KUNGL TEKNISKA HÖGSKOLAN

HØGSKOLEN I GJØVIK

NISlab
Norwegian Information Security Laboratory

Measuring Information Security Awareness – A survey showing the Norwegian way to do it

Johnny Mathisen

Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2002

Examensarbete 20 poäng
i data- och systemvetenskap
inom magisterprogrammet i informations- och kommunikations säkerhet,
Kungl Tekniska Högskolan

Preface

In my work with information security during the last eleven years the focus has mainly been on technical solutions like crypto devices, firewalls, and public key infrastructure. Such installations are of course important elements within the information security area. But they are far from enough. All possible technical installations will have no effect if the people using the systems don't behave correctly. It doesn't matter if the data are encrypted on the disk if an employee with legal access decides to distribute the content of the file on Internet. It just can't be stopped technically. The only way to ensure a proper level of security is by making the employees behave correctly. This reality, combined with the fact that the security industry mainly focuses on technical solutions, made me choose information security awareness as the topic of my MSc Thesis.

A feasibility study carried out in December 2003 among a number of security managers in Norwegian companies showed me that there was an interest in this kind of knowledge. The persons contacted were all positive to the topic, and they would gladly participate in a survey. This made me even stronger in my belief that there was a need for this kind of work and I decided to go on.

The work with the Thesis has turned out well without any major obstacles or delays. The feasibility study showed me that the best way to get in contact with the right persons was through the telephone. It is so easy to forget to reply to e-mail. Therefore I decided to conduct the survey via telephone after first sending out information about the project on e-mail. I was aware that security managers are usually busy people and therefore could be difficult to get in contact with. That is why I contacted so many companies and organisations in the first place. I finally managed to get an interview with about half of the contact persons, and they gave me enough information to write this Thesis. A response rate of 50 percent is obviously what you can expect on this kind of survey, as this is also the situation for other similar MSc Thesis work this semester at Gjøvik University College.

It would not have been possible to complete this project if my contact persons had not helped me. Some have used their time on my interviews, some have given me valuable advices, and some have helped me getting in contact with the right persons. Unfortunately I can't mention any names, but I haven't forgotten any of you. I am very thankful for all the assistance you have given me during this project! Hopefully you will get something back when reading this report.

The teaching supervisor of this thesis work has been Prof. Einar Snekkenes at Gjøvik University College.

Finally I would like to thank my employer, Telenor, who have let me use some of their time on this project, and my wife, Vibeke, and children, Petter and Morten, who have let me use evenings, weekends, and holidays as well to finish the work. Thank you, all!

Oslo, 17th of June 2004

Johnny Mathisen

Abstract

The attitudes and awareness of the employees are very important for the information security in a company of today. In fact it is a common view that the people and their behaviour mean more to information security than all technical solutions. This fact is well known by all large companies in Norway today. And therefore they work very actively in order to raise the awareness and improve the behaviour and attitudes among their employees. Many do this by arranging special security campaigns. But do they know anything about the effect of their work?

- Do the campaigns really lead to better attitudes and behaviour when it comes to information security?
- Can the effect of information security awareness campaigns, or any other work with awareness and attitudes, be measured?
- Do someone measure the effect of their work or do they just hope and believe that their effort have a positive effect on the way the employees behave?

We have done a survey in many Norwegian companies to find the answers to these questions. Security managers and other people working with awareness and attitudes to information security have been interviewed to provide the necessary information. They have been asked questions about how they work to raise the awareness and improve the attitudes among their employees and how they measure the level of awareness. Some companies arrange security campaigns quite often while others seldom or never do it. Some develop their own campaigns while others use a customized version of a commercial product. And some of the companies actually try to measure the level of awareness among their employees. This is done for instance through internal surveys, internal controls, or measurements of traffic on the internal computer network. But none of the organisations say they use the measurements systematically to measure the effect of their work. Those who use such measurements mainly use them to see if there is a need for special security awareness campaigns. But the interviewed security managers say there is a need for such measurements, and they look forward to see the results of this work.

In order to help them measure the effect of the work with security awareness, we have identified and defined a set of security metrics. The set is not meant to be a complete set of awareness metrics, 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 I at the end of this report for all companies and organisations to use.

It is important that the metrics can be used in practical work and that they give added value to the organisations using them. A practical test of the metrics is therefore very important. This is however out of the scope of this project and will not be described in this report. But it is considered a natural continuance of the work that is done here.

Sammendrag (Abstract in Norwegian)

Holdningene og bevisstheten blant de ansatte har stor betydning for informasjonssikkerheten i dagens bedrifter. Det er en vanlig oppfatning at menneskene og deres oppførsel faktisk betyr mer for informasjonssikkerheten enn alle mulige tekniske løsninger. Dette er velkjent også blant alle store norske bedrifter og organisasjoner. Og derfor jobber de også veldig aktivt for å heve bevisstheten og forbedre oppførselen og holdningene blant sine ansatte. Mange gjør dette ved å arrangere spesielle sikkerhetskampanjer. Men vet de noe om effekten av dette arbeidet?

- Fører kampanjene virkelig til bedre holdninger og bedret oppførsel når det gjelder informasjonssikkerhet?
- Kan effekten av informasjonssikkerhetskampanjer, eller annet holdningsskapende arbeid, måles?
- Er det noen som måler effekten av det arbeidet de gjør eller håper og tror de bare at innsatsen deres har en positiv effekt på de ansattes oppførsel?

Vi har gjort en undersøkelse blant mange norske bedrifter for å finne svarene på disse spørsmålene. Sikkerhetsledere og andre personer som jobber med bevissthet og holdninger til informasjonssikkerhet har blitt intervjuet for å frembringe nødvendig informasjon. De har blitt stilt spørsmål om hvordan de jobber med å heve bevisstheten og forbedre holdningene blant sine ansatte samt hvordan de eventuelt måler nivået på bevisstheten. Enkelte bedrifter arrangerer sikkerhetskampanjer ganske ofte mens andre sjelden aller aldri gjør det. Noen lager sine egne kampanjer mens andre bruker tilpassede versjoner av kommersielle produkter. Og enkelte bedrifter forsøker faktisk å måle nivået på bevisstheten blant sine ansatte. Dette blir gjort for eksempel gjennom interne spørreundersøkelser, interne kontroller eller trafikk-målinger i det interne datanettverket. Men ingen av organisasjonene sier at de bruker målingene systematisk for å måle effekten av det holdningsskapende arbeidet. De som foretar slike målinger bruker disse i hovedsak til å se om det er behov for spesielle sikkerhets-kampanjer. Men de intervjuede sikkerhetslederne sier at det er behov for slike målinger, og de ser fram til resultatet av dette arbeidet.

For å hjelpe dem i arbeidet med å måle effekten av det holdningsskapende arbeidet har vi identifisert og definert et sett av sikkerhetsmetrikker. Dette settet er ikke ment å være et komplett sett av bevissthetsmetrikker, men forhåpentligvis kan de tjene som eksempler og gi inspirasjon til å definere andre metrikker. Metrikkene er definert i henhold til tilgjengelige maler, og de er presentert i Appendix I til slutt i denne rapporten slik at alle bedrifter og organisasjoner som ønsker det kan bruke dem.

Det er viktig at metrikkene kan brukes i det praktiske arbeidet og at de gir økt verdi for de organisasjonene som bruker dem. Det er derfor viktig å prøve ut metrikkene i praksis. Dette ligger imidlertid utenfor rammene til dette prosjektet, og det vil derfor ikke beskrives i denne rapporten. Men det vil være en naturlig videreføring av det arbeidet som her er gjort.

Table of Contents

List of figures

List of tables

1 Introduction

1.1 Topic covered by this thesis

In the last years information security has become a more important issue for most large companies around the world. These companies have also understood that better security can't be achieved by just installing another security hardware device like a firewall or an intrusion detection system. Even the most secure system won't give you any security if the people operating it have the wrong attitudes and don't behave, as they should. It's a common view that information security heavily depends on the behaviour of the employees. Some say information security consists of 20% technical concepts and 80% human behaviour; some say the ratio is 10/90. In an AT&T Network Security survey from March/April 2003 [AT&T] Mr. Byrnes from Meta Group estimates that "30% of IT security relates to technology, and 70% relates to people and practices".

Mr. Gullik Wold also points out the importance of awareness in his MSc Thesis "Key factors in making ICT Security Policies effective" [Wold]. His survey shows "that organisations that do not promote information security awareness are more likely to experience a major security incident than those that do promote awareness."

Yet companies spend much more money on technical solutions than on employee's awareness and behaviour. In fact only 16 percent of the companies rank awareness among the top three areas of information security spending according to the "Global Information Security Survey 2003" performed by Ernst & Young [GISS]. As shown in Figure 1, awareness is ranked sixth, far behind technology.

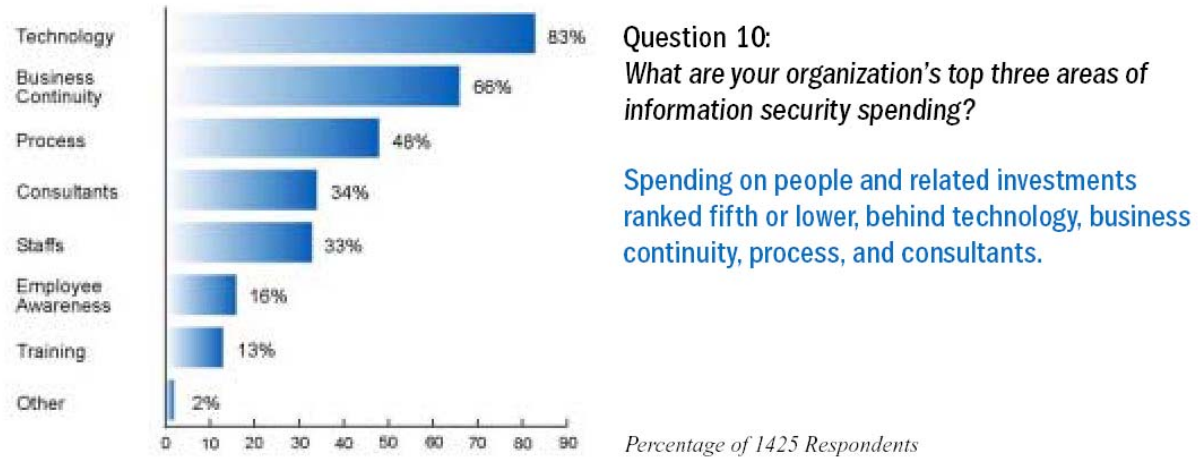

Figure 1 - Organisation's spending on information security [GISS]

Even if awareness is not among the top five on this list, there are although some companies that focus on awareness and attitudes. In this article we will try to find out what Norwegian companies and organisations do to raise the awareness and improve the attitudes to information security among their employees.

Many companies arrange some sort of campaigns to raise the level of security awareness and to change the attitudes and behaviour in a better direction. They believe that a security awareness campaign will increase the level of information security in the company. But is this

just something they believe or do they actually measure the effect of their campaigns? This is something we will also look into in this report.

Based on what is done by the companies today in order to measure the awareness and the research done on this area, we will finally define some metrics for awareness. Such metrics will hopefully make it easier for the companies to do reliable measurements.

But first we must define what we mean by awareness. ISF (Information Security Forum) [ISF] defines IT security awareness in this way [ISF93]:

> **IT Security Awareness** is the degree or extent to which **every** member of staff understands:
>
> - the importance of IT security
> - the levels of IT security appropriate to the organisation
> - their individual security responsibilities
>
> … and acts accordingly.

While NIST (National Institute of Standards and Technology) [NIST] uses this definition of awareness [NIST16] :

> 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 formal, having a goal of building knowledge and skills to facilitate the job performance.

The contents of those definitions are quite similar as they both define awareness as understanding the importance of information security and then behave accordingly. The behaviour of the employees is namely very important as it is what they really do that matters, and not what they know they should do. This meaning of the word awareness coincides with our own comprehension and we will therefore use this definition of the word in this report.

But instead of using the term “IT security”, as both ISF and NIST do, we will use the term “information security”. This indicates that we will look at information security in a wider context, including areas like shredding of security-graded documents, social engineering, physical access to the office etc. We consider those areas just as important as the IT systems.

1.2 Problem description

The information security in a company does not depend only on the implemented technical solutions. The attitude and behaviour of the employees is also playing an important role. It is therefore common to try to improve the attitude, usually through an awareness campaign in a relatively short period of time. But it is also a fact that it is hard to reach all employees with such campaigns. Some doesn't register the campaign at all. Other doesn't catch the message while many see the campaign and understand the message, but they choose to believe that this doesn't concern them. The effect of an awareness campaign on the employee's attitude to information security in the company is therefore very uncertain.

- Do such campaigns reach only those employees who already are conscious about the security in the company?
- Do the campaigns lead to increased consciousness regarding security issues in the company?
- What could possibly be done to make an awareness campaign get larger effect?
- Does a campaign have the same effect in different business sectors?
- Is the effect of a campaign ever measured? And if so, how is this done?

1.3 Justification, motivation and benefits

Most large companies today have good technical solutions to take care of the information security. The weakest link in the security chain is therefore the employee. To raise the level of security in the company it is therefore of vital significance that the employees are conscious about how the security is best taken care of. The attitude and awareness of all employees is very important for the information security. And good attitudes are something that must be built. We therefore wish to know how we in an effective way can create better attitudes and higher awareness of information security for all employees in a company. And we also want to measure the employees' awareness to security issues for better to know when to arrange the next campaign.

Stakeholders for such knowledge would typically be security managers, or other people responsible for information security, in both small and large companies, especially Norwegian ones since this survey is conducted in Norway.

1.4 Research questions

To be able to make better awareness campaigns we need more knowledge of how the campaign should be made for the message to be understood by as many employees as possible. We also have to measure the effect of such campaigns in posterity. To accomplish this we first have to measure the attitudes and the level of awareness among the employees. This has to be done both prior to and after a security campaign is arranged. How this should be done is not fully known today and is a question that needs more research.

To summarize the research questions answered in this article:

- What do Norwegian companies do to raise the level of awareness and attitudes among their employees with respect to information security?
- How do these companies measure the level of awareness and attitudes to information security among all their employees?
- Can we define a set of metrics for measuring the level of awareness and attitudes to information security?
- How should an information security awareness drive be made to give the best return of investment?

To help answer these questions we will first take a closer look at what has already been done of research in this area.

2 Review of state of the art

As already mentioned, most people today are aware of the fact that information security is not just a matter of technical solutions. The awareness, attitudes, and behaviour of the users are just as important. How to raise the awareness and improve the attitude is unfortunately not that intuitive. This chapter contains a literature survey of what has been done of research in this area related to the research questions stated in chapter 1.4.

2.1 Working with awareness and attitudes

What do companies and organisations do to raise the level of awareness and attitudes among their employees with respect to information security?

A project called "Information security and inside problems" (original Norwegian title is "Informasjonssikkerhet og innsideproblematikk") was finished in June 2003 [ROSS]. The project was done as a cooperation between the Norwegian University of Science and Technology (NTNU) [NTNU] and "Nasjonal Sikkerhetsmyndighet" (NSM) [NSM]. The goal of this project was to focus various aspects of information security in relation to internal conditions in organisations. In addition to the final report, this project produced five articles related to the goal of the project:

- [ROSS01] focuses on the employees as a threat against information security and tries to explain why and how insiders can cause security violations.
- [ROSS02] presents taxonomy for classifying human challenges to information security.
- [ROSS03] describes a framework for information security culture to see if it can help solving the insider problem.
- [ROSS04] describes and discusses a self-developed tool for mapping of attitudes, behaviour and culture related to information security in organisations.
- [ROSS05] presents the tool in the form of a questionnaire.

All of these documents contain valuable knowledge for anyone working with such abstract concepts as awareness and attitudes.

To our knowledge, nobody has gathered and made public information about how the practical work with attitudes and awareness is done in companies and organisations, whether in Norway or any other country. The only work we have found in this area is [ROSS04], which describes a pilot survey among three companies in Norway. But the intention of these surveys was to measure the awareness and attitudes in the companies, not to check how the companies worked with awareness and attitudes.

ISF [ISF] did though conduct a survey among the member organisations in 1990/1991 [ISF91] to find out how the organisations worked to raise the awareness of information security among the employees. But unfortunately, since "this document is confidential and purely for the attention of and use by organisations that are members of the Information Security Forum (ISF)", the results from that survey can't be used in this report.

2.2 Measuring awareness and attitudes

How do these companies measure the level of awareness and attitudes to information security among all their employees?

No work has been found covering this topic except for [ROSS04] as mentioned in the previous section. The results from that project show however how the awareness and attitudes to information security among the employees can be measured.

[ROSS05] contains the tool used to measure the awareness and attitudes. The questionnaire, which is written in Norwegian and based on a tool called "Hearts and Minds", developed by Shell International Exploration and Production, 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 behaviour 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".

The rest of the questionnaire consists of 31 questions divided into two categories with a total of eight subcategories:

- Human factors
  - Behaviour
  - Knowledge and attitudes
- Cultural factors in the organisation
  - Policy and management
  - Inclusion and learning
  - Distribution of responsibility
  - Procedures and formalisation
  - Analyses, evaluation and revision
  - Awareness and human relations.

Each question has five possible answers, and they all demand some brainwork. Table 1 shows the four questions in the first category, "Behaviour", with their possible answers, all translated from Norwegian.

The tool was used in three different organisations in 2003. One large group implemented the tool as an internet-based questionnaire while a smaller company used a paper-based questionnaire. In the third organisation the survey was done as interviews, both individual and in groups with following discussions. The discussion of the tool in [ROSS04] contains experiences from all the four pilot surveys.

Table 1 - Questions about behaviour from the NTNU/NSM survey [ROSS05]

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.

The four different ways of doing the survey all have their advantages and disadvantages:

- A large internet-based questionnaire has the advantage that it is possible to use statistical analysis of the results and thereby compare the results from different groups of employees. It is also easy to make it possible for all employees to participate in the survey. 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.

- A smaller paper-based questionnaire 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 internet-based survey.

- Personal interviews take longer time to conduct and it may therefore be a problem getting enough information to give a representative result for a whole organisation. It could also be a problem that the respondents don't answer as honest in an interview as they would on a questionnaire. But the big advantage with interviews is the possibility to go deeper into each question and solve misunderstandings. It is easier for the respondent to give additional information related to the questions.

- There are big challenges attached to a group discussion process. It can be difficult to motivate all employees to participate in a rich discussion, and some have problems talking in large meetings.

There were also some general problems with the tool, regardless of the survey method used. Some complained that there was no "Don't know"-category. This was done on purpose to make the respondents think about the problem and don't choose the easy "Don't know"-solution.

Some felt the survey was too big and comprehensive and took too long to finish and that some questions were not good. This will be looked upon before the next version of the survey is released later this year.

There exist several commercial products for creating security awareness programs. Some of them claim that the results from the program can be measured:

- ***Symantec*** *[Syma]* is one of the leading companies in Internet security. They claim that their program is "a quantifiable investment that offers tools for gauging employee participation and tracking security metrics". There is no information available of how this is done.

- ***Get Insight*** *[GetI]* is a company that focuses on training. They have security awareness campaigns and e-learning programs. They say nothing about how the effect of their campaigns is to be measured.

- ***Corporate Security Awareness*** *[CSA]* is a British consultancy company focusing on guidance and training in information security risk management, policy development and corporate awareness. They can help with awareness campaigns but they say nothing about measuring the effect.

- ***Commissum*** *[Comm]* has a program for raising the corporate security awareness. Through regular reports they provide metrics against benchmarks to ensure improvement is measured and monitored.

- ***Native Intelligence*** *[NaIn]* is an American company focused on information security awareness. They specialises in web-based training and awareness solutions. Their program includes a quiz that gives an indication of how well the information has been understood.

- ***Easy i*** *[Easy]* is a company that focuses on internal communication of business critical issues to large numbers of employees. They have developed the e-learning program "For Your Eyes Only" that is about information security. It ends with a quiz that indicates if the messages of the program have been understood.

If the companies to be interviewed use these or other programs, or if the attitudes and awareness are measured in other ways, is revealed in the interviews.

2.3 Metrics for awareness

Can we define a set of metrics for measuring the level of awareness and attitudes to information security?

Information security education and training needs to be valued and assessed from various perspectives. In their paper "The Value and Assessment of Information Security Education and Training" [Yngs], Louise Yngström and Fredrik Björck present two differing viewpoints from which such an evaluation can be perceived – those of the individual and the organisation. Some sorts of profits are sought after by each of the two, although this is expressed and hence valued differently depending on the perspective taken. The need for measuring the effect of information security education and training is examined, in addition to identifying possible techniques and problems connected with doing this in practice.

The vast majority of all information security education and training efforts have been aimed at computer specialists, but recently the need to educate and train also other groups of individuals has been noticed.

From the perspective of the individual, there are several reasons for measuring the effect of the training. Individuals are always looking for knowledge that can make their life a little bit better. They might strive to get a job, to obtain a better position or to perform tasks at work more efficiently. Whatever cause, the necessity to evaluate information security training is apparent. To evaluate this, regular pedagogical evaluations can be made. The students can be asked questions at the end of the course measuring how much information they have absorbed. Another possibility is to ask the same questions about their awareness and attitudes prior to and after the course.

From the viewpoint of an organisation, information security not only assists safeguarding information assets but it can also provide the organisation with a competitive advantage through lower costs and new business opportunities. And an organisation would like to measure the effect of its invested resources in information security education and training.

Whatever decision is to be taken in an organisation, some kind of cost-benefit analysis is always carried out first. Investments in information security training must compete against other possible investments.

While measuring the impact of information security education and training, one is actually trying to measure the resulting change in human behaviour and its impact on the organisation's ability to reach its goal. One problem with such measurements is the discrepancy between what people say and what they do. There is a possibility that some employees won't state the truth about their own attitudes or level of awareness. Therefore, the focus should not be on what an employee knows but on what he or she does with this knowledge. Another problem is the process of putting a number on such an issue as

information security awareness. It is very difficult to find such a number, and if you do; 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 organisation's number from last year.

There is obviously a clear need for measuring the effect of information security education and training, both from an individual's and an organisation's point of view. But the problem is how this is to be done, especially for an organisation.

The Information Technology Laboratory is a major research component of the National Institute of Standards and Technology. In their bulletin from June 1998 [ITL] they are evaluating the effectiveness of results-based learning. The role- and performance-based model they are referring to is the one presented by NIST [NIST] in "NIST Special Publication 800-16" [NIST16] from April 1998 titled "Information Technology Security Training Requirements: A Role- and Performance-Based Model".

In this model, learning is represented as a continuum that starts with awareness, continues with training and evolves into education. Awareness about IT security is the point-of-entry into the learning process for all employees.

Organizations should evaluate the scope of their IT security training needs and the effectiveness of the training provided. Evaluations enable decision-makers to allocate their training resources sensibly and to derive the greatest return on their training investment. To evaluate teaching, it is necessary to collect trend and other related data. Before initiating evaluations, organizations should develop plans for gathering the evaluation information that they need. One important element from such a plan is that the measures of success should be derived from the individual's normal work products rather than from classroom testing. The evaluation plan should also show how the data would be collected and used.

There are four levels of evaluation that progress from relatively simple to rather complex.

- Level 1 is measuring the student's satisfaction. This could be done by asking the students simple questions about their satisfaction at the end of the course.

- Level 2 is measuring the effectiveness of learning and teaching. It measures how much information was transmitted from the teacher to the student.

- Level 3 is measuring the effectiveness of student performance. This is a "before" and "after" job skills comparison. In some cases this information is difficult to obtain. At this level, the evaluation should begin to show the extent to which the learning activity benefits the organization as well as the employee.

- Level 4 is measuring the effectiveness of the training program. Such evaluations can be difficult to undertake and hard to quantify. Possible approaches could be follow-up interviews with students, comparison of outputs produced by a student both before and after training, and some form of benchmarking. This level of evaluations can help senior managers answer questions about the most cost-effective way to spend training resources.

It is important that the organization commits time and attention to the analysis of the collected data in order to fully review the costs and benefits of IT security-training programs and to make wise decisions in the expenditure of training resources.

NIST has done an extensive work in defining security metrics. In July 2003 they released their "Security Metrics Guide for Information Technology Systems" [NIST55]. Appendix A in this guide describes some examples of security metrics. We will use them as a template when defining our metrics, but with some modifications as for instance including fields for cost, validity and reliability.

Appendix B in the NIST publication "Building an Information Technology Security Awareness and Training Program" [NIST50] from October 2003 contains a sample of an awareness and training metric. The template defined in [NIST55] is used when defining this metric. The full definition of this metric, included accompanying comments, is shown in Table 4 in Appendix F.

ISF has also defined some metrics for awareness based on suggestions from the members. These metrics are described in their "Effective Security Awareness Workshop Report" [ISF02] from 2002. This report is however only available for ISF members, and we can therefore not use this information in our work.

The tool described and analysed in [ROSS04] and [ROSS05] doesn't contain any metrics definitions, but work has been done to try to measure the level of awareness and attitudes to information security among employees in Norwegian companies.

2.4 Making an effective security campaign

How should an information security awareness drive be made to give the best return on investment?

There has been done some research in health care establishments to determine the training needs of personnel classes with respect to information systems security. In his article "Health care management and information systems security: awareness, training or education?" [Kats] from 2000, Sokratis Katsikas discusses a methodology for determining this need.

Learning, in terms of knowledge, can be abstractly thought of as evolving in three distinct but interleaved levels, which together form a continuous rather than a discrete process. It starts with awareness, builds to training and evolves into education. These levels correspond to different types of learning, mostly delineated by differences in the degree of comprehension and detail, both of which increase as we move from awareness towards education.

Awareness activities aim at attracting the attention of individuals to the subject, in our case security, and at allowing them to recognise the concern for information systems security and to respond accordingly. Such activities are usually directed towards broad audiences, and the knowledge gained through them tends to be short-term, immediate and specific, unless the activity is repeatedly exercised.

The training level of the learning process aims at building knowledge, thereby producing relevant and needed security skills. Training usually takes longer than awareness, is more formal and requires that learners take a more active role in the training process. Knowledge gained through training tends to be long term, but quickly becoming obsolete, in particular in fast-moving technological fields such as information systems security.

The third and last level of the learning process, education, aims at creating expertise necessary for information systems security specialists and professionals. The main difference between

training and education is the exploratory nature of the latter, by virtue of which advances in thought and theory make their way into practices.

The appropriate level of training for managers within health care establishments is that of training. Raising the awareness is not enough.

The NIST publication "Building an Information Technology Security Awareness and Training Program" [NIST50] from October 2003 provides guidance for building an effective IT security awareness and training program. Like [Kats] it describes the relationship between awareness, training, and education: "Learning is a continuum; it starts with awareness, builds to training, and evolves into education" [NIST50, p.7]. This continuum is illustrated in Figure 2. The three concepts used in [NIST50], awareness, training, and education, are defined in [NIST16]:

Awareness

> 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 formal, having a goal of building knowledge and skills to facilitate the job performance.

Training

> The "Training" level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialities other than IT security (e.g., management, systems design and development, acquisition, auditing).

Education

> The "Education" level integrates all of the security skills and competencies of the various functional specialities into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.

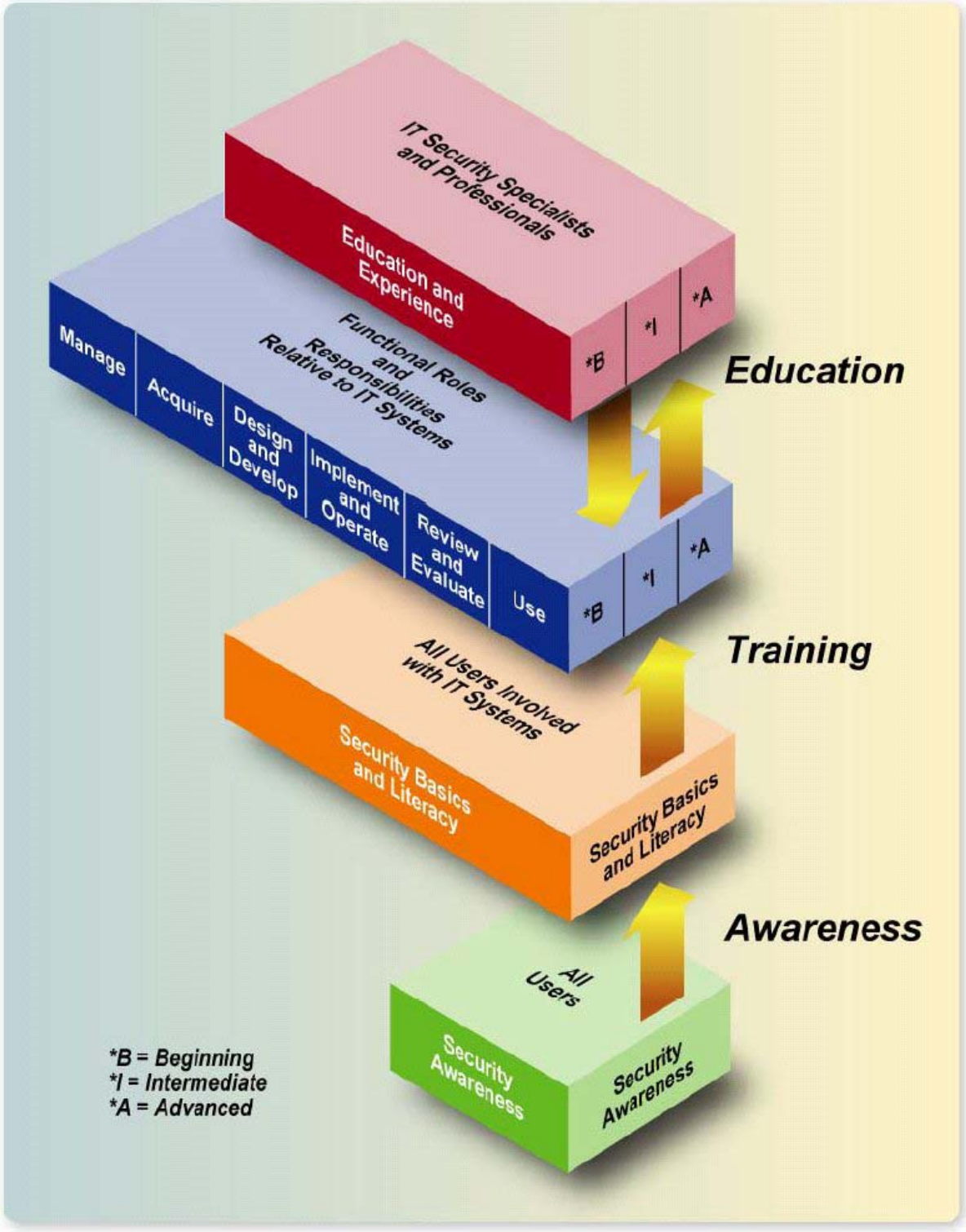

Figure 2 - The IT security learning continuum [NIST50]

The report identifies four critical steps in the life cycle of an awareness and training program. These steps are also illustrated in Figure 3.

- 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.

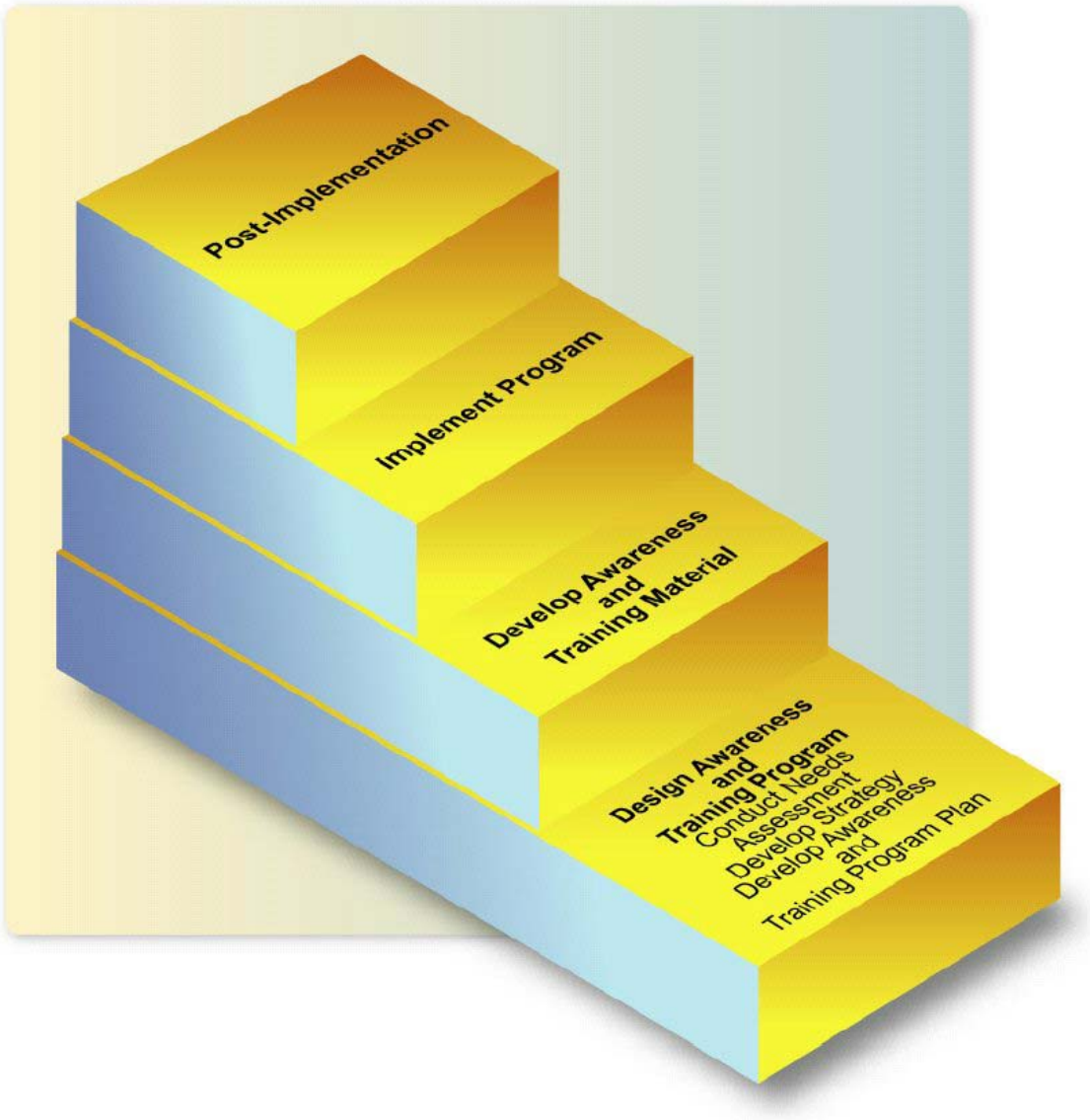

Figure 3 - Key steps in the life cycle of an awareness and training program [NIST50]

- Awareness and training material development includes selecting the topics for the campaign. Possible topics may be password usage and management, web usage, social engineering, and laptop security while on travel. It is important to use available sources of material that can be incorporated into the program. When developing the program, the NIST special publication "Information Technology Security Training Requirements: A Role- and Performance-Based Model" [NIST16] can also be used.

- Program implementation includes the activities of communicating the plan and delivering the awareness and training material. Possible techniques for getting the messages disseminated throughout the organisation may be to use posters, newsletters, giveaways, and screensavers among many others.

- 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. Figure 4 shows examples of such evaluation and feedback mechanisms. The feedback can be used to update the awareness and training program plan.

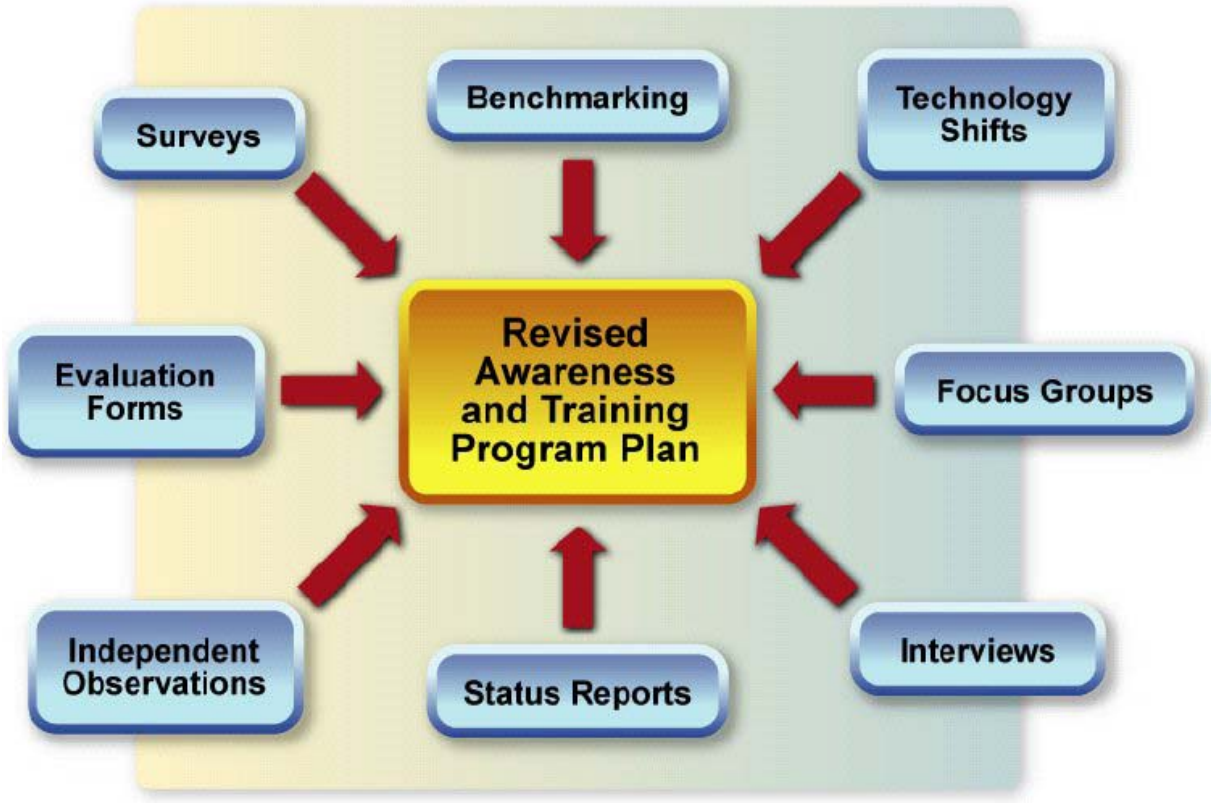

Figure 4 - Evaluation and feedback techniques [NIST50]

The appendices to the report contain a sample questionnaire and a template for an awareness and training program plan.

Chapter 29 in the Computer Security Handbook [Rudo] also contains tips and information about how to develop, implement, and evaluate a security awareness program. The basic ideas are the same as in [NIST50], but more examples and hints are given. In addition to just saying that posters may be used to communicate the messages, the chapter includes tips like "Posters should be colourful 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. Since many companies use posters in their campaigns, Appendix G in this thesis contains examples of posters found on the Internet. Some of the posters must be bought while others are free to use.

To measure the effectiveness of the program it is suggested that measurements, of for instance password strength or the number of employees leaving their terminal unlocked during lunchtime, are done both prior to and after the awareness program is run. As it say: "Unless a pre-program test or preliminary survey is conducted, measuring improvement is virtually impossible". In addition to measurements of the effectiveness of the program, audience satisfaction is also pointed out as an important aspect of measurement and evaluation.

ISF has also published a report on how to work with awareness [ISF02]. Figure 5 shows how they see an effective security awareness process, and this correlates well with the description in [NIST50]. The rest of that report "is confidential and purely for the attention of and use by organisations that are Members of the Information Security Forum (ISF)", and we therefore cannot make further use of that information.

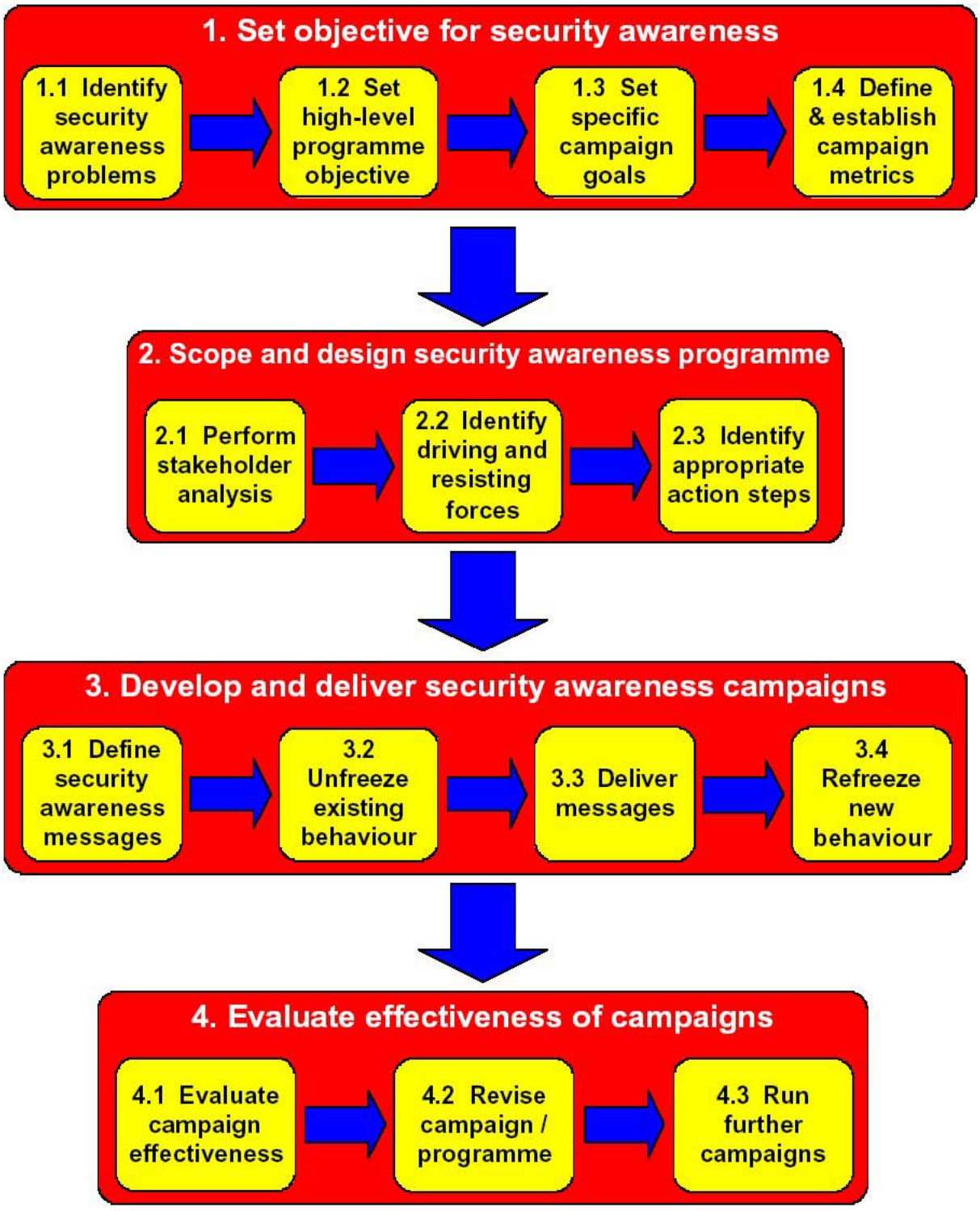

Figure 5 - Process for effective security awareness [ISF02]

The "Standard of Good Practice for Information Security" [ISF03] from ISF is an open document free for all to use. The Standard provides "a set of high-level principles and objectives for information security together with associated statements of good practice" that "can be used to improve the level of security in an organisation in a number of ways".

One of the issues treated is security awareness. The principle of security awareness is that "Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise". And the objective is "To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities".

When it comes to the specific activities that should be performed, these should be endorsed by top management, supported by a documented set of objectives, based on the result of a risk assessment, and be measurable. It is said, "The effectiveness of security awareness should be monitored by measuring: - the level of security awareness in staff and reviewing it periodically, - the effectiveness of security awareness activities, for example by monitoring the frequency and magnitude of incidents experienced". The Standard doesn't specify any further how the measurements should be done.

The Standard also provides a list of things users of applications should be made aware that are not allowed, like for instance using information or system without authorisation, downloading illegal material, unauthorised copying of information or software, and compromising passwords (e.g. by writing them down or disclosing them to others). The Standard doesn't specify any further how a security campaign should be made to give best effect.

The Standard can be used for remembering what to think of when making a campaign, but not as a description of how to make it.

Within the health care environment the importance of awareness and attitudes is well recognised, and in UK work has been done to start developing a security culture throughout the whole health care environment [Gaun]. In his article, Nicholas Gaunt points out five impediments to change towards a security culture: Attitudes, Ignorance, Conflicting demands, Inadequate systems, and Inconsistent policies.

Even though the article focuses on the health care environment, we believe that these impediments also are applicable to other environments and business sectors. Companies working with awareness and attitudes should therefore have these impediments in mind.

Since a person's attitudes regarding information security are made when he or she is first introduced to information technology, a proposal has been made for introducing information security awareness in secondary education in Greece [Bint]. For instance when given their first password, the teacher should explain to the students why passwords are used, how they should be made, how often they should be changed and so on. By doing this, the students will be aware of security issues at an early stage, and good attitudes can be built. It is easier to create good attitudes of young people than changing the attitudes of an adult.

In his paper "Making information security awareness and training more effective**"** [Thom], Mark Thomson examines the importance of information security awareness programs in modern organisations. An expanded program is suggested to cater for more employee

groupings in the organisation. Security awareness and training programs should be aimed at three diverse employee groupings: top management, IT personnel and end-users.

- Top management need to provide the lead and impetus for the awareness program. They must believe in the need for information security in order to provide the necessary backing needed to make the program a success. Terminology and definitions, business continuity and legal issues are among the topics that should be covered in this phase of the program.

- IT personnel are responsible for the identification, implementation and management of controls, which will 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 topics in this part of the program are assignment of responsibilities, selection of risk analysis strategies and making security recommendations.

- The end-users need information about the information security policy and controls so that they can carry out the laid procedures, which are designed to maintain information security. Possible threats, passwords, viruses and ethics are topics that should be covered in this part of the program.

The success of such a program depends on how this information is presented for the employees. The most important part of the program when dealing with presentation techniques is the end-user program. This is because the end-user is the person carrying out the day-to-day tasks, which could have a severe impact on information security if not carried out correctly. The end-user program must be divided into a number of shorter sessions. During each session, some factors from social psychology can be applied in an awareness program:

- 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 behaviour.

- 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 behaviour.

- Reciprocity. This refers to the returning of a favour. If the attendees feel that the presenter has done them a favour, 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.

There is a definite need for security awareness programs in the workplace. They do, however, need to be properly implemented to ensure that they are as effective as they should be. And to make an awareness program more effective, ensure that the correct information is being addressed at the correct audience, and make use of techniques that will ensure that the attendees will adopt the guidelines presented so that they will become second nature in their day-to-day operations.

It is though not easy to evaluate the effect of a campaign. In the report from a project conducted at Harvard University Graduate School of Education [Coff], it says "There are countless challenges that make evaluation difficult and progress incremental".

As shown in Figure 6, the report visualises a theory of change for individual behaviour change campaigns. This is a general theory and is not specially made for information security. In the first column the various types of message dissemination a campaign might use is presented. The second column contains the short-term and intermediate outcomes from the campaign. This clearly shows that raising the awareness or changing the attitudes is not the ultimate goal of a campaign. What we really want to achieve, as indicated in the third column, is to change the individuals' behaviour.

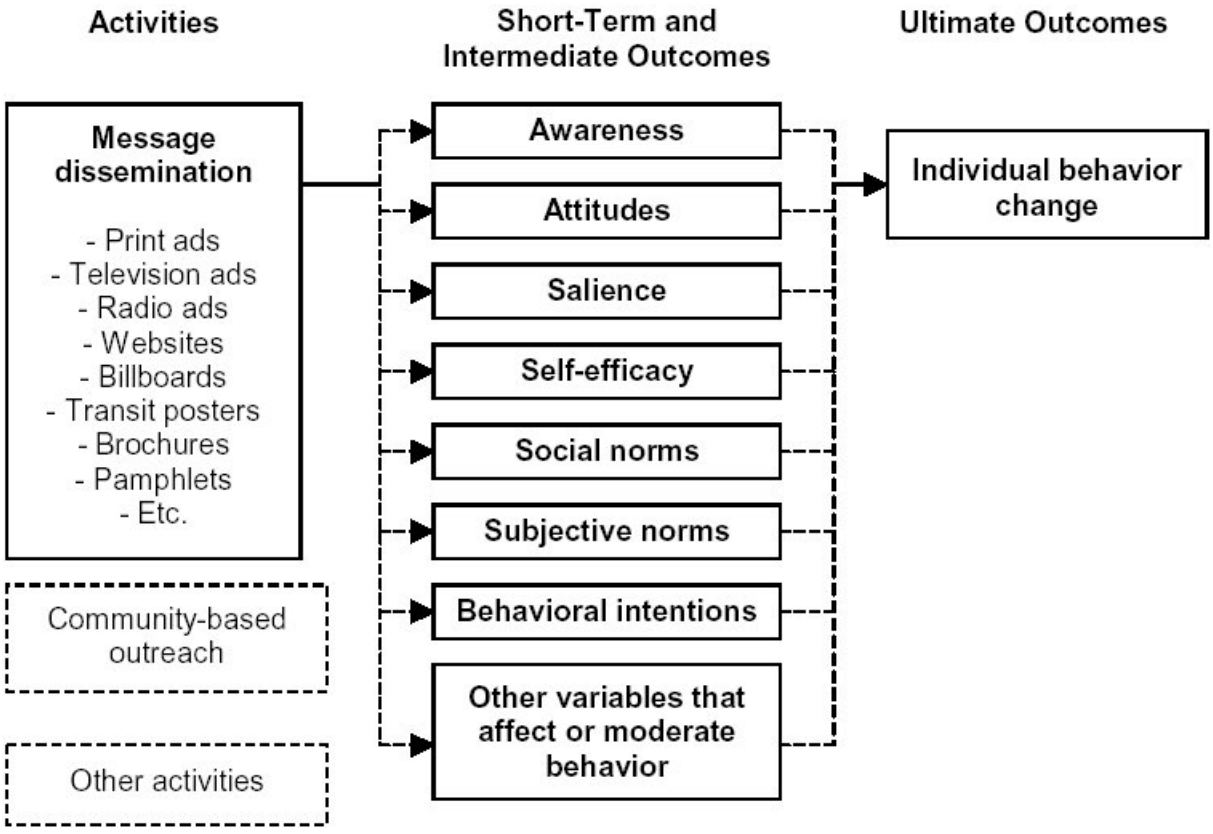

Figure 6 - General theory of change for individual behaviour change campaigns [Coff]

The report describes evaluation of five different campaigns. None of them are related to information security, but the results might still be of some interest for those planning to design and develop a new campaign. Those results will however not be discussed in this thesis.

As many security managers know, an information security policy is an important tool when working with awareness and attitudes. But as stated in [Wood], "policies alone do not constitute a sufficient awareness effort". In his article, Charles Wood claims that there are numerous management misconceptions regarding policies and awareness. He finishes the article with a laundry list of over 50 awareness-raising methods. This list may be valuable to any company wanting to raise the awareness among its employees. 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).

When trying to change the employees' attitudes and behaviour to information security a lot of tools can be used. Information can be given through pamphlets, posters, web pages and pep talks among others. One important document to distribute, as already mentioned, is the organisation'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 [Kowa]. 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 behaviour 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. Even so, the difference in attitudes and behaviour was significant and hence should be thought of when designing an information security campaign.

In his article "Managing Network Security: The Limits of Awareness" [Cohe] from June 1999 Fred Cohen says that awareness has its limits and that its limitations are quite substantial. In the last years there has been a lot of publicity around new computer viruses such as the Melissa virus. Many companies got the virus and got problems with their electronic communication. The anti-virus companies were quick to update their filters and inform their customers of this. Despite of this new viruses still can cause major problems for many companies. Why? It could not be lack of competence. Everybody knows today that computer viruses exist and that they can be dangerous for your network or your computer. Even companies that have experienced problems continue to carry on as usual without fixing the problem once and for all. This should be the height of awareness. You get hit, you know you were hit, you know what it cost you, you know that it could have been far worse, and you know that the cost of getting rid of the problem would be far less than getting hit again. And still you do nothing.

The problem is that there is limits to what awareness can do, and those limits are rather severe. Awareness of serious security problems is not useful unless the people who are aware are serious about security.

When arranging another security awareness campaign we should not expect that the fact of awareness produce good decisions.

3 Survey

3.1 Choice of methods

In this thesis work we intend to look at information security from a practical perspective. The intention is that the results from this work should be of interest for all those working with information security awareness. With this in mind, the following methods are relevant for the work:

- Literature study
- Interviews of security managers in some Norwegian companies
- Use of models and theories for constructing new security metrics

To help decide which approaches to research to use for the different research questions we have used the definitions in John W. Creswell's book "Research Design. Qualitative, Quantitative, and Mixed Methods Approaches" [Cres]. He defines three approaches to research:

- A quantitative approach is one in which primarily postpositivist claims are used for developing knowledge. This means thinking of cause and effect, use of measurement and observation, and testing theories. Data are collected on predetermined instruments yielding statistical data.
- 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.
- In a mixed methods approach, knowledge claims are based on pragmatic grounds as for instance consequence-oriented or problem-centred. Both numeric and text information are collected so that the final database represents both quantitative and qualitative information.

By interviewing security managers in some large Norwegian companies we wanted to find out how they work with attitudes and awareness and if they measure the attitude or level of awareness of information security among their employees. From these interviews we would also find out how such measurements are done in practice. As we draw our conclusions based on answers from a relatively small number of companies, these interviews will be a qualitative approach to research.

At the beginning of this project we were not able to construct questionnaires to be used in a quantitative survey about measurements of awareness, attitudes, and behaviour. We simply did not know exactly what questions to ask. Therefore we chose a qualitative survey with open questions. As John Creswell says: "Qualitative research is exploratory and is useful when the researcher does not know the important variables to examine. This type of approach may be needed because the topic is new, the topic has never been addressed with a certain sample or group of people, or existing theories do not apply with the particular sample or group under study" [Cres].

The goal of this survey is to find best practice in the work with awareness and attitudes among Norwegian organisation. The intention of the work is not to find out how many percent of the companies and organisations in Norway that arrange a special type of campaign, make their employees sign a security document every year, or perform any other special activity. Since no statistical data are collected, this also implies a qualitative approach to research in favour of a quantitative or mixed methods approach.

A qualitative approach to research means that the list of activities and inputs, which comes as a result of the interviews, might not be complete. What one security manager sees as an important activity, another will not mention even though they also do it. The open questions also make the work with analysing the results a bit harder.

To learn how the companies work with awareness, they were asked what they do in this area with questions about making and arranging security campaigns. They were also asked how they measure the effect of their work today. In order to get some good ideas from all the experienced security managers, also from those who don't yet measure awareness, they were asked how they think awareness can be measured.

To find out how we can measure the attitude or level of awareness of information security among the employees in a large company, we wanted to do a literature study. This would show how such measurements could be done, both theoretically and practically. As shown earlier, there has already been done some work in this area. We use this work as we try to be more specific and definite and relate this to Norwegian conditions.

When defining new security metrics we have studied existing models and theories, and we have used existing templates for the definitions. The templates have though been modified to include information about validity and reliability.

To find out how a security awareness campaign should be made to give the best return of investment, we did a literature study. This was combined with interviews of the security managers to make use of their experience. Most companies have arranged several security campaigns and may have at least a feeling, if not definite measures, of which types of campaigns have the greatest effect.

The main part of the project is the collection of data from different companies and organisations in Norway to learn about their experiences with information security campaigns. To accomplish this, the right person or persons in each organisation was identified and interviewed.

Since the purpose of the interviews would be to collect experiences from companies working with information security awareness, we contacted companies that were believed to be security conscious. Therefore we started with the list of members of ASIS Norway [ASIS]. From this list, a selection of about 35 companies from various sectors was made. In addition to those, teaching supervisors at Gjøvik University College and other personal contacts pointed out about 10 other organisations. The identified contact persons were contacted by e-mail with information about the project and the questions we wanted to ask. They were all written in Norwegian since only companies in Norway were contacted. All e-mails sent out were personalised with information about how we found their e-mail address. A representative sample of one such e-mail, translated to English, is found in Appendix H.

All the information given to me during the interviews must be handled in such a way that full anonymity is maintained. To achieve this, no names of companies or persons will be mentioned in this report. For the same reason all the interviewed persons are entitled "he", although some of them are women, and they are also entitled "security manager" even if this may not be the correct title for everyone. In fact several people were interviewed in some organisations. The anonymity of the companies and persons are in this project valued more than the correct sex and title of the interviewed persons. The companies are, though, grouped by industry to see if the work with information security awareness and attitudes in some way is industry specific. Table 2 shows the group division of the industries used and the number of interviewed companies belonging to each industry. The results from these interviews are given in chapter 4 while the complete notes from all interviews are found in the appendices to this report as indicated in Table 2.

Table 2 - Number of interviewed companies in each industry

Industry	Number of companies contacted	Number of companies interviewed	Appendix containing notes from interviews
Bank/Finance	10	4	A
Energy	7	5	B
IT/Telecom	6	4	C
Public activity	11	5	D
Other	10	4	E
Total	44	22	

4 Results

An analysis of the notes from the interviews shows that this survey does not reveal any significant differences between the various business sectors in the way they work with awareness of information security. There are no activities that are common in one sector and not used at all in the others. As mentioned in the last chapter, the fact that one security manager hasn't mentioned one particular activity doesn't necessarily mean that they don't do it.

The fact is there are actually greater differences within some of the sectors than between the various sectors. Therefore we have chosen to present the results from the survey as a whole and not sector by sector. For those interested in one particular sector we encourage to read the full notes from the interviews as they are presented in appendices A through E.

To improve readability, the results from the survey are divided into the same subchapters as chapter 2 - Review of state of the art. Since this division is adapted to the four research questions it should be easy to correlate the results from the survey with the state of the art and with the corresponding research question.

4.1 Working with awareness and attitudes in Norway

The survey shows that the selected companies focus on information security and do a lot of work in order to raise the awareness among their employees. We have got a lot of good inputs and comments from the interviewed security managers on how their company work with awareness and which issues and activities they regard as important. The essence of those interviews is presented in this subchapter, and hopefully this may serve as a form of "best practice" to help other companies in their own work with security awareness.

All the activities and factors mentioned in the interviews are put in one out of ten groups to enhance the readability of the report:

1. **Foundation**

   - For the work with information security to be effective it is important that the top management is involved. If the chief manager isn't concerned about information security, then the working conditions for the security department will be very difficult.

   - It is also important that the work with information security awareness is done in a systematic way. Create a plan for the work and make the top management read it and give their approval before it is implemented.

2. **Education and training**

   - Long-time education and training is important in order to raise the awareness. One single campaign may help for a short period of time, but the effect in a longer perspective is minimal. Continuous work over several years is what helps. And it is important that all employees are given the necessary training and education dependent of their position and work tasks.

- Exercising is the best way to check if for instance contingency plans are followed in a crisis situation. Such exercises, perhaps with external observers, do also help increase the awareness among those employees involved in the exercise.

- Instead of using external teachers in the education and training, the use of mentoring may be more successful. In this way both the "teacher" and the "student" will gain new knowledge. The internal communication in the organisation would also improve as the employees get to know each other better.

3. Incident handling

- Many of the interviewed companies have good systems and routines for incident reporting. When the employees know that all security incidents are reported to the security department, they will hopefully think twice before they do something illegal.

- When it comes to making information about the incidents public to all employees the interviewed companies have different policies. Some never publish this kind of information as they feel it could reveal too much about their security installations. It is also possible that the information could leak outside the company and for instance to the press. Other companies are more liberal and publish some of the incidents on their internal web. This is of course done after a thorough evaluation of each single case. Names of persons or departments are of course never published either.

4. Inspections

- Some companies use external inspections, conducted by for instance the Data Inspectorate [Data], actively to raise the awareness. When managers and employees know they are about to be controlled, they usually do what is needed to improve the security.

- External companies inspect not all organisations. But an internal inspection may have the same effect on the employees as nobody like to get caught doing errors or mistakes.

- In addition to catching people while they are doing something wrong, it could be just as effective catching them doing the right thing. In this way security would be understood as something positive.

5. Communication and visibility

- To communicate security messages to the employees, many companies heavily use the internal web and the intranet. Some security departments have their own web pages or web portal. From these pages it is easy to get in contact with the security staffs by e-mail.

- To distribute important security messages e-mail is often used. Newsletters through mailing lists are also used.

- Pamphlets are often used to communicate simple messages. One common approach is to distribute pamphlets containing ten simple security rules.

- Using posters is another way of communicating simple messages to all employees. Placing the posters at popular meeting places, like for instance at the coffee machine, increases the probability for them being read.

- A unique and uniform branding of security messages can make them more noticeable for the employees. After some time they will recognise a security message just out of the colour, font or logo used in the message.

- It is important that the security staffs are visible and participates in internal meetings, conferences and seminars. Some organisations arrange special security meetings and/or conferences for all employees.

- Many security managers point out the visibility of the security department as very important. The security staffs should walk around in the organisation so that most people know them and then dare to contact them. It should not be frightening for anyone to contact the security department.

- One organisation has established an internal security prize. They hope that both the nomination process and the prize itself will help raise the security awareness.

- One company has an internal security forum that meets regularly and discusses security issues.

6. Surveys

- Several of the interviewed organisations are members of ISF [ISF] and carry out their survey every second year. All of them say the survey is of great importance in the work with awareness. It is not only the survey itself that has a positive effect, but the process of collecting the necessary information throughout the organisation is just as important.

- Conducting an internal survey is a good alternative for those organisations that are not ISF members. Some companies actually do both. Such a survey usually consists of a questionnaire sent out to all managers and/or employees. The intention by making a survey can vary. Some use surveys to see how satisfied people are with the security department while other use surveys to check if the employees are familiar with the security policies and procedures. It is though important that the survey is not too comprehensive and takes too long to complete.

7. Security from day number one

- To ensure high awareness among all employees it is important that security is a natural part of the work from day number one in the organisation. In many organisations security clearance is performed on all employees before they are hired. Making the employees signing a declaration of confidentiality, rules for IT users, codes of conduct, or other security documents is also very common. In some companies the signing process must be repeated yearly to keep up the awareness.

- About half of the interviewed companies say they have a training program that includes information security and is mandatory for all new employees. In some organisations the employees have to go through a security course at regular intervals.

8. Campaigns

- Most of the companies arrange some sort of security campaign from time to time. They are very different both regarding layout and content, but they all try to change the employees' behaviour in some way.
  - Some campaigns are a direct consequence of internal or external incidents or threats while others are part of an approved policy or communication plan.
  - Some use small campaigns, like a quiz on the web, to keep up the awareness. To make as many people as possible go through the quiz, small prizes are often very effective.
  - There are many ways to bring out a message during a campaign. Posters, pamphlets, e-mail, and internal web are the most used, but other things like coffee mats, ice scrapes, reflector disks, comic strips, and ice cream are also used to attract attention.
  - Some organisations say that the most successful campaigns are the ones that give the employees something they can use at home. One example of this is free CDs with firewall software, anti-virus software or anti-spam software for use at their private computers. Making them aware of security threats at home hopefully have a positive effect at work too.
- More campaign ideas are found in the complete notes from the interviews in appendices A through E.

9. Evaluations

- Some also mentions risk management, risk evaluations, and vulnerability evaluations as important parts of their work with awareness. The process of making a risk evaluation or a vulnerability evaluation makes the participating people aware of the risks, vulnerabilities, and threats, and this is often just as valuable as the final report.

10. Documentation

- Classification of documents with corresponding handling-rules can help raise the awareness.
- It is important that it is well documented what the employees are allowed to do and what they are not. Such documentation must be easily accessible for the employees when they need it. Examples of such important documents are the security policy, routines, and procedures. Some organisations have their own rules or handbooks for IT users that contain information security topics.
- It is not enough just to write a policy or a routine and publish it on the internal web. It is just as important that all such documents are revised and updated regularly. Documents that are outdated and full of errors just make the employees loose their respect for them.

All these actions and inputs clearly show that the interviewed organisations put a lot of effort into raising the security awareness among their employees. Hopefully other companies can get some good ideas they can use in their own work. More detailed information about the various actions and inputs are found in appendices A through E.

4.2 Measuring awareness and attitudes in Norway

During the interview, the security managers were also asked if they ever did any measurements related to security awareness or if they had any ideas about how this could be done. The answers to these questions are included in the complete notes from the interviews. This chapter just summarizes the findings.

As in the last subchapter, all actions and inputs regarding measurements of awareness are put into a category. We have used the same categories, as in chapter 4.1, but measurements are only done in the first six of those ten categories:

1. **Foundation**

   - One organisation says they have established Key Performance Indicators (KPI) for information security awareness that is used to measure the managers every year. These are just qualitative and contain questions like "Have you had a security conversation with all your employees during the last year?" Such measurements indicate how concerned the managers are about information security.

2. **Education and training**

   - It is quite easy to measure how many of the employees that go through learning programs in the organisation, and hence some companies do such measurements. But if this says something about the security awareness is an open question.

   - Measuring how many of the employees that go through e-learning programs and complete the final test do perhaps give a better indication of the level of awareness as they check if the employee remembers the most important messages in the program. "For Your Eyes Only" [Easy] is an example of such a program that is used by some of the interviewed organisations.

   - Conducting exercises is a good way to see if people behave as they are supposed to. Some observers can register what is done and what is not, and this can make some good measurements of awareness. Doing a similar exercise again after a while can show if the awareness has increased and the behaviour has improved.

3. **Incident handling**

   - Most companies having a system and routines for incident handling also use this system to measure the number of registered incidents. When the system is first introduced and put into production an increase in the number of reported incidents is expected, as the employees get aware of the new routines. But after a while, perhaps some months or a year, the top is reached and the number will hopefully start to decrease as the employees change their behaviour in order to not get reported.

4. **Inspections**

   - When performing inspections at a regular basis, measurement data can be collected that say something about awareness and behaviour. A number of such inspections measurements have been mentioned in the interviews:

     - The numbers of employees following the company's policy of leaving the desk clean when finishing the day.
     - The number of meeting rooms found OK, i.e. no confidential information left on paper, whiteboard, flip-over etc.
     - Number of times a person gains access to a restricted area by tailgating, i.e. following after an authorised person through locked doors.
     - The amount of paper documents that are shredded compared to the amount that are thrown in the wastebasket.

   - Another form of measurements in this category is to register the amount of illegal or unwanted traffic on the internal computer network. This will give a good indication of how the employees really behave.
   - Statistics for virus attacks or spam-mail provide information about the awareness of the IT department and if necessary software for protection is updated according to the procedures.
   - Measuring how many of the users' passwords that are easily found, using for instance dictionary attacks, also give an indication of the security awareness among the employees.

5. **Communication and visibility**

   - The number of people reading articles on the web indicates if the security messages are reaching out to the employees.
   - The number of requests to the security department or security staffs indicates the level of awareness. These are requests about security issues and not reports of incidents. An increasing number of requests could indicate an increasing level of awareness as this means people are concerned about security and dare to ask.
   - Participation in meetings and conferences also gives an indication of how visible or popular the security staffs are in the organisation. An increasing level of meeting requests probably indicates an increasing level of awareness.

6. **Surveys**

   - One of the interviewed organisations carries out an internal survey every month to check the popularity of the security department, among others, among the employees. Only a few departments participate in each survey, and it is not the same participants every month.

- The ISF [ISF] survey, which is conducted every second year, gives a very good indication of the level of security awareness in the organisation. It can be used as a benchmark against other organisations, but it also shows if the level of awareness has increased or decreased in the organisation since the last survey two years ago.

- Measurements from internal surveys can be used to see if the level of awareness is increasing or decreasing in the organisation.

- Qualitative measurements and questionnaires are pointed out by some of the security managers as possible ways of measuring security awareness.

In the last four categories none of the interviewed companies have done any measurements.

The inputs from the security managers show that there are many ongoing activities for measuring awareness although very few of the organisations use the measurements systematically in improving their work with awareness and attitudes.

The received inputs will in the next subchapter be used when defining some metrics for awareness.

4.3 Metrics for awareness

From the answers given in the interviews we can derive some metrics for awareness. We have identified the following nine metrics that can be used to measure awareness and behaviour in different ways:

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 list is by no means meant to be complete, but hopefully the identified metrics can serve as examples and inspiration for identifying and defining other similar metrics.

In addition to these it is possible to define some metrics that can be measured during exercises and/or surveys. This could be metrics like “Number of ‘dead’ persons in a fire exercise”, “Number of employees familiar with the content of the security policy”, or “Number of employees taking backup of their personal computer regularly”. Such metrics depend on the exercise or survey conducted, and they will not be defined in this report.

When defining the metrics we have used the template defined in [NIST55]. This template is used by NIST when defining the sample metric in Appendix F. We have chosen to do some modifications on this template:

- The cost of doing the measurement is added to the definition, as this information is interesting for every company planning to do measurements. Ideally the cost should have been given as an amount in for instance Euro, but we have chosen to list the factors that influence on the cost rather than presenting a formula for calculating the exact cost.

- Information about validity and reliability is also added to the definition instead of writing comments at the end.

- For some of the metrics proper questions must be asked in order to collect the necessary information. The design of such questions requires a lot of work and is considered out of scope for this thesis. Therefore information about Implementation Evidence is removed from our definitions.

With these modifications, every metric is defined according to the template in Table 3.

Table 3 - Template for definition of a security metric

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.*

Using this template we can define the nine identified awareness metrics. The definitions are shown in Table 5 through Table 13 in Appendix I, and they show that it is possible to measure at least some aspects of awareness and behaviour among the employees.

4.4 Making an effective security campaign

As we saw in chapter 2.4, a lot of work has been done to help organisations in their work with awareness: Chapter 29 in the Computer Security Handbook [Rudo] contains valuable tips when planning and developing a campaign, the article of Charles Wood [Wood] has a laundry list of more than 50 awareness-raising methods, the Special Publication 800-50 from NIST [NIST50] describes the whole process from planning a campaign to measuring the effect, and the Standard of Good Practice for Information Security from ISF [ISF03] provides a set of high-level principles and objectives for information security included awareness. In addition, the workshop report from ISF on effective security awareness [ISF02] is available as help for members of ISF.

From the results of our survey, we can make a list of tips that the interviewed security managers consider most important when planning, developing and arranging an information security awareness campaign. Tips for measuring the effect of the campaign is of course also added to the list.

- Work systematically from planning, through development and implementation to measuring.
- Involve the top management, and make them give their approval to the plan before going any further.
- Make a long-time plan for education and training, as a single campaign won't have any effect in a longer perspective.
- Measure the level of awareness before the campaign is run. This must be done in order to be able to measure the effect of the campaign.
- Develop your own security logo that can be used in all campaigns and other communication from the security department.
- Make sure the campaign focuses on a limited number of aspects of information security.
- Use simple messages that are easy to understand for all employees, not only security people.
- Use humour to catch the attention.
- Present the messages with a twinkle in the eye. This is much better than scare campaigns.
- Use pamphlets with a few, simple messages.
- Place posters with simple messages at popular meeting places.
- Arrange small security quiz on the web with the possibility of winning small prizes.
- Use something popular and useful to attract attention, like for instance coffee mats, ice cream, cookies, or reflector discs.

- Give the employees something they can use at home, like a CD with firewall and anti-virus software to use on their private computer.
- Measure the level of awareness again after the campaign has been run to find the effect of it.
- Continue with periodic and systematic measurements to see when a new campaign is needed.
- Think about validity and reliability when doing the measurements.
- Don't measure too often, but often enough to see a trend.
- Be careful when using the results from the measurements. A change in awareness or behaviour isn't necessarily caused by the campaign. It could just as well be the result of organisation changes or high pressure of work.
- Use the results from the measurements and feedback from the employees when making the next campaign.

As a last tip, we will recommend using available work, like this report and the articles and reports mentioned at the beginning of this chapter, as help in your work.

5 Conclusion

There is an increasing focus on awareness and behaviour in the work with information security today. There are several publications describing best practice in this area, and the number of security companies working with awareness is already high. And many companies are focusing on awareness, attitudes, and behaviour in their work. This survey has shown that the contacted companies and organisations do a lot of work in trying to raise the awareness and improve the attitudes to information security. And the work they do coincide to a great extent with what is recommended in the literature. The list of good tips for making an effective security campaign shown in chapter 4.4 contains many of the tips already published in similar lists. But the interviewed security managers have also provided good tips that are not easily found in the literature.

From what was expected at the start of this project, surprisingly many of the interviewed organisations try to measure the level of awareness and behaviour in some way. Some conduct a survey and ask the employees how they behave when for instance working with security graded information. Others do practical measurements of for instance password strength or amount of unwanted traffic on the internal computer network. Measurements are also done on the results from internal controls. Examples of this are to measure the number of employees locking their computer when not sitting at the desk or the number of employees leaving their desk clean at the end of the day. But what is common for almost all of the interviewed companies is the fact that the measurements are not taken, nor used, in a systematic way. In this field the companies have a potential for improvements.

Based on the inputs from the interviews and available methods and templates, we have identified and defined nine unique security awareness metrics. These cover many different aspects of information security awareness, as for instance training, security incidents, paper shredding, weak passwords, and customer satisfaction. The set of metrics is not complete in any way to measure the awareness and behaviour, but hopefully they may serve as examples and give inspiration for the definition of other similar metrics.

6 Further work

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

Another way to carry on with this work is to measure the level of awareness in one or a few specific areas as for instance paper shredding or clean desk. Then carry out a campaign covering the same area(s) and do the same measurements again after the campaign is run. In this way the effect of one particular campaign can be measured. This work should be done in cooperation with one or a few organisations planning to do a security campaign.

Based on the inputs from the interviews in this survey, it should now be possible to make a good questionnaire that can be used to do a quantitative survey. Such a survey must be done in many companies and organisations and in different business sectors. The purpose of such a survey would be to find out how companies and organisations in one country work with awareness and measurements, and also to compare the work done in different sectors.

In this semester, several of the MSc Theses at Gjøvik University College have focused on security management issues. In addition to this thesis, Mr. Gullik Wold has written about "Key factors in making ICT Security Policies effective" [Wold], Mr. Ola Holm about "Risk management in dynamic environments" [Holm], Mr. Frank-Arne Stamland about "Is BS7799 worth the effort?" [Stam], and Ole Kristian Målbakken has written about "Measuring legal compliance" [Målb]. Correlating the results from these five theses may give valuable knowledge in the area of information security management.

Bibliography

[AIS] Advanced Information Security web site (developers of ISAP) http://www.ais.as/ II

[ASIS] American Society for Industrial Security - Norway web site http://www.asis-norway.no/index.html 22

[AT&T] Achieving Network Security - An AT&T survey and white paper in cooperation with the Economist Intelligence Unit. 2003. Electronic version found at http://eb.eiu.com/upload/Network_Security_White_Paper_FINAL.pdf 1

[Atte] Atterbury Foundation web site http://www.atterbury.org/ XXXVIII

[Bint] A. Bintziou, N. Alexandris, V. Chrissikopoulos. Introducing IT-Security Awareness in Schools: The Greek Case. *Proceedings of the IFIP TC11 WG11.3 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden, pp. 247 – 257.* Electronic version found at http://citeseer.nj.nec.com/ 17

[Coff] Julia Coffman. Lessons in evaluating communications campaigns. Harvard University Graduate School of Education. June 2003. Electronic version found at http://www.gse.harvard.edu/hfrp/content/pubs/onlinepubs/lessons/lessons.pdf 19

[Cohe] Fred Cohen. Managing Network Security: The Limits of Awareness. *Network Security.* June 1999. Electronic version found at http://www.sciencedirect.com/ 20

[Comm] Commissum web site http://www.commissum.com/ 8

[COSO] The Committee of Sponsoring Organizations of the Treadway Commission web site http://www.coso.org/ I

[Cres] John W. Creswell. *Research Design. Qualitative, Quantitative, and Mixed Methods Approaches.* Second Edition. SAGE Publications 2003. 21

[CSA] Computer Security Awareness web site http://computersecurityawareness.com/ 8

[Dale] Erling Lars Dale. *Pedagogisk profesjonalitet*. Ad Notam Gyldendal, Oslo. 1989. I

[Data] The Data Inspectorate web site http://www.datatilsynet.no/ .....26; XIX

[Easy] Easy i web site (developers of the e-learning program "For Your Eyes Only") http://www.easyi.com/ .....9; 29; II; IV; XV; XVI

[Gaun] Nicholas Gaunt. Practical approaches to creating a security culture. *International Journal of Medical Informatics 60 (2000)*, pp. 151 - 157. Electronic version found at http://www.sciencedirect.com/ 17

[GetI] Get Insight web site http://www.getinsightnow.com/ .....8; XXXVII

[GISS] Ernst & Young. Global Information Security Survey 2003. Electronic version found at http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf..... 1

[Holm] Ola Holm. Risikohåndtering i dynamiske omgivelser. MSc Thesis. Gjøvik University College, June 2004. 37

[ISF] Information Security Forum web site http://www.securityforum.org/html/frameset.htm ..... 2; 5; 27; 31; IV; VI; XV

[ISF02] Information Security Forum. Effective Security Awareness - Workshop Report. April 2002. 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 11; 16; 33; VII

[ISF03] Information Security Forum. The Standard of Good Practice for Information Security. March 2003. Electronic version found at http://www.isfsecuritystandard.com/index_ie.htm ..... 17; 33; VII

[ISF91] European Security Forum. Security Status Survey 1991, IT Security Awareness. September 1991. 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 5

[ISF93] 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 2

[ISO] International Organization for Standardization web site http://www.iso.org/iso/en/ISOOnline.frontpage ..... VI; XV

[ITIL] IT Infrastructure Library web page http://www.itil.org/ VIII

[ITL] Training for information technology security: Evaluating the effectiveness of results-based learning. *ITL Bulletin.* June 1998. Electronic version found at http://sbc.nist.gov/PDF/NIST_ITL_Bulletin_06-98_Training_Results_Based_Eval.pdf 10

[Kats] Sokratis K. Katsikas. Health care management and information systems security: awareness, training or education?. *International Journal of Medical Informatics 60 (2000)*, pp. 129 - 135. Electronic version found at http://www.sciencedirect.com/ 11; 12

[Kowa] 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 20

[Målb] Ole Kristian Målbakken. Measuring legal compliance - A case study on Directive 95/46 EU, article 17 security in processing. MSc Thesis. Gjøvik University College, June 2004. 37

[NaIn] Native Intelligence web site http://nativeintelligence.com/ ..... 8; XXXI

[NIST] National Institute of Standards and Technology web site http://www.nist.gov/ .... 2; 10; XXXV

[NIST16] Mark Wilson (Ed.), Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, John B. Ippolito. Information Technology Security Training Requirements: A Role- and Performance-Based Model. *NIST Special Publication 800-16.* April 1998. Electronic version found at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf http://csrc.nist.gov/publications/nistpubs/800-16/Appendix_E.pdf.....2; 10; 12; 14

[NIST50] Mark Wilson and Joan Hash (NIST). Building an Information Technology Security Awareness and Training Program. *NIST Special Publication 800-50,* October 2003. Electronic version found at http://www.csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf ..... 11; 12; 13; 14; 15; 16; 33; XXIX

[NIST55] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash and Laurie Graffo (NIST). Security Metrics Guide for Information Technology Systems. *NIST Special Publication 800-55*, July 2003. Electronic version found at http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf..... 11; 32

[Noti] Noticebored web site http://www.noticebored.com/index.html..... XXXVI

[NSM] Nasjonal Sikkerhetsmyndighet web site http://www.nsm.stat.no/.....5; XVI; XXVI

[NTNU] Norwegian University of Science and Technology web site http://www.ntnu.no/ ....5; XVI; XXVI

[PDA] Datatilsynet. Act of 14. April 2000 No. 31 relating to the processing of personal data (Personal Data Act). April 2000. http://www.datatilsynet.no/lov/loven/poleng.html . II; XIX; XX; XXIII

[ROSS] Ivar Kufås, Roy Are Mølmann. Informasjonssikkerhet og innsideproblematikk. Rapport nr. ROSS (NTNU) 200301. Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. 2003-06-30. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf.....5; XVI; XXVI

[ROSS01] Eirik Albrechtsen. A review of the insider threat to organisations' information security level. Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. December 2002. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf..... 5

[ROSS02] Roy Are Mølmann. The Human Factor – Taxonomy for classifying human challenges to information security. Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. May 2003. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf..... 5

[ROSS03] Ivar Kufås. A Framework for Information Security Culture – Could it Help on Solving the Insider Problem? Norwegian University of Science and Technology, Department of Industrial Economics and Technology Management. December 2002. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf5

[ROSS04] 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. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf 5; 6; 11

[ROSS05] 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. Electronic version found at http://www.nsm.stat.no/dokumenter/Informasjonssikkerhet.pdf 5; 6; 7; 11

[Rudo] 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 15; 33

[SeAw] Security Awareness Incorporated web site http://www.securityawareness.com/index.htm ..... XXXIII; XXXIV

[SecA] Department of Defence. Act of 20 March 1998 No. 10 relating to Protective Security Services http://www.ub.uio.no/ujur/ulovdata/lov-19980320-010-eng.pdf ..... XXV; XXVI

[Stam] Frank-Arne Stamland. Is BS7799 worth the effort? MSc Tesis. Gjøvik University College, June 2004. 37

[Syma] Symantec web site *http://www.symantec.com/* 8

[Thom] 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/ 17

[WASC] Western Administrative Support Center, Western Region Security Office web site http://www.wasc.noaa.gov/wrso/index.htm XXXII

[Wold] Gullik Wold. Key factors in making ICT Security Policies effective. MSc thesis. Gjøvik University College, June 2004. ..... 1; 37

[Wood] 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/ 20; 33

[Yngs] Louise Yngström and Fredrik Björck. The Value and Assessment of Information Security Education and Training. *Proceedings of the IFIP TC11 WG11.3 First World Conference on Information Security Education, 17-19 June 1999, Kista, Sweden, pp. 271 – 292.* Electronic version found at http://citeseer.nj.nec.com/ 9

Appendix A – Interviews in sector Bank/Finance

Company B1

This company is part of a global group. They never arrange any special security campaigns, but the security manager points out these activities as the most important:

- They have risk management as a part of the internal project control. They use COSO [COSO], a model and a framework for operational control and revision. This spans from emergency plans to financial risk.

- They arrange large exercises with observers every year. The observers register what is done and why. From these observations the need for education is revealed. Similar exercises are arranged every year, and from these it is possible to see the effect of any training and educational measures carried out during the last year.

- All new employees must be given a security clearance and must study the company's security profile. In a conversation with the manager they learn about the responsibility of the individual employee. If they are, for some reason, not comfortable with that, necessary educational measures are taken.

- In connection with education and training they use mentoring to a great extent. For instance, the network administrator, who has competence on network security, can be used as mentor and be responsible for teaching sales personnel how to connect their laptops to the internal network via Internet in a secure way. The employees are positive to this kind of training. Both sides get a better understanding of the others' needs and challenges in their work, and both the mentor and the students benefit from this.

- Long-term education is very important. This company has been working very actively with information security for the last six years and now they start getting the right attitudes and awareness among their employees.

- Didactic rationality[1] is another important catchword for this company's educational work.

[1] *Erling Lars Dale uses a model with three competence levels to describe different sides of the concept didactic rationality [Dale]:*

- *Level K1 is about the concrete teaching/ learning process where the relation between teacher and student is central. Didactic rationality here means the ability to evaluate the content of an expressed plan.*
- *Level K2 is about development of learning programs. It is a work concerning transforming curriculum goals into concrete plans for practical use. At this level didactic rationality means to see the connection between formalised expectations and the organisation's compliance with those.*
- *Level K3 concerns construction of, and communication with, a didactic theory where critical thinking, arguing and discussions about definitions are important. At this level of didactic rationality, the organisation's ability to rational renewal depends on the members' rational behaviour. Critical discussion becomes the main foundation for rational renewal.*

Company B2

This company is a Norwegian finance institution. They are working actively with awareness and attitudes both on a daily basis and through special campaigns. Their major activities are as follows:

- This organisation develops and uses e-learning programs when educating the employees. One of the security programs focuses on the Personal Data Act [PDA] and how this affects the employees' work. It is measured how many of the employees go through these programs.
- They have also implemented an e-learning program for raising the awareness and measuring the understanding of information security. This is a commercial product called "For Your Eyes Only" (FYEO)[2] developed by Easy i [Easy].
- Education within Health, Security and Environment also includes a module about information security.
- All in all the company do have several learning programs that focuses on awareness and attitudes to information security, but they are not mandatory for all employees to go through.
- They use the Intranet to communicate information security messages. Here simplification of the message is very important.
- The company depends on the employees following established and documented routines. They use internal control to ensure this is happening.
- In conjunction with incident reporting they are now doing a pilot implementation of a commercial tool called ISAP developed by AIS [AIS]. This is a large tool for incident reporting and risk management and will include areas like financial crime and information security. They hope this tool will help improve the work with security incident reporting.
- All new employees must read and sign the company's codes of conduct, a declaration of confidentiality, and the company's security policy before they can start working.
- Recently all employees were given a pamphlet with all they need to know about security in the organisation. It is important that the messages in such pamphlets are kept as simple and clear as possible.

[2] *For Your Eyes Only is an e-learning program developed by Easy i. The program focuses on information security awareness. The employee needs about one to three hours to go through the whole program, and it ends with a quiz that indicates if the messages of the program have been understood. The program won't be marked as fulfilled until the test is passed.*

Company B3

This company is a regional financial institution in Norway. The security manager outlines these issues as the most important in their work with awareness and attitudes:

- The company is working with attitudes and awareness in a regular manner, focusing more on education and training than arranging special security awareness campaigns.

- All new employees are trained in information security. This is a half-day course that is mandatory for all new employees, including temporary staff and leave substitutes like for instance students working in their summer holidays.

- As already mentioned, the company does not rely on security awareness campaigns, but from time to time they do arrange small campaigns. Those campaigns are developed and made within the company. They have never bought one of those awareness campaigns available from security companies.

- The management is focusing on information security in their regular meetings.

- The chief manager is very concerned about information security. This influences the work with security in the whole organization, both among the other managers, the security staff, and all the other employees. A security focused chief manager is essential for succeeding in the work with awareness and attitudes among the rest of the staff.

- Every month an internal survey is conducted within the company. It is though, not the same departments that are asked every time. But during a year, every employee will have participated in the survey a couple of times. This survey tends to measure how satisfied the employees are with the various staff departments. The security department is one of those departments that the employees are asked to say what they think about. The results from these surveys show that the employees in the organisation are very satisfied with the security department and the work they do. This means that the employees know about the security department and what they do, and it is also reasonable to believe that they are aware of information security issues.

- The company does not do any other measurements in order to check if the awareness and attitudes are at an acceptable level.

Company B4

This company is a Norwegian financial institution. They are working very actively with information security and have a strong focus on awareness and attitudes:

- Some years ago they implemented and started to use the e-learning program "For Your Eyes Only" [Easy] (see note 2 on page II). This is considered as basic training within information security, and all new employees must go through the program and pass the finishing test. The implementation of this program has been a success in this organisation, and about 80-90 percent of all employees have taken the course and passed the test.

- They usually carry out one or two large security campaigns every year. These are often combined with some sort of control. For instance did one campaign focus on the request for employees to carry visible identification at work. In addition to sending out information to all employees, a control was held during the campaign period. Those not carrying visible identification were contacted by the security staff and informed about the campaign. They were also given a cardholder if they didn't have this.

- Every week a new security tip is placed at the front page of the internal web. To read the whole article the user must click on the link. Approximately 30 to 40 percent of the employees read those articles every week.

- The security department has its own pages on the web where the users can find links to security related information. From those pages it is also possible for all employees to send e-mail to the security department with questions or comments about security.

- The company is planning a new campaign where the theme is shredding of classified paper documents. In addition to information to the employees about this topic, the security staff will help them by making available a large paper-shredding machine. By doing this, the security department can measure how much paper are shredded.

- All security incidents are reported and handled. In some cases, an actual incident is used as an example in the weekly security tip on the internal web without saying that it is a true story. Other incidents are made public on the internal web, but of course without any names, neither of persons nor departments. The company considers this as useful in the work with awareness and attitudes.

- Logging of traffic on the internal computer network shows the amount of illegal or unwanted traffic. The measurements are not done systematically. Therefore there exists no quantitative measurements of illegal traffic, but it gives an indication of how big this problem is.

- This company is a member of ISF [ISF] and goes through their survey every second year. The survey is used very actively in making employees, especially system owners and IT staff, aware of information security issues. The survey is also used to measure the level of security in the company. It is possible to see how well security is handled in this company compared to other companies in the same country, in the same region, or in the same industry. The results from the survey also show how the company is doing compared to previous surveys, and hence it shows if the organisation is heading in the right direction.

Appendix B – Interviews in sector Energy

Company E1

This company is part of a global group where the corporate staffs are responsible for all policies. Yet some initiative is taken locally to improve attitudes and increase awareness. These are the major activities in the work for better attitudes:

- All documents are classified in one of four classes; Open, Internal, Company Confidential and Company Secret. Guidelines describe how documents in each category are to be handled. Unfortunately not all documents are handled according to those guidelines.

- This company practices clean desk. From time to time inspections are carried out to ensure that everyone follow this principle. Classified documents, laptops etc. found unguarded are collected by the inspectors. Also common areas on the file servers are checked for files that should not be there.

- Every second year a large "health survey" is carried out in the group. This questionnaire includes topics like awareness and attitudes.

- All new employees are informed about the security policy in the group. They must confirm that the rules are understood and will be followed by signing a document.

- All traffic on the internal computer network is logged to reveal any illegal activity. Depending on the degree of seriousness every breach of rules will have some consequence. Such incidents are not communicated to the rest of the employees as this may reveal information of what is logged and which security measures are implemented.

- Last year a campaign was carried out where all employees got a CD with anti-virus software for use on their private computers. In addition posters were put up and small coffee mats with a rebus was given out. This campaign was very popular among the employees since they got something they could use at home. There was a chance of winning a small prize for those who solved the coffee mat rebus.

- This year the security department has sent out information about spy ware and how to get rid of those. Also this is something that can be useful at the home computer, and so people are positive to this initiative.

- The next similar campaign will probably be free anti-spam software for use at home. It has shown that giving the employees something they can use to improve information security at home is very popular. And hopefully this leads to better attitudes and increased awareness at work too.

- The company has an internal security forum consisting of several managers. Every month they are presented statistics over virus attacks which make them more aware of that threat.

Company E2

This company is also part of a global group. They are member of ISF [ISF] and certified according to ISO 17799 [ISO]. The company works continuously with awareness and attitudes, and their major activities can be summarised as follows:

- The company's Intranet is used actively as a communication channel for information security issues. Policies, guidelines etc. are available for all employees on this network.

- All new employees and hired consultants have to sign a declaration of confidentiality after having read the distributed folder about information security. In addition an introductory course is held. About ½ - 1 hour of this course is about security.

- The company has a development program for managers. This program includes one whole day about security, and attitudes and awareness are important parts of this.

- Half-day information meetings on information security have been held where all employees were invited. There were both external and internal speakers on those meetings, included representatives from the management. Some of the lectures were of a technical nature. The meetings were very popular among the employees and the attendance was large. The internal speakers have later been invited to other meetings in the organisation to speak about information security.

- From time to time special security awareness campaigns are held. In the last one, internal experts on layout and graphics design were engaged to make sure the message was clear and understood by the employees. It is important to keep the message as simple as possible. The aim of this campaign was to inform the employees about the company's fundamental conduct requirements. These codes of conduct were listed in a small folder that was distributed to all employees. To mark the start of the campaign, which was held in December, and to make sure as many as possible noticed the campaign, all employees were served Christmas cookies and mulled wine when they arrived at the office, and they also received a reflector disc since this was a security campaign. The security department received positive feedback from the employees after this campaign.

- The HSE department (Health, Security and Environment), which also has a responsibility for security, has used large posters to communicate the security messages. They have also managed to get security in as a KPI (Key Performance Indicator). Although the security indicators are strictly qualitative, managers and departments do get measured on their work with security.

- All security incidents are to be reported, and the security manager sees an increasing number of reported incidents as an increased level of awareness.

- The contingency plans are being tested regularly to see if the documented routines and procedures are being followed.

- Site audits, included social engineering tests, are carried out regularly. They give a good snapshot of the security situation in the organisation.

- As already mentioned, this company is a member of ISF and they use this organisation actively. The survey is carried out every second year, and it gives a good indication of how this company is doing on the security area compared to other companies as well as a comparison against how this company was doing in the previous surveys. They also use the ISF Workshop Report "Effective Security Awareness" [ISF02] and "The Standard of Good Practice for Information Security" [ISF03] in their work as these documents show the best practice on this field.

Company E3

This company is part of a global group. The security manager is part of the corporate staff, and he is responsible for defining policies and best practice in the information security area. He is also the one taking initiative to arrange special security awareness campaigns. The individual area of operation can apply for permission to make local adaptations to the policies. The major activities within the area of awareness and attitudes in this organisation is as follows:

- About one year ago this organisation started to work systematically with information security awareness and attitudes. This is done by first making the top managers in the group aware of the security challenges in the organisation. Thereafter the managers of the individual areas of operation, local information security managers and special departments like the Health, Security and Environment department were the target group for information from the security manager. Steering documents, guidelines and best practices were made and distributed. Finally the focus was set at the rest of the employees. A campaign was made with pamphlets containing 10 simple security rules.

- Their security campaigns are very event driven. A campaign is often started as a result of an internal or external security incident.

- According to the policy, all security incidents shall be reported. The company is about to start using ITIL[3] for service management, and they believe this will improve incident reporting and give better statistics of the number of incidents etc.

- The company has lots of measurements data, like for instance number of viruses removed, number of spam-mail removed etc., but none of these are used systematically to measure the level of awareness and attitudes.

- The security manager counts the number of requests by phone or e-mail and interprets an increasing number as a sign of increasing awareness among the employees. He also registers an increasing number of invitations to meetings and conferences, something that also indicates an increasing level of security awareness in the organisation.

- The security department is planning a campaign on social engineering.

- Information about internal security incidents are made public for all employees if it can have a positive effect for the company, but in general this company is very restrictive to do so. But such incidents do get a consequence for the employees involved.

- All new employees have to sign a declaration of confidentiality and they are given the necessary security training. An information day for all new employees also deals with information security. There are plans for making the employees having to sign the declaration of confidentiality every year and at the start of special projects.

---

[3] *ITIL is the acronym for the "IT Infrastructure Library" guidelines. According to their web site, "today, ITIL is the de-facto global standard in the area of service management. It contains comprehensive publicly accessible specialist documentation on the planning, provision and support of IT services." [ITIL].*

- The meeting rooms are checked frequently to see that no confidential information is left by the participants on paper, flip-over, whiteboards etc.

- The security manager says that awareness and attitudes must be measured qualitatively and that the measurements must be done quite often. It is also important to measure in special periods like Christmas and Easter. It is the security department that should be doing such measurements.

Company E4

Also this company is part of a global group that takes security seriously. They work actively with security awareness in many ways:

- The company develops a program for security awareness every year. This program focuses on security in general, not information security in particular. The program is presented for the top management, and they must give their approval before the program is implemented in the organisation. A typical yearly program may look like this:
  - Early in the year the employees get new batteries to use in their fire alarms at home. New fire alarms are also handed out to those who need it.
  - The campaign before Easter focuses on the mountain codes, the danger of avalanche, the need to use suntan lotion etc.
  - In May it is a campaign for making the employees use their bicycle at work. In conjunction with this the company offers a free check of bicycles for the employees and their families.
  - In the summer a special security day is arranged. This is an annual happening that goes on for the 12th time this year, and it is open for employees and their families. The focus on such a day may be on drowning, traffic security, home accidents etc.
  - The autumn campaign is arranged in cooperation with a car driver organisation where the employees can get their car checked to see if lights, tyres etc. are as they should be.
  - The campaign in December focuses on the danger of fire, use of candlelight, doughnut cooking etc. It also focuses on cleaning the desk before Christmas holiday.
  - Every third year the employees must attend a course on defensive car driving.
  - All of these campaigns are developed and made within the company itself. The effect of them is not measured, but the company believe all the campaigns help to increase security awareness among the employees.
- The most important campaign, when it comes to information security, is inspections. Last year every office and department was inspected to see if paper documents were treated as they should, if personal computers were locked etc. The goal this year is to do the same inspection at 10 percent of the offices.
- All new employees must attend a security course. In addition an awareness-training course is mandatory for all employees every year.
- It is important to focus on information security at all time to get the attention from the employees. Posters are used as well as participation in meetings.

- The security manager emphasizes one activity as very important in the work with awareness, and that is to catch somebody doing something right. That is much more effective than catching someone in doing something wrong. In this way the employees will consider information security as something positive.

- Without going into details, the company performs a lot of information security measurements that are used in enhancing their work.

- The security manager also emphasizes the importance of education and knowledge among the employees in order to change their behaviour. Because it is their behaviour that must be changed, not their attitudes. A person's attitudes are made during the four first years of living, and they are very difficult, if not impossible, to change later. All the failed campaigns to change people's attitudes to car driving, smoking etc. throughout the years show this. It is therefore useless to try to change the attitudes to information security among the employees. What we need is to increase the awareness and to change the behaviour through knowledge and education.

Company E5

This company is part of a global group where both securities in general and information security in particular are very important.

- In order to make the employees behave as they are supposed to do, both force and information is used. The use of passwords is one example of this. On the company's servers a password policy is implemented forcing the employees to use strong passwords. But many of the applications used in the company reside on external servers where this company does not control the password policy. Then information is the only way to ensure that strong passwords are used nevertheless.

- The company now has focus on computer viruses in their work with awareness. Here again it is a combination of force and information. It is impossible for the users to install anything on their computers due to technical measures. The work with awareness therefore focuses on e-mail based viruses as these may come into the network before the anti-virus software is updated with new signatures. To prevent viruses on the internal network it is important to make the employees not to open any unknown attachments in e-mails. Informing about the threats via the intranet, information meetings and posters does this. The employees can also use the company's anti-virus software on their private computers at home. This will hopefully make them aware of the virus problem and keep them from double-clicking on every attachment by default.

- New security messages and articles are often published on the internal web with a link or a banner on the start-page for all employees. If it is an extra important message that must be distributed quickly, e-mail is sent out from the security department to all employees in the organisation.

- This company seldom arranges special information security awareness campaigns.

- No measurements on information security awareness are done in the Norwegian part of the group. The security manager knows however that some forms of measurements are done in other countries, but he has no detailed information about those measurements. And they are also out of the scope for this Norwegian survey.

Appendix C – Interviews in sector IT/Telecom

Company IT1

This Norwegian company is part of a global group, and the security manager mention these as their major activities for increasing awareness of information security:

- All new employees must go through a 1-day course where information security is an important part. They must also sign a security declaration stating what they can do and what they can't. All contract workers must also sign this declaration before they are allowed to work for the company.
- Information security is very important for this company, and the management is engaged in the work.
- The security policy is available on the internal web for all employees to read.
- They do not use security campaigns to a great extent, but they arrange a couple of small campaigns every year.
- The security department is very active and strive to be visible in the organisation, both on the web and physical out among the employees.
- The company has developed a handbook for IT users. This book contains information about security and is handed out to all employees.
- All security incidents are to be reported to the security department. They consider, for each single incident, if it shall be made public for all employees.

Company IT2

This company is part of a global group. They work continuously with awareness and attitudes to information security. In addition special campaigns are carried out from time to time. Their major activities are as follows:

- Intranet is a very important channel of communication for security related information.
- Direct e-mail is also used for communication between the security manager and the other managers.
- Special awareness campaigns are held approximately every second or third year depending on the need.
- All security policies are revised and updated every year. It is important that these are not outdated if the employees are to follow them.
- Every new employee has to go through a security course on approximately 1 hour.
- They have some ethical rules, or codes of conduct, that every employee has to read and sign once a year. These include, to some extent, rules for information security.
- Once a year every manager gets a questionnaire from the security manager with about 24 questions regarding security. These must be answered and returned, and they form a good basis for statistics about information security. It is, among others, these returned answers that show the need for special security campaigns.
- In an attempt to measure the attitudes among the employees, they measure how easy it is for an unauthorized person to enter a restricted area by tailgating, i.e. following close after an authorized person through a secured door. Letting people from the security firm do practical sampling tests from time to time does this. The results from such tests indicate how the employees' attitudes are towards this threat.
- This company is practicing clean desk, i.e. all employees must remove paper documents, laptops etc. before leaving the area. Every manager is responsible for checking this once every quarter of a year and must report the results to the security manager. All classified documents and laptops found during such an inspection are collected and locked down. The rightful owner will have to contact his manager to get it back. This practice helps the company keeping their desks clean.

Company IT3

The security manager has the responsibility for information security in a large Norwegian group. He is responsible for the work with awareness and attitudes in the whole group, but some initiative is also taken locally in the individual company.

They carry out several types of awareness campaigns, both general ones and more specific. Their major activities are as follows:

- Pamphlets and intranet are used in special situations as for instance in conjunction with large virus attacks. This typically happens four-five times a year.
- All employees must go through the e-learning program "For Your Eyes Only" [Easy] (see note 2 on page II) that covers the NS/ISO 17799 standard [ISO]. Violating the group's security rules may result in the employee having to take the e-learning program and the test again.
- Small web campaigns are conducted from time to time. These are small questionnaires with approximately 20 multiple-choice questions that won't take more than 5 minutes to complete. Small prizes are drawn among those having correct answers.
- Large posters with 10 simple rules are located at strategic spots around the building, for instance at the coffee bar.
- About 12 to 15 internal controls are held each year. These help raise the awareness about information security.
- Several vulnerability evaluations are conducted throughout the year. Results from these evaluations are presented for those employees affected leading to raised awareness.
- Several emergency exercises are held during a year. Observers register the behaviour of the employees. This is a way of measuring the attitudes. It is sad to say that there is very little improvement in attitudes despite all the campaigns. At fire tests many people don't behave as they are taught. Maybe they know it's a test because nobody are ever struck by a fire…
- The security department has an e-mail address where all employees can send requests about information security. It is of great importance that all requests are replied to within a short time. There are an increasing number of requests to this mailbox, something that indicates a growing awareness among the employees.
- Security incidents have been reported for the last three years. After an increasing number of reported incidents during the first six months, the number is now decreasing. People seem to have noticed that all security violations will be reported to the management, and hence they behave differently.
- The group is a member of ISF [ISF] and carry out their survey every second year. Many employees are involved in this work, leading to increased awareness among those. The results from the survey are also presented for the employees in order to raise their awareness and improve their attitudes.

Company IT4

This company is part of a global group. They have an active security department that has many activities in order to raise awareness to information security:

- All new employees must sign the company's rules for IT users and it's codes of conduct.
- The security department has it's own web pages with links to policies, procedures, relevant laws and articles. Links to new articles and banners to campaigns are placed at the home page so that everyone sees it when launching their Internet browser.
- Direct e-mail is also used to employees subscribing to this service.
- The security department arranges an annual internal security conference for the whole organisation. The attendance to this conference is increasing from year to year.
- They have established an internal security prize. The prize that consists of a diploma and a gift of considerable value goes to a person outside the security staffs that have done a special effort in the security work. Everyone in the organisation is free to suggest candidates for the prize, and this will hopefully help increase the security awareness in the company.
- The company is about to make the security-training program "For Your Eyes Only" [Easy] (see note 2 on page II) available on the intranet. The employees will be encouraged to go through the program, and there will probably be some small prizes to win in order to get as many participants as possible. The program will at this time not be made mandatory for all employees.
- About once in a month the security department arranges free breakfast meetings where a representative from the security staff talks about a special security topic like computer crime, corruption or the security act.
- This organisation was involved in the pilot project of NTNU [NTNU] and NSM [NSM] in 2002/2003 [ROSS] and they are planning to do a new survey again this or next year. Perhaps the greatest value with this survey is the fact that many employees did answer. Both the questions and the answers demand some brainwork, and hopefully this will help raise the awareness. The results from the survey also pointed out some areas where action was needed. The feedback from the employees was mainly positive, but some said the survey was too big and comprehensive.
- The company is a member of ISF [ISF] and carry out their survey every second year. This involves many people in the organisation and helps raise their awareness to security. In fact the experiences with this survey are so good that a subset of the survey will be used internally in some departments the years in between.
- Branding of security is considered important. A logo and a slogan are developed for use in presentations, reports and documents. This will make it easier to recognise the security messages.

- Several campaigns are arranged during the last two years, and all of them have the same image; a yellow smiley is used to attract attention, there are no scare campaigns, and the message is presented with a twinkle in the eye. Another thing all campaigns have in common is a reference to the security portal on web for more information. These are some of the arranged campaigns:
  - Hundreds of posters and stickers were posted on doors and boards in the buildings on the day the new security portal on web was opened. This made people aware of the new web pages, and thousands of hits were registered on the first day.
  - A photo story focusing on social engineering was published in the internal magazine.
  - One day last summer all employees got a pamphlet with ten simple security rules. A part of the pamphlet could be exchanged in an ice cream during lunchtime. This was a very popular campaign as the weather was warm that day.
  - In the autumn all employees got a yellow ice scraper with a small security tip printed on it.
  - The ongoing campaign focuses on e-mail. This campaign consists of comic strips where a new strip is published on the intranet every week.
- The company has done some measurements, for instance on password strength, but these are not used systematically to measure the effect of the security awareness campaigns.

Appendix D – Interviews in sector Public Activities

Company P1

The security manager in this organisation has been working with information security for many years. He claims to have great experience in what does not help to improve attitudes or raise awareness. Many of the employees work with personal data all day, and they are therefore familiar with the concept of privacy, the Personal Data Act [PDA] and the Norwegian Data Inspectorate [Data]. Those people are, with the exception of security staff, the ones with the best attitudes to information security. The challenge is to reach all the other employees in the organisation. What they do to manage this can be summarised as follows:

- They have been doing a lot of work with security manuals, security policies and security organisation. The effect of this work is though minimal if no one ever read what is written.

- It is important to get the employees involved in the security work. This is done through a process-oriented risk evaluation where many people are engaged in the work.

- Another important element is internal control as this is also described in the Personal Data Act [PDA].

- They also use inspections from the Data Inspectorate as an element in improving the attitudes. At least the managers react when they know an inspection is scheduled. And the management is very important in the work with attitudes to information security. If they don't care about security they can't expect their employees to do either.

- Some security courses have been held and some pamphlets are given out, but the effects of these initiatives are not known.

- They are about to start reporting and handling security incidents, and they hope this will have a positive effect on awareness and attitudes as this is absolutely needed among many of the employees.

Company P2

The security manager has been working in this organisation for the last four years. Without having done any formal measurements he claims that the awareness has been increased and the attitudes have been improved over this period with respect to information security. What he sees as the most important elements in their work with awareness can be summarised as follows:

- All necessary security documentation exists. It is well structured and available on intranet for all employees.

- The top manager, who has the formal responsibility for the security in the organisation, takes this part of the job seriously. This marks the awareness and attitudes to information security among the employees. It is though big differences among the various departments and sections. Those people who are used to work with sensitive personal information and the Personal Data Act [PDA] have the best attitudes and highest awareness.

- All new employees must, during their first six months on work, go through an organised training programme. This programme covers everything a new employee must know, and information security is a part of that. The problem is that you can do many fatal mistakes in the months prior to the course.

- The security manager wants all employees to sign the rules for information security. In this way they will learn where to find those rules, and hopefully they will read them before they sign. It has shown to be hard to get this routine implemented due to resistance in the personal department. They claim that those rules are not relevant for all kind of employees in the organisation, and hence they cannot force everyone to sign them. Perhaps they change opinion some day so that this signing routine can be implemented in order to improve information security in the organisation.

Company P3

This organisation is quite small and very concerned about information security. Their existence is totally dependent on trust among their customers. Therefore all work is pervaded by information security. For instance they use two physically separated computer networks; one for open and one for restricted information. This is not a typical public organisation, but nevertheless, their experiences may be valuable for other companies and organisations. Their major activities within the area of awareness and attitudes to information security can be summarised in this list:

- All new employees must be given a security clearance in order to work in this organisation. They must also read through relevant security documentation and confirm this by signing a document. In addition a security conversation is arranged with the manager. Such a conversation is also a part of the appraisal interview held every year with all employees.

- There exists a routine to be followed by the last person leaving the office in the afternoon. This routine includes activities like closing all windows, locking all safes, enabling the alarm and locking the doors. Everyone accepts the routine, and they do follow it. It is also accepted that any security incident is reported to the manager who will then take the necessary actions.

- External people carry out inspections in the office from time to time to see if the employees are handling confidential information as described in the routines.

- All security documentation is revised and updated continuously.

- From time to time seminars are held in order to improve attitudes and increase awareness.

- This organisation has worked very actively with information security for several years, and the attitudes and awareness among the employees is now believed to be good. The effect of the actions mentioned here has though never been measured.

Company P4

This is a quite large organisation that works actively with awareness and attitudes to information security. The security manager emphasizes the importance of foundation in the management for this work to be effective. Their major activities within this area are summarised as follows:

- The internal web is used actively for communicating information security messages to the employees.
- All new employees are given the IT security regulations to read.
- The company is about to upgrade all clients by installing a new operating system. This will improve the security. In conjunction with this, there will be arranged a campaign focusing on information security.
- The company is now planning an IT security campaign that will focus on awareness and attitudes. They will give away a CD to all employees. The CD contains several security applications for home use, like anti-virus, anti-spam, personal firewall and so on. There will also be arranged a quiz with possibility to win prizes. This will be the first time this company is trying such a campaign. The top manager stands fully behind this campaign to ensure that everyone takes it seriously. The whole campaign is developed and fully taken care of by the company itself.
- Since they have never before arranged a special information security campaign, they have not measured the effect of such a campaign. Neither do they have any plans for measuring the effect of the planned campaign. As most other companies, they just hope such a campaign will have a positive effect on the awareness and attitudes among the employees.

Company P5

This organisation is quite large and the security manager has close connections with the top management. He is part of the corporate staff and is responsible for requirements and guidance regarding information security. The company has an IT-centre that is responsible for carrying out information security in practice. Laws, like for instance the Personal Data Act [PDA], regulate many of the company's activities. This means the company has to take information security seriously. The security manager pointed out these as the most important issues in their work with attitudes and awareness:

- The security manager has a close and good dialogue with the top management where information security is taken very seriously. He also has a good connection with the executing IT-centre. This is emphasized as very important for achieving a high level of security.

- The internal web is an important communication channel for security messages. Important security articles are linked directly from the home page of all employees. This home page cannot be changed, and everyone who opens his or her Internet browser will therefore see the security message. The security manager has no problems arguing with the web editor that a security message is important enough to be placed on the front page of the internal web.

- All new employees in this organisation must sign a declaration of confidentiality. In addition, everyone with a valid user ID on the computer network must sign a computer user contract. This contract consists of about 20 items stating what is allowed and what is not on the clients and on the network. The user must sign the contract again whenever his or her access rights are to be changed or the user is applying for a new hardware device like for instance a CD writer.

- Internal audits are arranged frequently. Employees are then asked if they know about the computer user contract, if they remember to have signed this and if they are familiar with the content of this contract. Such a control will reveal if the employees know how to behave but not if they actually behave as they should.

- Those users with need for access to the most sensitive information are trained before they are granted access. This course includes a topic like information security.

- They are considering an internal certification on information security in order to increase the awareness and improve the attitudes to information security. This is not yet implemented, but it is one of more activities under consideration.

- Another activity under consideration is a security quiz on the Intranet with the chance of winning small prizes.

- The security manager has this year also been involved in another master thesis work about awareness and attitudes to information security. A questionnaire consisting of 15 questions has been sent out to some of the employees in the organisation. The results from this survey are not yet available, but hopefully they will give an indication of how good the attitudes to information security are within the organisation.

- Every year an internal control is arranged among all departments and divisions. This control contains some questions about awareness and attitudes to information security. It gives the security manager some ideas of what kind of activities and where in the organisation special activities are needed. This is based both on what is said in the answers and what is not said.

- The organisation has a system for incident reporting where major incidents are reported to the security manager and minor incidents are reported to the IT-centre. Work is done to improve this system. Some of the reported security incidents are made public to all employees with an indication of how much this costs the company in time and money. This is done to help prevent similar incidents from happening again. No names, whether it is on persons, departments or divisions, are ever mentioned in such cases. This is done deliberately to ensure that everyone takes it seriously and that nobody says, "That is typical for that department, a similar incident could never happen here".

Appendix E – Interviews in sector Other

Company O1

This company is bound to follow the Security Act [SecA], and all employees know that if they don't do it, the company will soon be out of business. The awareness and attitudes of the employees are therefore of great importance, and the company has the following activities within this area:

- The company has a two-level computer network for both unclassified and classified information. In conjunction with this there exists policies, user manuals etc. to inform the users how to behave and what to do on the client and on the network.
- From time to time small courses are arranged to keep up the awareness among the employees regarding information security.
- All new employees must be given a security clearance before they can start working in this company. They must also sign a declaration of confidentiality. In addition to this, a one-hour introduction course, covering security among other items, is mandatory for all new employees.
- For every new project that is started, a security contract is made, and all members of the project have to sign this. Such a contract states what is allowed to do and what is not and how the project members, both company internal and external, are supposed to behave.
- The company has a system for reporting and handling security incidents. Such incidents are not made public on the Intranet, but as words spread, most of the employees will eventually know of it.
- They work with attitudes and awareness on a daily basis, and they have never arranged any special security campaigns. Nor do they have any plans for doing this either.

Company O2

This company is bound to follow the Security Act [SecA], and all employees are fully aware of that. The security manager points out the following activities as most important in their work with attitudes and awareness:

- There exist well-defined routines to follow when hiring new employees. These include security clearance, declaration of confidentiality and training.

- This organisation was involved in the pilot project of NTNU [NTNU] and NSM [NSM] in 2002/2003 [ROSS]. They plan to use that tool in their further work with awareness and attitudes. But they will wait some time so that the implemented activities have had time to work.

- The security department is very active and service minded. They have their own pages on the internal web where they have security related articles, links to laws and regulations, and a possibility to send e-mail to the security staff. Walking around in the organisation talking to people is another important activity. And so is participation in internal meetings. They also have an open security office with two computers for everyone to use. One is connected to Internet and the other is on the restricted network. Those machines are often in use, both by internal employees and by external contractors. With candy on the table, this office serves as a place where both employees and contractors can drop in for an informal talk about security. It should not be frightening to contact the security department.

- All security incidents are reported and handled. They are never made public, but the experiences from such incidents are used more indirectly. Some incidents may lead to specific actions; technical or non-technical like for instance articles on the web in order to increase the awareness to a particular problem.

- They often do audits, both internally and out at contractors and partners.

- From those audits and inspections they have a lot of measurement data. They are however very careful when they use such data. The measurements are very situational and time dependent. Due to special circumstances the measurements from last month doesn't necessarily say something about the "normal" situation or the situation today. Organisational changes also make such measurements unreliable. The measurements and inspections are instead used as preventive elements and quality controls.

- The security manager keeps track of the number of inquiries made to him by phone or e-mail. An increasing number of inquiries may indicate an increasing level of awareness to information security in the organisation.

- He sees that the inspections do lead to increased awareness and better attitudes among the employees without having any systematic measurements to prove it.

- He also gets feedback from the employees and the managers in the organisation that the implemented actions do have an effect.

Company O3

This company is part of a global group. Information security has a strong focus in this organisation, and the security manager points out these activities as the most important in their work with attitudes and awareness:

- All new employees must sign a declaration of confidentiality. They must also attend at an introduction course where information security is an important part.
- This organisation, included the top managers, have a strong focus on information security. They have all the necessary documents in place, included business continuity plans, contingency plans, and appurtenant procedures and routines. These documents are now revised every year.
- Testing of the contingency plans is desired but very difficult to carry out in a full scale. But smaller tests are carried out in order to see if the procedures and routines function as intended and that the employees do what they are supposed to do.
- The internal web is used to communicate security articles and documents out to all employees. The security department has their own security pages where all relevant links and documents are placed.
- From time to time small campaigns are carried out. These focus on specific security issues like for instance locking the computer screen when leaving the desk. It is important to keep the messages as focused and simple as possible, and don't try to cover all aspects of information security in one campaign. Use time and take it step by step.
- Some measurements are done in specific areas. One example of this is checking that laptops are physically secured with a wire to the desk when not in use. The security staffs collect unsecured laptops, and the user has to contact them in order to get the machine back. Checks like that are done from time to time, and even if no systematic measurements are done, they do seem to have a positive effect. Other measurements like those also exist, but none of them are done or used in a systematic way.

Company O4

This company is part of a global group where information security is essential for the company to stay in business.

- The employees get security training dependent on their need, but two to three times a year an introduction course is held for all new employees. About four hours of this course is dedicated to information security. The course is mandatory for all new employees in the organisation.

- The new employees must also sign a declaration of confidentiality before they begin. All external contractors working for the company must also sign the declaration.

- The company has specific information packages on security that are available for the various departments to use. The security staffs are also invited to internal meetings and conferences to talk about information security.

- They arrange security campaigns when they see that it is needed. It can be as a result of internal or external incidents or specific threats. All campaigns are developed and made by the company itself, and they usually use pamphlets, posters, e-mail, web and their internal magazine in order to reach the employees with their messages.

- The management of the company is fully aware of the existing threats regarding information security, and the contact between the security manager and the top management is very good.

- Two times a year the security staffs perform inspections in order to see how the employees leave their workplace; Computers shall be locked, windows closed, no graded documents on the desk etc. Such inspections have been carried out for several years, and the security manager can see distinct improvements.

- The security staffs have also checked the paper waste from the company to see if any security-graded documents are thrown in the wastebasket instead of being shredded according to the regulations. From these inspections they saw a clear need for improvements. They changed the necessary routines regarding destruction of security-graded documents and arranged a campaign making the employees aware of this. When the next inspection was carried out they saw a distinct improvement in the treatment of graded documents as the amount of paper that was shredded had increased considerably.

- The security manager sees questionnaires as another way of measuring the awareness among the employees, but this has not been tried out in this company.

Appendix F – Example of awareness metric from NIST

Table 4 - Sample awareness and training metric defined in [NIST50]

Critical Element	Have employees received adequate training to fulfill their security responsibilities?
Subordinate Question	Are employee training and professional development documented and monitored?
Metric	The percentage of employees with significant security responsibilities who have received specialized training
Purpose	To gauge the level of expertise among designated security roles and security responsibilities for specific systems within the agency
Implementation Evidence	1. Are significant security responsibilities defined, with qualification criteria, and documented? □ Yes □ No 2. Are records kept of which employees have specialized security responsibilities? □ Yes □ No 3. How many employees in your agency (or agency component, as applicable) have significant security responsibilities? _____ 4. Are training records maintained? (Training records indicate the training that specific employees have received.) □ Yes □ No 5. Do training plans state that specialized training is necessary? □ Yes □ No 6. How many of those with significant security responsibilities have received the required training stated in their training plan? _____ 7. If all personnel have not received training, state all reasons that apply: □ Insufficient funding □ Insufficient time □ Courses unavailable □ Employee has not registered □ Other (specify) _____
Frequency	Annually, at a minimum
Formula	Number of employees with significant security responsibilities who have received required training (Question 6) / Number of employees with significant security responsibilities (Question 3)
Data Source	Employee training records or database; course completion certificates

Indicators	The target for this measure is 100 percent. If security personnel are not given appropriate training, an organization may not be equipped to combat the latest threats and vulnerabilities. Specific security control options and tools are rapidly changing and evolving. Continued training enforces the availability of necessary security information. This metric can be correlated with the number of security incidents and the number of patched vulnerabilities to determine whether an increase in the number of trained security staff is related to, and facilitates, a reduction in certain types of incidents and open vulnerabilities.

Comments: Question 1 and 2 are used to gauge the reliability of the information for this metric. Roles and responsibilities must be defined in policy and procedures, and personnel identified to carry out the roles. Question 4 and 5 provide information to help identify any specialized training that personnel need to complete. If sufficient training of personnel is not provided, Question 7 helps identify why. If the cause of insufficient training is known, management can institute corrective actions to remedy this deficiency.

Appendix G – Examples of awareness posters

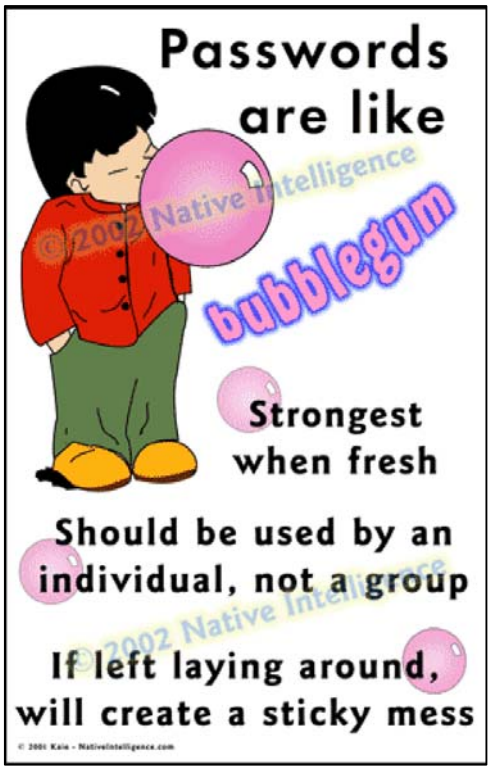

Figure 7 - Security awareness poster from Native Intelligence [NaIn]

Figure 8 - Security awareness poster from Native Intelligence [NaIn]

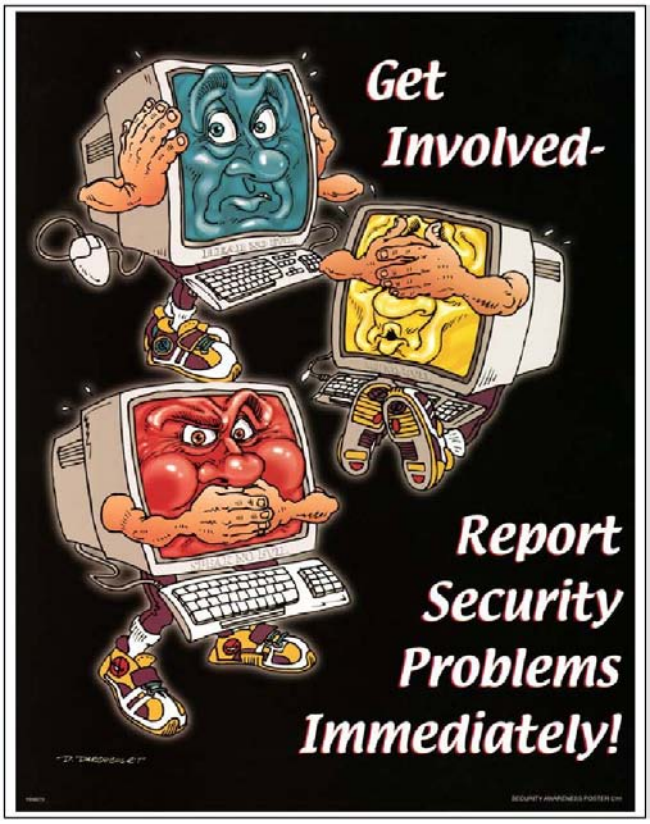

Figure 9 - Security awareness poster from Western Adm. Support Center [WASC]

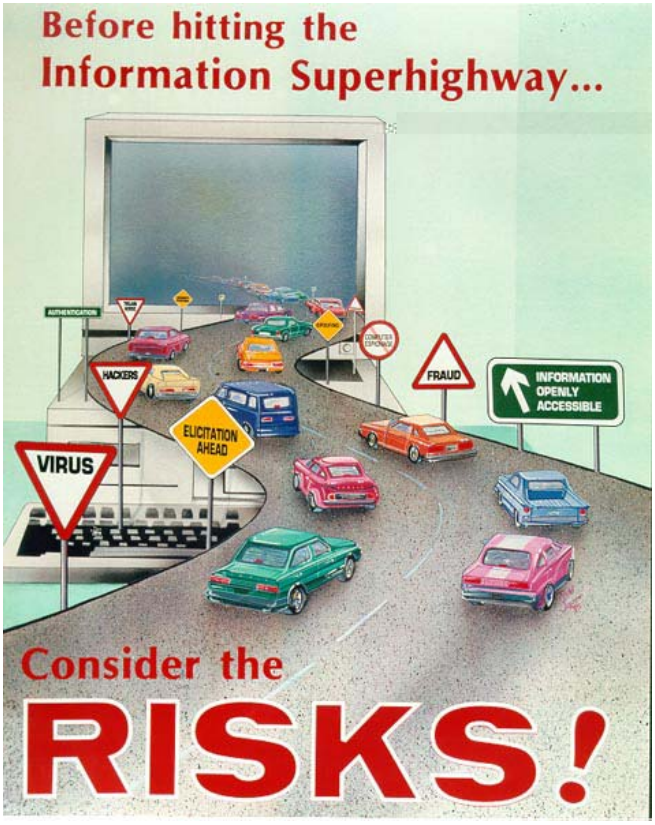

Figure 10 - Security awareness poster from Western Adm. Support Center [WASC]

Figure 11 - Security awareness poster from Security Awareness [SeAw]

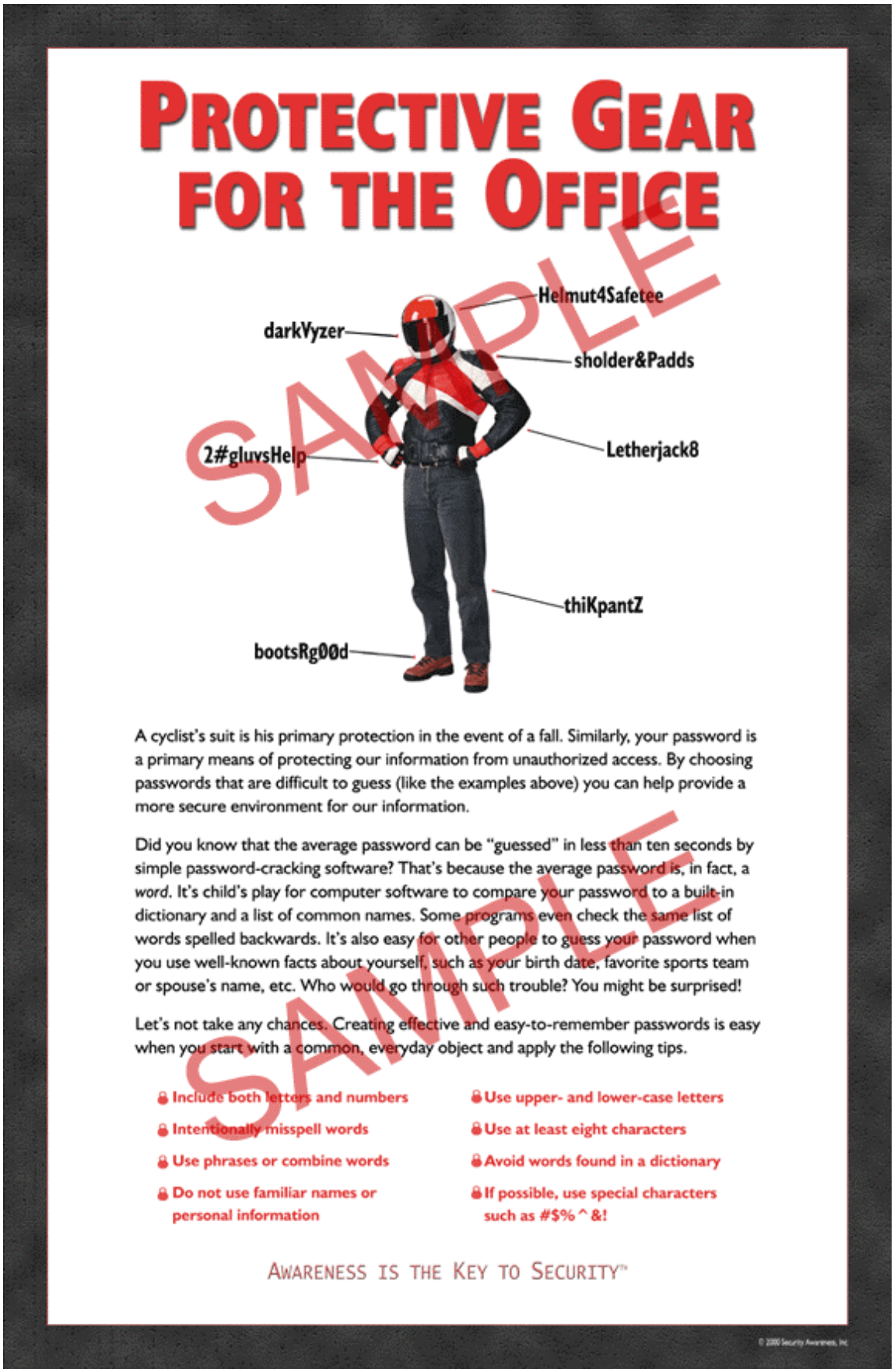

Figure 12 - Security awareness poster from Security Awareness [SeAw]

Figure 13 - Security awareness poster from [NIST]

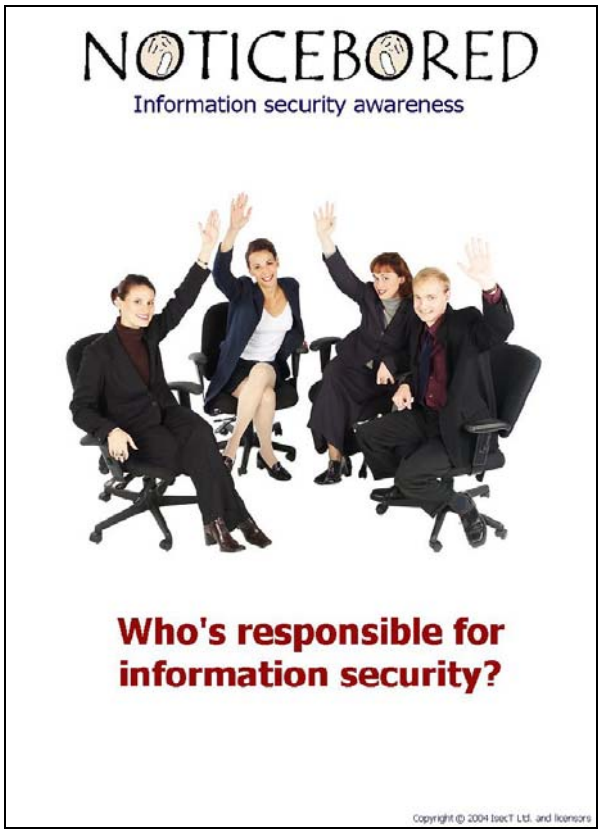

Figure 14 - Security awareness poster from Noticebored [Noti]

Figure 15 - Security awareness poster from Noticebored [Noti]

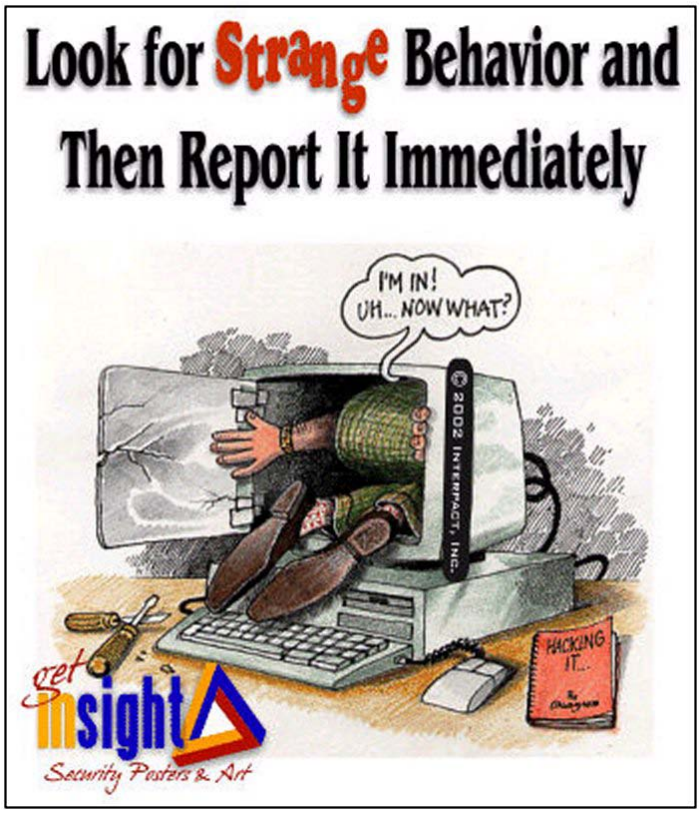

Figure 16 - Security awareness poster from GetInsight [GetI]

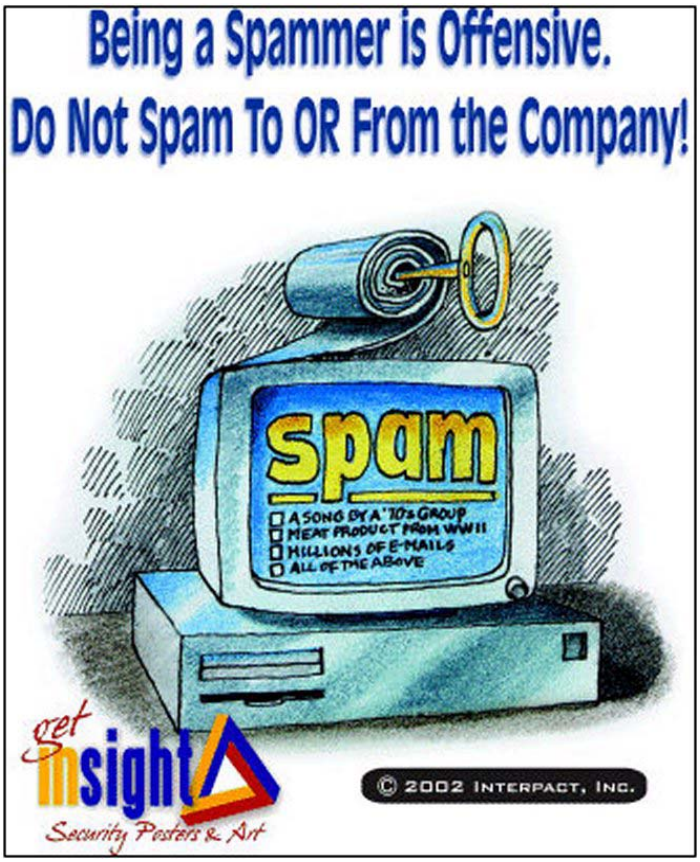

Figure 17 - Security awareness poster from GetInsight [GetI]

Figure 18 - Security awareness poster from Atterbury Foundation [Atte]

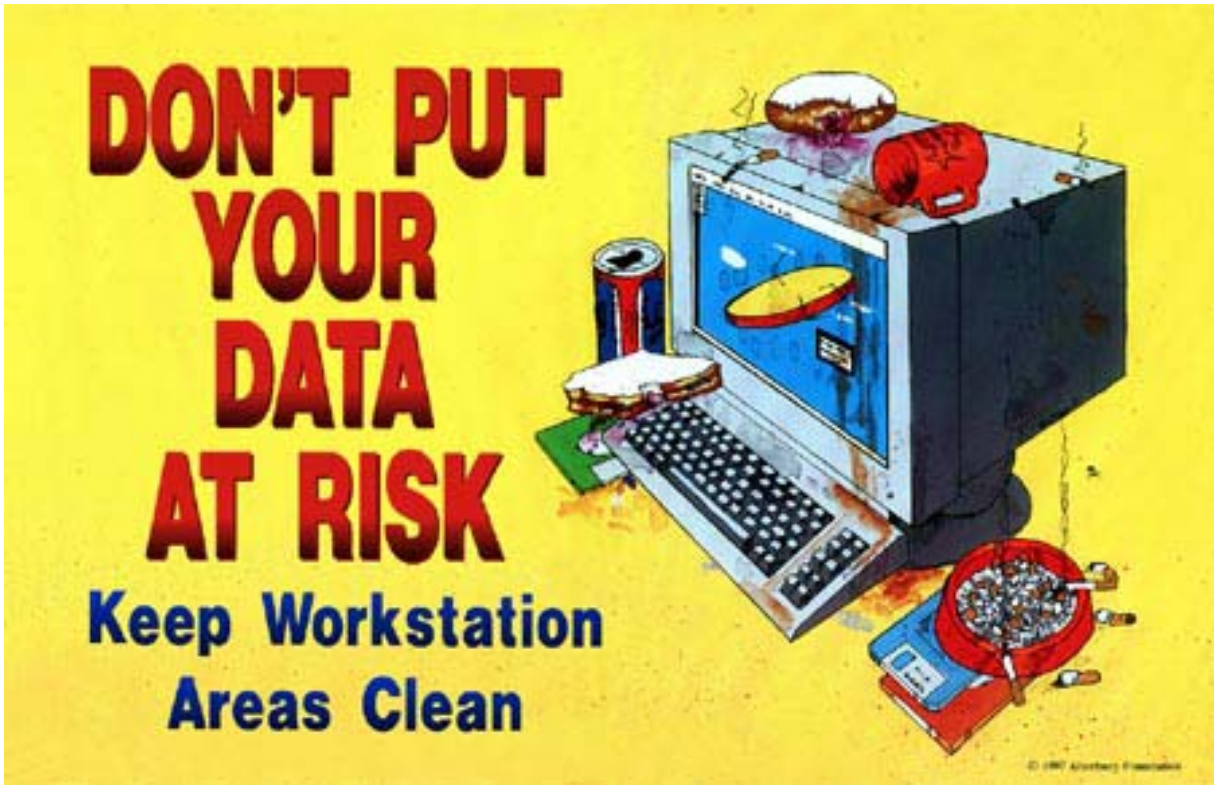

Figure 19 - Security awareness poster from Atterbury Foundation [Atte]

Appendix H – E-mail sent out to the security managers

Below is a sample of the e-mail sent out to the contact persons prior to the interviews. All e-mails were personalised. Some persons were contacted due to their membership in ASIS while others were contacted due to a reference from other persons. This was indicated in each message.

Since all e-mails were written in Norwegian, the sample below is translated to English.

Hello.

I am studying information security at Gjøvik University College in addition to working at Telenor. At this time I am working on my Master Thesis with the preliminary title ”Measuring the effect of an information security awareness drive”. In connection with this I want to collect viewpoints and experiences from companies and organisations in Norway that are working with improving the attitudes and awareness of information security among the employees.

You may have heard about this project earlier through ASIS.

I hope you can take your time to read this e-mail and think through the questions. Then I will call you during the next weeks for a short interview.

What I want to find out is how Norwegian companies and organisations, both private and public, work with attitudes and awareness, and if some of them have tried to measure the effect of this work. The management of a company is interested to know the return on investments. It is therefore suitable to ask the question if it is possible to measure the effect of an awareness campaign as raised awareness and improved attitudes among the employees.

As already mentioned I will call each of you during the next weeks to do a short interview about this. It would be nice if you could think through the following questions in advance:

- How do you work with awareness and attitudes?
  - Do you arrange special campaigns or do you work in a regular manner?
  - How often are security campaigns arranged?
  - What kinds of campaigns are arranged?
  - Who develop and make those campaigns?
- Is the effect of the campaigns ever measured?
  - How is this done?
  - How often is it done?
  - What is the result of these measurements?

- How do you see that attitudes and awareness can be measured?
    - How should the measurements be done?
    - Who should do the measurements?
    - How often should it be done?

This is not meant as a complete list of the questions I want to be answered, but an indication of what I will ask about when I call.

I hope you can spend some time on this and that I am allowed to call you. In that case, send me e-mail with your telephone number and an indication of when I can call you.

Best Regards
Johnny Mathisen
Senior Adviser
Centre of Excellence – Information Security
Telenor ASA

Appendix I – Metrics for security awareness

Table 5 – Definition of awareness metric A-1 – Security training

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.

Comment: See also Appendix F for the NIST definition of a similar metric.

Table 6 – Definition of awareness metric A-2 – Security incidents

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 7 – Definition of awareness metric A-3 – Clean desk

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 8 – Definition of awareness metric A-4 – Paper shredding

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 9 – Definition of awareness metric A-5 – Illegal traffic

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 10 – Definition of awareness metric A-6 – Weak passwords

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 11 – Definition of awareness metric A-7 – Hits on web pages

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 12 – Definition of awareness metric A-8 – Requests to security department

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 13 – Definition of awareness metric A-9 – Customer satisfaction

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.