropriate metrics is the important element for this measuring task. Possible security awareness metrics which can be considered use in NLI:

B-1.Percentage of individuals tested on the security policy (passing and failing)
B-2.Percentage of employee recognizing critical information in business
B-3.Percentage of users recognizing a security event scenario

This list is not meant to be a complete set of awareness metrics which can be used in NLI condition, but hopefully they may serve as examples and give inspiration to other metric definitions. The detailed definitions are shown in Table12 through Table 14 in Appendix C, and they show that it is possible to measure at least some aspects of awareness and behavior among the employees in NLI.

7. Conclusion

There is an increasing focus on information security issue for most companies around the world. The technical side of security in many companies including NLI is developed very well. The weakest link in the security chain is therefore the people factor. The "people factor" - not technology – is a key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this "asset." A robust and enterprise wide information security awareness and training programme is paramount to ensuring that people understand their information security responsibilities, organizational policies, and then acts accordingly.

I have done an interview in NLI and then understood their management organization, work processes and information system in use. Based on results of interview combined with some literature study, I analyzed and provided the main recommendations for NLI to build a successful information security awareness programme. These include what the curriculum of an information security awareness programme for NLI should be, how the information security programme should be organized to effectively deliver the necessary information to NLI employees and how the effectiveness of the information security awareness programme should be measured in NLI. Therefore, NLI can consider following these recommendations to build and implement exact information security awareness programme in practice later.

Especially in section 5.3 in chapter 5, I have identified and defined three security awareness metrics which used to measuring information security awareness programme for NLI based on the inputs from the interviews and available methods and templates. These cover different aspects of information security awareness, as for instance security policy, critical information and security event scenario. The set of metrics is not complete in any way to measure the awareness and behavior for NLI, but hopefully they may serve as examples and give inspiration for the definition of other similar metrics.

8. Future work

Chapter 6 provided the answers for the research questions. These answers just some recommendations, NLI should consider following these recommendations to build and implement exact information security awareness programme in practice later and test its effectiveness. However, before implementing this information security awareness programme, I suggest NLI establish an information security organization first or at least should arrange some experts who work for the information security in company. This organization or expert is responsible for making information security awareness training plan, publishing training information for employees, monitoring compliance, building, measuring and updating information security awareness programme.

How to build the information security organization, and distribute responsibilities for people who work on different position in this organization, how to make information security awareness training plan has not presented in this project, but many articles have described the general guideline for these issues. For example, United States Company—Aetna [9] have established a very good information security organization in company, which is a very good example for NLI. Mark Wilson and Joan Hash in their article "Building an Information Technology Security Awareness and Training Program" [14] have provided guidelines for building and maintaining a comprehensive awareness and training program, which included how to making information security awareness training plan and how to distribute responsibility for people who work on different position in the security organization of a company, it will also helpful for NLI.

The defined metrics are supposed to be used in the practical work with awareness in NLI also. To see if this is possible and expedient, the metrics must be tested in practice. Such testing has not been done in this project, but it is considered as a natural follow-up to this report. I suggest that some or all of the metrics are used to measure the existing level of awareness, attitudes, and behavior in NLI. From this it would of course be expected to find out if the metrics could be used or not, and another output could be the identification and definition of many new awareness metrics.

Bibliography

[1] Schlienger T & Teufel S (2002) IS security Culture: The Socio-Cultural Dimension in IS security Management. Proceedings of IFIP TC 11.
[2] Stanton JM, Caldera C, Isaac, A, Stam KR & Marcinkowski SJ (2003), Behavioral IS security: Defining the criterion space. In: Mastrangelo PM & Everton WJ (eds) The Internet at work or not: Preventing computer deviance. Symposium presentation at the meeting of the society for Industrial and Organizational Psychology, Orlando.
[3] Ward, P. and Smith, C.L. (2002), "The development of access control policies for information technology systems", Computers & Security, Vol. 21 No. 4, pp. 365-71.
[4] Schneier, B. (2004), Secrets and Lies: Digital Security in a Networked World,Wiley, Indianapolis, IN.
[5] Schultz, E. (2005), "The human factor in security", Computers & Security, Vol. 24 No. 6, pp. 425-6.
[6] Gullik Wold. Key factors in making ICT Security Policies effective. MSc thesis. Gjøvik University College, June 2004.
[7] European Security Forum. Implementation guide: How To Make Your Organisation Aware Of IT Security. July 1993. Document available to ISF members only, but an electronic version of the table of contents is found at http://www.securityforum.org/ReportsLibrary2003/categories/cat/aware.htm
[8] David Lacey. Managing the Human Factor in Information Security, Wiley (2009), pp.211
[9] Aetna: Developing and Implementing a Successful Information Security Awareness Program. Information security: contemporary cases, case 7, February, 2005.
[10] IT manager Hilde Gjevestad Hellenes in NLI personal communication in 2010.
[11] Information security awareness initiatives: Current practice and the measurement of success, European Network and Information Security Agency, Heraklion. July 2007.
[12] Charles Cresson Wood. Policies Alone Do Not Constitute a Sufficient Awareness Effort. Computer Fraud & Security, pp. 14-19, December 1997. Electronic version found at http://www.sciencedirect.com/
[13] Petri Puhakainen. A design theory for information security awareness, faculty of secience, department of information processing science, university of Oulu, July 2006.
[14] Mark Wilson and Joan Hash (2003) "Building an Information Technology Security Awareness and Training Program" Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology , Gaithersburg, MD 20899-8933.
[15] Hansche S (2001) Designing a Security Awareness Program: Part I, Information system security 10(1): 14-22.
[16] Moxnes, E. (2009). Presidential address: Diffusion of System Dynamics", System Dynamics Society. Proceedings of the 27th International Conference of the System Dynamics Society, Albuquerque: Available

at:http://www.systemdynamics.org/publications.htm#PresAddresses (last read: 30.06.2010).
[17] Annual Information Security awareness training, Department of Child Support Services.
[18] Janne Merete Hagen, Eirik Albrechtsen, (2009) "Effects on employees' information security abilities by e-learning", Information Management & Computer Security, Vol. 17 Iss: 5, pp.388 – 407.
[19] Mark Thomson. Making information security awareness and training more effective. Proceedigs of the IFIP TC11 WG11.3 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden, pp. 261 – 270. Electronic version found at http://citeseer.nj.nec.com/
[20] The UK DTI information security breaches survey (2007).
[21] Stewart Kowalski, Hans Nässla, Jens Karlsson, Veronica Karlsson. The Manual is the Message – An Experiment with Paper based and Web Based IT Security Manuals. Proceedings of the IFIP TC11 WG11.3 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden, pp. 293 - 303. Electronic version found at http://www.ida.liu.se/~hanna/papers/1999-WISE1-paper.PDF
[22] Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008a), "Implementation and effectiveness of organizational information security measures", Information Management & Computer Security, Vol. 16 No. 4, pp. 377-97.
[23] Hagen, J.M., Kalberg-Sivertsen, T. and Rong, C. (2008b), "Protection against unauthorized access and computer crime in Norwegian enterprises", Journal of Computer Security, Vol. 16, pp. 341-66.
[24] Ehn P. Scandinavian design: on participation and skill. In: Adler PS, Winograd T, editors. Usability – turning technologies into tools. New York: Oxford University Press; 1992.
[25] Greenberg ES. The consequences of worker participation: a clarification of the theoretical literature. Social Science Quarterly 1975; 56(2):191–209.
[26] Greenwood DJ, Levin M. Introduction to action research. Thousand Oaks, CA: SAGE Publications; 1998.
[27] Levin M, Klev R. Forandring som praksis. Læring og utvikling I organisasjoner [Change as practise. Learning and development in organisations] (in Norwegian). Bergen, Norway: Fagbokforlaget; 2002.
[28] Eirik Albrechtsen, Jan Hovden. Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. Computers & Security 29 (2010) 432 – 445. Available at www.sciencedirect.com
[29] R.S. Shaw, Charlie C. Chen, Albert L. Harris, Hui-Jou Huang. The impact of information richness on information security awareness training effectiveness. Computer & Education 52 (2009) 92-100.
[30] K. Rudolph, Gale Warshawsky, and Louis Numkin. Computer Security Handbook, Fourth Edition, Chapter 29, Security Awareness. 2001. Electronic version found at http://nativeintelligence.com/about-awareness/cshch29kr.PDF

[31] Johnny Mathisen. Measuring Information Security Awareness – A survey showing the Norwegian way to do it. Norwegian Information Security Laboratory (NISlab), June 2004.
[32] European Security Forum. Implementation guide: How to Make Your Organisation Aware Of IT Security. July 1993. Document available to ISF members only, but an electronic version of the table of contents is found at http://www.securityforum.org/ReportsLibrary2003/categories/cat/aware.htm
[33] Skinner BF (1991) The behavior of organisms: An experimental analysis. B.F. Skinner Foundation (reprinted).
[34] Festinger L & Carlsmith JM (1959), Cognitive consequences of forced compliance. Journal of Abnormal and Social Psychology 58: 203-210.
[35] Straub DW (1990) Effective IS Security: An Empirical Study. Information Systems Research 1(3): 255-276.
[36] Driscoll MP (2000) Psychology of Learning for Instruction. Allyn and Bacon, Needham Heights.
[37] Azrin NH & Holz WC (1966) Punishment. In: Honig, WA (ed) Operant behavior: Areas of research and application. Appleton-Century-Crofts, New York.
[38] Azrin NH (1967) Pain and Aggression. Psychology Today 1: 27-33.
[39] Seligman MEP & Maier SF (1967) Failure to escape traumatic shock. Journal of Experimental Psychology 74: 1-9.
[40] Sims HP & Lorenzi P (1992) The New Leadership Paradigm, Social Learning and Cognition in Organizations. Sage Publications, Newbury Park.
[41] Daniels AC (2000), Bringing Out the Best in People, How to Apply the Astonishing Power of Positive Reinforcement. McGraw-Hill, USA.
[42] Meyer P (1994) Can You Give Good, Inexpensive Rewards? Some real-life answers. Business Horizons (November-December): 84-85.
[43] Estes WK (1972) Reinforcement in Human Behavior. American Scientist 60: 723-729.
[44] Luc Pelfini. Assessing the Success of Awareness Campaigns. Euro CISA (2007).
[45] Ivar Kufås, Roy Are Mølmann. Informasjonssikkerhet, mennesker og kultur – Diskusjon av verktøyet. Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. June 2003.
[46] Argyris, Chris; Schön, Donald A. Participatory action research and action science compared: A commentary. American Behavioral Scientist, Vol 32(5), May-Jun 1989, 612-623. doi: 10.1177/0002764289032005008
[47] Ivar Kufås, Roy Are Mølmann. Informasjonssikkerhet, mennesker og kultur – Et undersøkelsesverktøy for kartlegging av holdninger og sikkerhetskultur. Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. June 2003.
[48] H.A. Kruger, W.D. Kearney. A prototype for assessing information security awareness. Computer & Security 25 (2006) 289-296.
[49] Belton V, Stewart TJ. Multiple criteria decision analysis. An integrated approach. Dordrecht: Kluwer Academic Publishers; 2002.

[50] Wasim A. Al-Hamdani. Assessment of need and method of delivery for information security awareness program, 2006.
[51] McNamara, Carter, PhD. General Guidelines for Conducting Interviews, Minnesota, 1999.
[52] Dapzury Valenzuela and Pallavi Shrivastava. Interview as a Method for Qualitative Research, 2007.
[53] John W. Creswell. Research Design. Qualitative, Quantitative, and Mixed Methods Approaches. Second Edition. SAGE Publications 2003.
[54] The qualitative research interview. Qualitative methods in organizational research: A practical guide. King, Nigel Cassell, Catherine (Ed); Symon, Gillian (Ed), (1994). Qualitative methods in organizational research: A practical guide, (pp. 14-36). Thousand Oaks, CA, US: Sage Publications, Inc, xii, 253 pp.
[55] Stinger ET (1999) Action Research, Second Edition. Sage Publications, Thousand Oaks.
[56] Spradley JP (1979), The Ethnographic Interview. Wadsworth, Belmont.
[57] Jan A Audestad. Network security, 2009 (2nd edition), Chapter 8 Mobile security.
[58] Blumstein A, Cochen J & Nagin D (1978) Introduction. In: Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington D.C.
[59] Estes WK (1972) Reinforcement in Human Behavior. American Scientist 60: 723-729.
[60] Daniels AC (2000), Bringing Out the Best in People, How to Apply the Astonishing Power of Positive Reinforcement. McGraw-Hill, USA.
[61] National Institute of Standards and Technology web site http://www.nist.gov/
[62] Zazzle web site http://www.zazzle.com/passwords_information_security_awareness_poster-228316661046601381
[63] Noticebored web site http://www.noticebored.com/index.html
[64] Atterbury Foundation web site http://www.atterbury.org/
[65] Get Insight web site http://www.getinsightnow.com/
[66] Securityposters web site http://securityposters.net/security.html
[67] Garton, L., Haythornthwaite, C., & Wellman, B. (1999). Studying on-line social networks. In S. Jones (Ed.), Doing Internet Research: Critical Issues and Methods for Examining the Net (pp. 75-105). Thousand Oaks, CA: Sage.
[68] Wellman, B. (1997). An electronic group is virtually a social network. In S. Kiesler (Ed.), Culture of the Internet (pp. 179-205). Mahwah, NJ: Lawrence Erlbaum.
[69] Wright, K. B. (2005). Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. Journal of Computer-Mediated Communication, 10, 3
[70] Dillman, D. A., G. Phelps, R. Tortora, K. Swift, J. Kohrell, J. Berck, and B. L. Messer. 2009. "Response rate and measurement differences in mixed-mode surveys using mail, telephone, interactive voice response (IVR) and the Internet." Social Science Research 38:3-20.

Appendix A – Examples of awareness posters

Figure 10 - Security awareness poster from NIST [61]

Figure 11 - Password information security awareness poster from Zazzle [62]

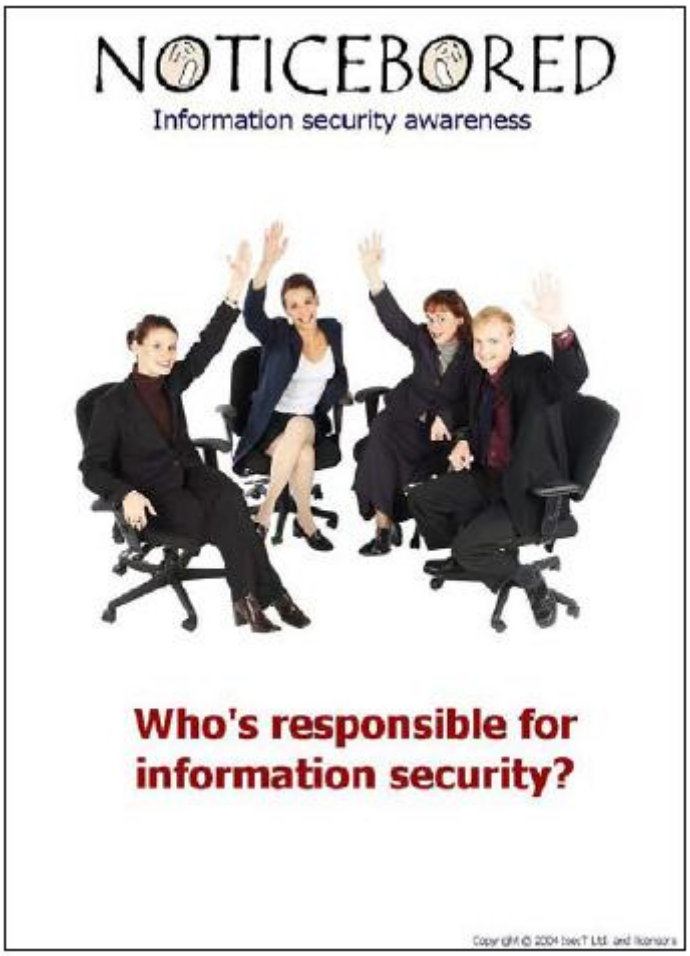

Figure 12 - Security awareness poster from Noticebored [63]

Figure 13 - Security awareness poster from Atterbury Foundation [64]

Figure 14 - Security awareness poster from GetInsight [65]

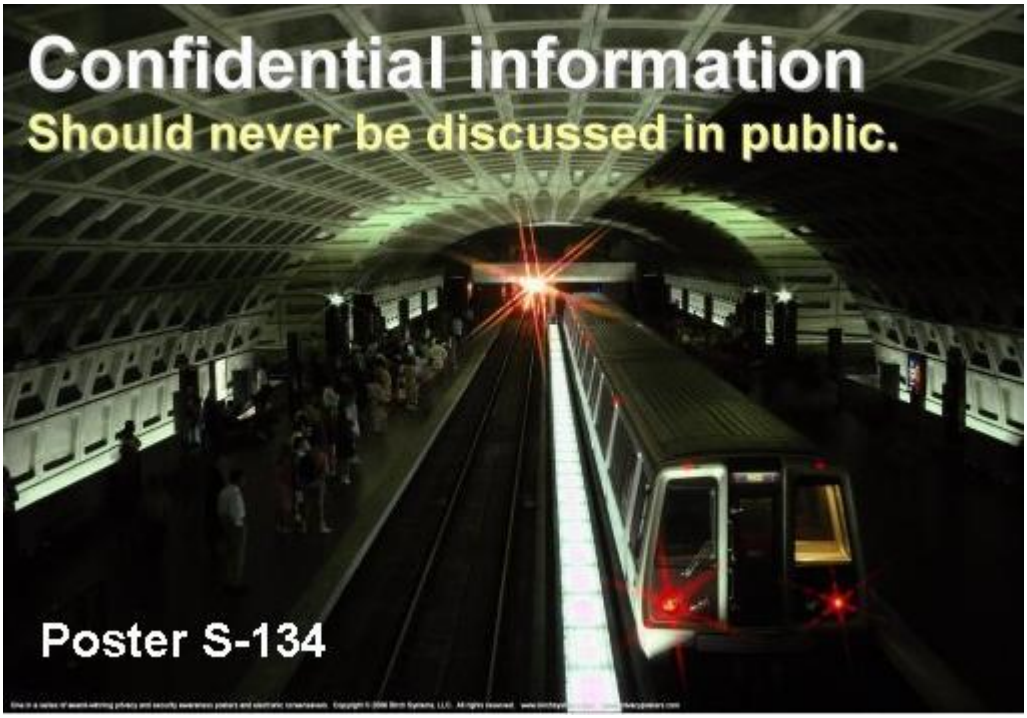

Figure 15 - Security awareness poster from Securityposters [66]

Appendix B –Awareness metrics from Johnny Mathisen (NISlab)

Table 3 – Definition of awareness metric A-1 – Security training [31]

Metric ID	A-1
Name	Security training
Description	This metric shows how many of the employees that have completed necessary courses, and passed the final test if this exists.
Metric	Percentage of the employees having completed the necessary security training in order to do their daily work.
Formula	(Number of employees having completed necessary security training) / (Number of employees needing security training) * 100
Purpose	Education and training is pointed out as very important. It is therefore essential that the employees be given the security training they need. The purpose of this metric is to show if security training is needed among the employees in the organisation.
Frequency	Measurements like this should not be necessary to do more than once, or maximum twice, a year as the level of training and education normally doesn't change very quickly.
Indicators	Since necessary training and education is of great importance for the awareness of security, the target for this metric should be 100 %.
Cost	To produce the necessary data for this metric, an overview of security competence is needed as well as an overview of the need for such competence. To collect this sort of data, if not already existent in the personnel system, a questionnaire sent out to all employees could be used.
Validity	If the courses have no final test, this metric will only measure how many of the employees that have participated in training courses and not if they have achieved the necessary knowledge and competence. In that case the validity of this metric may be poor in indicating the level of awareness. The validity will be better if the employees have to pass some sort of test in order to get the course marked as finished.
Reliability	Since the metric, preferably automatic, counts number of employees having finished and passed specific training courses, the reliability of the metric is quite good.

Table 4 – Definition of awareness metric A-2 – Security incidents [31]

Metric ID	A-2
Name	Security incidents
Description	This metric counts the number of security incidents that is reported to the security department.
Metric	Number of reported security incidents in the organisation. This will give an indication both of how many security incidents that happen in the organisation as well as how many of the incidents that are reported.
Formula	Number of reported security incidents.
Purpose	The purpose of this metric is to show if the number of reported incidents increases as the employees learn that all incidents should be reported and if the number decreases as the employees learn that all incidents are reported and will get a consequence.
Frequency	The frequency of the metric depends on the size of the organisation and the number of security incidents, and it will normally vary from 2 to 12 times a year.
Indicators	When a system for incident reporting is first introduced in the organisation the number of incidents will normally be very low. As people learn that all security incidents shall be reported the number will increase. Therefore an increasing number of reported incidents don't necessarily indicate an increasing number of incidents. As the employees learn that all incidents are reported and get a consequence, they are likely to change behaviour in order to decrease the number of incidents. The performance target for this metric should be zero reported incidents, but a realistic target could be to keep the number continuously decreasing after the introduction period where an increase is expected.
Cost	This metric depends on the organisation having a good system for incident reporting. In that case the number of reported incidents should be easy, and hence don't cost much, to obtain.
Validity	The validity of this metric heavily depends on how many of the security incidents that are actually reported to the security department. If this portion is low the validity will be poor. Likewise the validity will be good if all incidents are reported. In a large organisation the number of unreported incidents can be very difficult to find.
Reliability	As long as the metric counts all incidents that are reported and registered in a computer system the reliability is good. If it is manually decided which of the reported incidents that are to be counted in this metric, for instance because "small incidents" should not be counted, the reliability will decrease.

Table 5 – Definition of awareness metric A-3 – Clean desk [31]

Metric ID	A-3
Name	Clean desk
Description	This metric shows how many of employees that leave their desk clean at the end of the day.
Metric	Percentage of the employees following the organisation's policy of leaving the desk clean at the end of the day. A clean desk could be defined as having locked down all confidential paper and secured the laptop with a wire and a lock.
Formula	(Number of employees not leaving the desk as they should) / (Number of controlled employees) * 100
Purpose	The purpose of this metric is to see how many of the employees that follow the company's security policy with respect to leaving the desk clean.
Frequency	The frequency of the metric depends on the size of the organisation, and it will normally vary from 2 to 12 times a year.
Indicators	The performance goal of this metric should be zero percent, as the company wants all employees to leave their desk clean. At least the trend of this metric should be decreasing.
Cost	In order to collect data for this metric, an internal control is necessary. The security staffs must physically check a number of desks throughout the organisation in order to get representative data.
Validity	The validity of this metric is good, as we measure directly how many of the employees that follow the clean desk policy. If the policy states clearly that no security graded paper are to be left on the desk unattended, and that laptops shall be secured by a wire, it is easy to count how many of the controlled desks that are not left as they should.
Reliability	The reliability of this metric depends on how the measurements are done. If the controls are announced in advance it may influence the behaviour of the employees, hence giving not reliable results. Likewise, if the same departments are controlled every time, those employees may change their behaviour in a positive way while the rest of the employees in the organisation do not. The reliability of such measurements will not be very good. To achieve good reliability it is important that the controls are not announced in advance, that a representative sample of the employees are checked every time, and that it is not the same people or departments that are checked in all controls.

Table 6 – Definition of awareness metric A-4 – Paper shredding [31]

Metric ID	A-4
Name	Paper shredding
Description	The metric shows how much of the paper waste that is being shredded.
Metric	Percentage of paper waste being shredded.
Formula	(Weight of shredded paper) / (Total weight of paper waste) * 100
Purpose	The purpose of this metric is to show if the employees use the paper-shredding machine as often as they should.
Frequency	These measurements don't need to be done more than one to four times a year.
Indicators	The performance target of this metric is difficult to set. If the organisation has a policy saying that all paper waste shall be shredded, the performance target of this metric will of course be 100%. But most companies don't have this kind of policy regarding paper waste. They must find their own target according to their policies. Anyhow this metric will show to which extent the company's paper-shredding machines are being used.
Cost	The measurement data for this metric must be found by physically measuring the amount of paper waste, shredded or not, that goes out of the company. The amount can be measured by weight or by volume. The measuring could be done in cooperation with the company collecting the paper waste.
Validity	What we actually want to measure is if people are shredding all security graded paper, while this metric shows how much of the total amount of paper waste that is shredded. The metric says nothing about what kind of paper that is shredded. This means the validity of this metric might not be very good.
Reliability	The reliability of this metric depends on how the measurements are done. Doing a small number of sample tests in some departments may give poor reliability, while measuring the weight of paper waste, both shredded and not, going out of the organisation gives good reliability.

Table 7 – Definition of awareness metric A-5 – Illegal traffic [31]

Metric ID	A-5
Name	Illegal traffic
Description	The metric shows the amount of illegal or unwanted traffic on the internal computer network.
Metric	Percentage of illegal or unwanted traffic on the internal computer network.
Formula	(Amount of unwanted or illegal network traffic) / (Total amount of traffic on the same network) * 100
Purpose	The goal of measuring with this metric is to see if the employees use the computer network as described in the policies and not transmit or receive illegal or unwanted traffic. Many organisations automatically stop unwanted traffic through their firewalls, but there will often be some illegal or unwanted traffic that is let through. The purpose of this metric is to see the amount of this traffic.
Frequency	This kind of measurements can be done quite often, as for instance every month.
Indicators	As this metric directly shows the amount of unwanted traffic in the internal computer network, the performance target should be zero. An increasing performance trend may indicate that people have found a hole in the firewall and that the rules must be adjusted.
Cost	The data for this metric typically come from log files on firewalls, routers, intrusion detection systems, web servers etc. When the logs, and a system for analysing the logs, exist, the cost of measuring with this metric is relatively modest.
Validity	Since we measure the amount of illegal computer traffic and this directly relate to the behaviour of the employees, the validity of this metric is quite good.
Reliability	To achieve good reliability of this metric it is important that it is well defined what is illegal or unwanted traffic in the network. These definitions should be implemented in the log analyser tool to make sure the same definitions are used whenever the measurements are done. If the operator has to manually decide what is unwanted traffic every time he or she does the measurement, the reliability will be poor.

Table 8 – Definition of awareness metric A-6 – Weak passwords [31]

Metric ID	A-6
Name	Weak passwords
Description	This metric counts the number of weak user passwords.
Metric	Percentage of the user passwords registered in the various systems that are considered weak.
Formula	(Number of weak passwords) / (Total number of user passwords) * 100
Purpose	The goal of this metric is to show if people choose strong passwords even if it is technically possible to choose weak ones.
Frequency	This kind of measurements, that must be done fully automatically, can be performed as often as every month. Many organisations have a password policy that forces the employees to change their passwords every month. This also indicates that the measurements should be done every month.
Indicators	Ideally there should be no weak user passwords in the systems; hence the measurement target should be zero for this metric. This is however quite unrealistic if there are no technical solutions installed to ensure this. A large number of weak passwords can make it easier for an intruder to log into the systems as an authorised user, so the target for this metric should be as low as possible.
Cost	Simple password crackers are free to download and use. When given the necessary password files, the system will automatically generate the desired results. The costs of doing these measurements are therefore quite small.
Validity	By measuring the number of weak user passwords in the systems we directly find how the employees choose their passwords. The validity of this metric is therefore good in measuring user behaviour.
Reliability	If the same password cracker program with the same rules is used every time, the reliability is good. The rules define what a "weak" password is. It could for instance be words from dictionaries with some numbers added. If the rules are changed, the reliability decreases.

Table 9 – Definition of awareness metric A-7 – Hits on web pages [31]

Metric ID	A-7
Name	Hits on web pages
Description	The metric counts the number of hits on security related web pages.
Metric	Number of times an article or a web page containing security information is loaded.
Formula	Number of times a specific web page is loaded
Purpose	The purpose of this metric is to see if a security message reaches out to the employees via the internal web.
Frequency	The frequency of this type of measurement can vary between once a day and once a month depending on the content of the web page. If it is a news article measurements should be done every day. The number of hits on the web page containing for instance the security policy is not necessary to measure more often than once every month.
Indicators	This metric doesn't have any measurement target. It gives though a good indication of how often particular pages are visited. If the number of hits on an important page decreases against zero it may be necessary to take some action in order to get the message out to everyone via other channels than web. Or maybe some internal advertising for the web pages is what helps. It is important to notice that the number of hits on a page is not the same as the number of employees having visited the page as some may have loaded the page several times.
Cost	The data for this metric can easily be retrieved from the log files on the web server or by installing a counter on the page. The cost is therefore very low.
Validity	The number of times a web page is loaded gives a good indication of how many of the employees who have read the content. The validity of this metric is therefore quite good. It must though be noted that some people may load the page several times making the reported number higher than the actual number of employees having loaded the page. It is also worth noticing that loading the page doesn't necessarily mean that the contents have been read and understood.
Reliability	Since this measurement is done fully automatic the reliability is good. If the program works correctly, it will always report the correct number of times the page has been loaded.

Table 10 – Definition of awareness metric A-8 – Requests to security department[31]

Metric ID	A-8
Name	Requests to security department
Description	This metric counts the number of requests, for instance by phone or e-mail, to the security department.
Metric	Number of requests by phone or e-mail to the security staffs.
Formula	Number of requests to the security department
Purpose	The purpose of this metric is to measure the awareness among the employees. Counting the number of requests to the security department does this.
Frequency	The frequency of this metric could vary from weekly to quarterly depending on the size of the organisation. If there are only a couple of requests in a week, the measurements should be done on a monthly or quarterly basis.
Indicators	It is impossible to set a performance target for this metric. The purpose of the metric is merely to show a trend rather than a particular value. An increasing trend may indicate an increasing level of awareness among the employees as they dare and care to ask questions about information security.
Cost	The measurement data for this metric must to a great extent be collected manually. If the security department has a mailbox for incoming requests, the number of requests during the last period is quite easy to obtain. But in addition to this, the security staffs must register all requests by phone or e-mail made to them personally. If such a registration system exists, for instance a spreadsheet, the costs of doing the measurements are quite small.
Validity	Provided that there is a connection between the level of awareness and the number of requests, something that several security managers have indicated, the validity of this metric is good since all requests are counted.
Reliability	Since the collection of measurement data has to be done manually by the security staffs, the reliability of the metric may not be as good as desired. It depends on how well a "request" is defined. Some may count all incoming calls and e-mails while other only count requests about specific security problems. To achieve good reliability it is important that all of the security staffs agree about what is to be counted and what is not.

Table 11 – Definition of awareness metric A-9 – Customer satisfaction [31]

Metric ID	A-9
Name	Customer satisfaction
Description	The satisfaction among the customers of the security department.
Metric	Satisfaction among the employees in the organisation regarding the security department and the job they do.
Formula	Average of grade from all participating employees.
Purpose	The purpose with this metric is to show how satisfied the people in the organisation are with the security department and the job that they do. It can also show to what extent the employees know about the security department, i.e. its visibility in the organisation.
Frequency	Depending on how the measurements are done, the frequency could typically vary from monthly to yearly. It is important that the measurements are not done so often that they are seen as a hassle by the employees. By doing sample tests and not asking the same persons more than twice a year it is still possible to get data on a monthly basis.
Indicators	The ideal performance target of this metric would be to achieve the top grade, but this is somewhat unrealistic. Another target could be to be the best department or to do better than last period. The performance trend of this metric is just as important as the actual value. A decreasing satisfaction among the employees may indicate that the security department should change the way they work and communicate with the employees in the organisation.
Cost	The measurement data for this metric are collected through internal surveys or questionnaires. The costs of doing the measurements therefore heavily depend on the size of the questionnaire and the number of employees asked to participate. Using electronic questionnaires, for instance on the internal web, will ease the work, and hence lower the costs, of analysing the received answers.
Validity	The validity of the metric depends on the questions asked in the questionnaire. Detailed questions like "How do you like the new presentation of the security policy on web?" can give a good indication of customer satisfaction as well as valuable information back to the security department.
Reliability	Also the reliability depends on the questions asked. To achieve good reliability it is important that both the questions and the possible answers are so simple that they are not misunderstood. Questions like "How satisfied are you with the two-factor authentication method on your computer?" may give many "don't know"-answers from non-security employees. If the answers are to be given as a number between 1 and 5 indicating the level of satisfaction, it is important that either 1 or 5 is always "very satisfied" to prevent people from answering the opposite of what they meant to on some questions, leading to poor reliability.

Appendix C – Metrics for security awareness for NLI

Table 12 – Definition of awareness metric B-1 – Security policy testing

Metric ID	B-1
Name	Security policy testing
Description	The metric shows how many employees tested on the security policy.
Metric	Percentage of individuals tested on the security policy (passing and failing).
Formula	(Number of individuals have tested on the security policy) / (Number of individuals should be tested on the policy) * 100
Purpose	The security policy clarifies routines for correctly handling confidential information and information resources. It is therefore essential that the employees remember, understand and then comply with the security policy. The purpose of this metric is to show whether people have read and remember the security policy.
Frequency	The frequency of this metric can be done 1 or 2 times a year.
Indicators	Since policy testing is one way for the awareness of security , the target for this metric should be 100%
Cost	This metric depends on organizations having set monitoring tools to identify those employees who have or have not yet tested the security policy. If not already existent in the organization, a questionnaire sent out to all employees could be used.
Validity	If have not additional sub metrics to show how many individuals passed the test and how many failed the test, this metric will only measure how many of the employees that have participated in security policy testing and not if they have achieved the necessary knowledge showing on the security policy.
Reliability	Since the metric, preferably automatic, counts numbers of employees have tested security policy. The reliability of the metric is quite good.

Table 13 – Definition of awareness metric B-2 – Critical information recognizing

Metric ID	B-2
Name	Critical information recognizing
Description	The metric shows the extent of employees familiar with the company critical information.
Metric	Percentage of employee familiar with critical information in business.
Formula	(Number of employees familiar with critical information in business) / (Number of employees should familiar with critical information in business) * 100
Purpose	If the business's critical information is disclosed to the related competitive business, it will influence the development of whole business. It is therefore essential that the employees recognize what is the critical information in their business and then remember it and protect it carefully. The purpose of this metric is to show whether people familiar with the company critical information.
Frequency	Measurements like this should not be necessary to do more than once, or maximum twice a year as the critical information in business doesn't change frequently, employee just need recognize, remember it and then protect it carefully.
Indicators	Recognizing critical information is the first step, after that people will know what kind of information should be carefully protected. The target for this metric should be 100%.
Cost	In order to collect data for this metric, a questionnaire should be well designed to send out all employees, which cost not too much.
Validity	Since we measure employees who are familiar with critical information in business which is directly relate to the basic security awareness of the employees, the validity of this metric is good.
Reliability	The reliability of this metric depends on whether the related internal policy or guidelines have listed what critical information are in business for employees and good questionnaire designing for the data colleting.

Table 14 – Definition of awareness metric B-3 – Security event scenario recognizing

Metric ID	B-3
Name	Security event scenario recognizing
Description	The metric shows the extent of employees recognizing a security scenario.
Metric	Percentage of users recognizing a security event scenario.
Formula	(Number of employees recognizing a security event scenario) / (Number of employees should recognize a security event scenario) * 100
Purpose	The goal of this metric is to show whether people recognize a security event scenario as learned from security awareness training or others.
Frequency	This kind of measurement can be done 1 or 2 times a year.
Indicators	The target for this metric should be 100%. All employees should aware of security event scenario, or at least the rate should as higher as possible.
Cost	In order to collect data for this metric, a questionnaire should be well designed to send out all employees, which cost not too much.
Validity	Since we measure employees who are familiar with a security event scenario which is directly relate to the security awareness of the employees, the validity of this metric is quite good.
Reliability	The reliability of this metric depends on the questionnaire designing for the data colleting.