Improving Security Awareness and Ownership using a method based on Action Research

by
Bjørnar Prestaasen

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

Abstract

Despite the security training and hours spent in educating users, security tests implemented by the security department show that employees in Norsk Tipping have broken the security guidelines stated in the overall security policy. The security education has been done in large groups of employees and the security department wants to develop the security education and test a new method for awareness training in Norsk Tipping. One of the key features in this education is that the employees should be able to participate more in the education and to have the opportunity for a security dialogue in the organization.

The hypothesis for this thesis is that a method based on action research can improve security awareness amongst the employees. Based on literature review and the guidelines provided from the security department a method based on principles from action research seemed promising and would be suitable as method for the security department in Norsk Tipping.

The method that was designed in this project was based on four small-group interventions with employees and their line manager in Norsk Tipping. The core concepts in these sessions were co-generation of knowledge and have opportunity to discuss situations provided by the employees. This should make the content more understandable for the employees. By adopting security categories from the ISO/IEC 27001 standard and a cognitive classification from the educational research the method was intuitive and adjustable for Norsk Tipping.

The project resulted in a method that was easy to understand for the participants. The evaluation identified that all of the employees found this method positive and several of the employees explained that the dialogue was interesting and the content was more understandable. The group interventions also identified several areas where employees should improve awareness. The security department did also get new knowledge about the different roles to the participants. The method can be used to adjust the security education for the employees in the future.

Sammendrag

På tross av kontinuerlig sikkerhetsopplæring så har sikkerhetstester implementert av sikkerhetsavdelingen i Norsk Tipping avdekket brudd på sikkerhetsbestemmelse blant de ansatte. Sikkerhetsopplæringen har blitt gjennomført med store grupper ansatte og sikkerhetsavdelingen ønsket å teste ut en ny metode for å øke sikkerhetsbevisstheten blant de ansatte i Norsk Tipping. Viktige elementer i opplæringen var at de ansatte skulle være mer involvert i opplæringen og det var ønske om få en bedre sikkerhetsdialog med de ansatte.

Hypotesen for dette prosjektet er at metode basert på action research kan øke sikkerhetsbevisstheten blant de ansatte i Norsk Tipping. Etter å ha gjennomført litteraturstudie og diskutert retningslinjene med sikkerhetsavdelingen virket en metode basert på prinsipper fra action research lovende og interessant.

Metoden som har blitt designet i dette prosjektet er basert på fire gruppebaserte intervensjoner med ansatte og deres linjeledere i Norsk Tipping. Viktige elementer i intervensjonene har vært og sammen skape ny kunnskap og ha muligheten til å diskutere kjente situasjoner fra de ulike rollene til deltagerne. Ved å hente sikkerhetskategorier fra ISO/IEC 27001 standarden og en kognitiv klassifisering fra pedagogisk forskning ble metoden intuitiv og mulig å tilpasse til Norsk Tipping.

Prosjektet resulterte i en metode som var enkel å forstå for deltagerne. Evalueringen av metoden identifiserte at alle deltagerne synes at metoden var positiv og flere deltagere forklarte at dialogen i intervensjonene var interessant og at innholdet var enkelt å forstå. Gruppeintervensjonene identifiserte også flere områder hvor de ansatte burde forbedre sikkerhetsbevisstheten. I tillegg lærte sikkerhetsavdelingen nye aspekter ved de ulike rollene til deltagerne. Dette gjør at metoden kan brukes for å tilpasse sikkerhetsopplæringen til de ansatte i fremtiden.

Preface

First of all I want to thank my supervisor, adjunct associate professor Dr. Finn Olav Sveen for all his support during this thesis and also the preparation courses in the previous semester. He has provided guidance in all of different phases in the project and has been available whenever needed.

I will also like to thank Trond Laupstad which is CSO at Norsk Tipping. He gave me the opportunity to work with an interesting topic and also to test the method in a real situation. This has been an important experience for me and it has been interesting to work in a company that is well-known for their security culture.

Knut Henrik Nilsen is a security advisor in Norsk Tipping and has been my supervisor. He has invested many hours in guiding the research. Knut Henrik has participated in all of the meetings with the line managers and also been the security expert in the group interventions. He has given me important feedback and guidance throughout the project and was responsible for the communication with the employees in Norsk Tipping.

I will also thank all of the employees that participated in the project. This includes the line managers and the other employees that participated in the group interventions and the interviews. Without their positive attitude and desire to improve the security education, it would have been difficult to complete this research.

Table of contents

List of figures:

List of tables

1 Introduction

To be able to defend an organization from the different security attacks, technical countermeasures like firewall, anti-virus and IDS[1] must be implemented. These countermeasures deal with automated attacks that are launched from Internet and are often implemented in today's organizations [1]. Directed attacks like social engineering will often address the people in the organization. These attacks might create a bigger impact because people are often the weakest link in the information security chain, as they might be a single or the least reliable barrier[2]. To deal with these attacks the security education of the employees is crucial [3]. This project will address the security education of employees related to security awareness and compliance towards the security guidelines defined by Norsk Tipping. This project consists of the design of a method based on principles from action research and the test-implementation of this method in Norsk Tipping. The method is also evaluated with qualitative interviews.

1.1 Justification, motivation and benefits

The motivation for addressing the relations between security awareness and compliance is to deal with targeted attacks towards Norsk Tipping. With a proper reconnaissance phase, an attacker can tailor the attack towards the employees and include legitimate information that the employees find compelling. Hence, they will open the attachments. By including malware[2] with an unknown signature, antivirus and antimalware systems are not capable to detect these attacks. By increasing the compliance of the employees, Norsk Tipping can detect attacks in an earlier phase and in addition have increased awareness and understanding of these attacks. The method will use principles from action research (AR) to improve the compliance of the employees. AR is carried out by a team, which define the problem, cogenerate relevant knowledge, take actions and interpret the result together [4]. The cogeneration of knowledge and the interaction between the researcher and the employees are the most important aspect of AR. By performing the research process together, the employees can bring their expertise related to their jobs, while the researcher can bring expertise on the theory. The reason for choosing this method is that Norsk Tipping wants to define the security aspect of different roles in the company, define the current security level of the employees and to define what security levels the employees should be on. AR has been used in other research areas like psychology and risk with success. In security research Puhakainen and Albrechtsen have performed single studies based on AR with success. The interaction between the employee and the security officer is the key aspect of this method. By defining the security aspect of a job together, the employees can improve their awareness and the security department can get better insight in the specific security roles for the employees.

[1] Intrusion detection system – www.en.wikipedia.org/wiki/Intrusion_Detection_System

[2] Malicious software - software designed to secretly access a computer system without the owner's informed consent

1.2 Research questions

The main goal of this project is to design a method for improving security awareness and ownership for the employees in Norsk Tipping. A summary of the research questions are presented here in order to create an overview of the project topic. The research questions are fully described in chapter 3 in the report. With the new method for improving awareness and ownership, Norsk Tipping may improve the usage of resources and the knowledge to the different job-functions in the company. The defenses towards the targeted attacks can also be improved. Below is the research questions presented.

- Can a method based on principles from action research increase the knowledge and understanding of security to the employees in Norsk Tipping?

The motivation for choosing a technique based on action research is to improve the employees' awareness and ownership by participation. When the employees participate in this process with knowledge related to their daily work, it is easier to relate the security aspects to an understandable level for the employee. With a better understanding of the security aspects, the security compliance may also be improved. Recent research shows a positive effect by using small groups and discussion for improving awareness and compliance [5, 6]. The second goal is to identify how this technique may improve the awareness in Norsk Tipping. It is important to find out if this method has an impact on the employees and measure the effect of the method.

- Did the employees find this method positive and effective for improving information security awareness and compliance?
    - What do they think of the process of the education and did the method improve their ownership towards security?

In addition this method can also improve the knowledge of the security department. By including the employees in the security discussion, the security department can learn the specific security considerations for the different departments. This effect should also be investigated in the project because this is an important feature of the method.

- Can a participatory method based on principles from action research improve the security team's knowledge of specific security aspects for the employees?
    - Does the security team find this process effective and can it be used in the future?

1.3 Choice of method and report structure

To create the report structure for the thesis, a method called P'HAPI is chosen. The first P stands for problem. This includes the description of Norsk Tipping and the problem description. In addition the literature review is placed in chapter 2. The H stands for hypothesis and is chapter 3 in the report. This is where the research questions are described that is related to the problem description and the literature review in the previous chapter. In chapter 4 the A is described. A stands for analyze and this includes the choice of method and design of the participatory method. In chapter 5 the implementation of the participatory method is described. This includes the documentation of the

different group interventions completed as the test phase. Chapter 6 is the evaluation of the method and includes the qualitative interviews with the participants. Both chapter 5 and 6 is included in the analysis section. The second P stands for policy and this chapter addresses possible solutions to the problem. The discussion and the conclusions are included in this section of the report and is chapter 7. The final letter in the method is I and stands for implementation. This includes a description of how the possible solutions can be implemented in Norsk Tipping and is chapter 8 in the report.

The main research method in the project is built on principles from AR. This is because Norsk Tipping wants to develop and continuously improve the security education and include the employees on a higher level in the security education. Research based on employee participation and cogeneration of knowledge between the researcher, security personnel and the employees has given positive results and improvement of security awareness, so it was decided that a method based on these principles should be tested on the employees in Norsk Tipping.

The first phase of the project is to find relevant literature, to acquire knowledge and investigate if there has been done similar research and the current state of the security awareness education. The organizational structure of Norsk Tipping is also defined a prerequisite for creating a suitable design of the participatory method. The following phases will be to design the method, test it on groups of employees and evaluate the completion of the method.

1.4 Keywords

Security awareness, security compliance, security culture and action research.

1.5 Planned contributions

The aim of this master thesis is to provide a method for Norsk Tipping to improve the compliance towards security among their employees. By using a method based on principles from action research where the employees participate in shaping the research, we believe that this can have a positive effect on the compliance and thereby improve security awareness and security knowledge among the employees in Norsk Tipping. Hopefully after the test phase, the method can be adopted to other groups of employees and used by the security team in Norsk Tipping in the future. The project can also provide a method for using action research in a security education and this can be adapted to other companies as well.

1.6 Thesis constraints

The main goal of this thesis is to design and test a method for improving awareness and compliance among the employees in Norsk Tipping. This results in a foundation that the security department in Norsk Tipping can adjust and improve to the security education in the future. There will be a selection of groups of employees to evaluate the test phase. Because this evaluation is completed with qualitative interviews, the potential improvement of the employees is not measured. It is also important to remember that the method is

tested on a sample of the employees and cannot be generalized as an accurate picture of Norsk Tipping as organization.

1.7 Guide in document

In chapter 2 the problem description is provided together with the literature review. Chapter 3 contains the hypothesis for the project in addition to the research questions. In chapter 4 the design of the participatory method is provided. This includes the description of the participatory model and the description of the intervention with the employees. Chapter 5 is the documentation of all the interventions and the test phase of the method. In chapter 6 is the results presented. This includes the interviews with the employees and the security department. Chapter 7 is the discussion and conclusion while chapter 8 is the recommendations for further work.

2 Problem description

Content of the chapter:

- Short description of Norsk Tipping
- Description of the main problem
- Presentation of the relevant literature
- Problem in P'HAPI

2.1 Description of Norsk Tipping

Norsk Tipping[3] is a wholly state-owned company under the jurisdiction of the Ministry of Culture and Church affairs[4]. It was created in 1946 and has contributed almost NOK 85 billion to good causes in society like sports, culture and voluntary organizations. Norsk Tipping has today approximately 360 employees and provides games through commission agents (4000) in grocery stores and other shops, via Internet or on mobile phone. Norsk Tipping's structure is visualized in Figure 1.

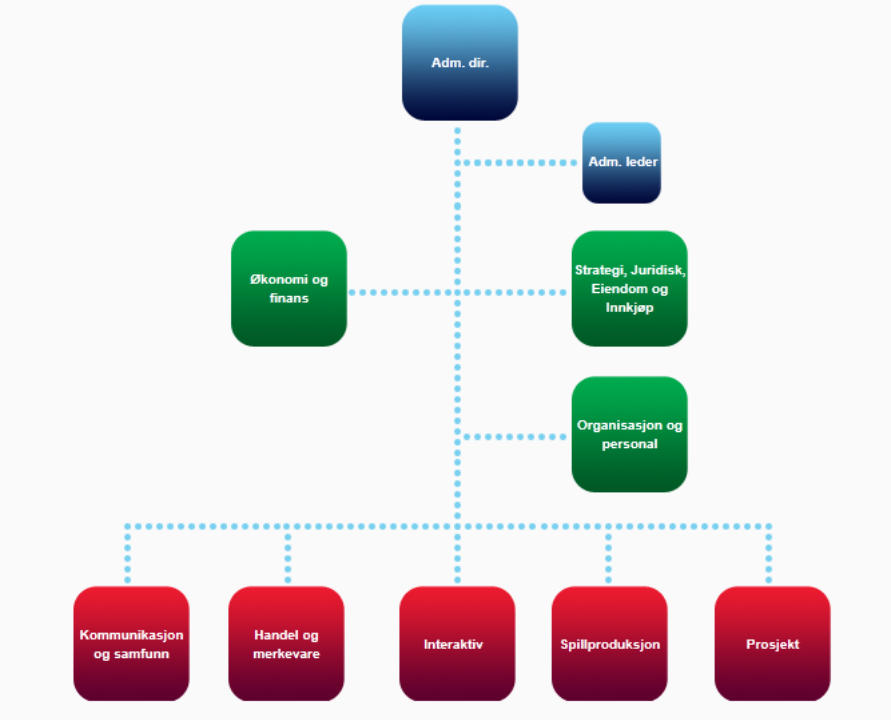


Figure 1 - Organizational structure of Norsk Tipping

3 www.norsk-tipping.no
4 www.norsk-tipping.no/selskapet/english - accessed June 2011

There are 3 administrative departments (green color). In addition there are 5 departments that support the daily operation of the organization. These are marked with a red color in Figure 1.

The security team is located in the economy and financial department and has 5 members. One of their main tasks is to provide security education to employees and other people related to the organization and ensure compliance to the ISO/IEC 27001[5] and the WLA SCS[6] documentation. The ISO/IEC is the general standard for information security, while the WLA SCS is a security standard provided by the World Lottery Association. When an organization is certified in ISO/IEC and WLA SCS it demonstrates that the organization fulfills a minimum set of requirements related to security and follows a set of best practices.

2.2 Problem description

This chapter presents the problem, the P in the P'HAPI method. It includes a description of the problem defined by the problem owner and an explanation of literature related to the problem description.

The security department in Norsk Tipping is defined as the problem owner in this project. Norsk Tipping is a certified organization to the ISO/IEC 27001 and the WLA SCS and is well-known for their attention to security. The security department has recognized the importance of security awareness training; all new employees are given initial security training by the CSO[7] in the company. The security training has annual follow ups for all the employees, consultants and other people related to the organization are also given security training. This is often a method based on classroom-education, either with hired external professionals or the internal security personnel, which address important security topics.

Despite the security training and hours spent in educating users, security tests implemented by the security department show that employees have broken the security guidelines stated in the overall security policy. These tests are not described to the reader, because it is sensitive information to Norsk Tipping. The employees do to a certain extent have security awareness, but they are not compliant with the security policy in the organization.

The human aspect is an important factor when it comes to the security level of an organization. Employees are an important asset that are often referred to as the weakest link in the information security chain, as they may be a single or the least reliable barrier [2]. The new trend is more targeted attacks towards the employee than towards the technical defenses in the organization [7]. These targeted attacks can create more damage because of the privileges of an employee, and it is also easier for an attacker to trick an employee than to create software to avoid the technical defenses [7].

Because of the importance of the human aspect and the continuous development of methods for attacking information systems, Norsk Tipping wants to improve their security awareness and compliance education. Because they have used classroom education regularly in the past years, they now see the need of trying a different method to improve awareness and compliance. The overall goal is to decrease the number or avoid security policy violations by the employees in Norsk Tipping.

[5] Information Security Management System standard
[6] World Lottery Association Security Control Standard
[7] Chief Security Officer

The security department is eager to test a new method for improving security awareness. The education has been done with large groups of employees with a small amount of interaction between the security team and the employees. The security department is therefore interested in testing a method where the employees can be more active in the education. They believe that interaction is important when teaching security and that interaction can improve both awareness and also the employees' ownership to security.

The problem owner states that the employees should feel ownership to security in Norsk Tipping. When the employees have ownership they might think more about security related issues in their daily duties. Because of the ownership aspect, the additional method should also concentrate on improving the employees' ownership to security. Recent research shows that by including the employees in discussion and dialog rather than using classroom education with a big audience, the feeling of ownership to the employees can be improved.

One problem that is well known in security awareness education is to measure the results of the education. The choice of suitable metrics and method for the measurement is often complex and difficult. This problem is addressed in a report produced by PricewaterhouseCoopers for ENISA[8] [8].

In order to provide a functional method that is adjusted to the demands from the security department a literature study must be completed. This is used to identify the different methods that are used in security education where interaction with the employees is central. The following section is the literature review on security awareness and different methods to educate employees. In addition security measurement is also included in order to identify the possibilities of measuring the results of the chosen design.

2.3 Literature review

This section is provided to introduce relevant literature on the topic, where researchers have done similar experiments or as background material to other aspects related to the project. The following section will address literature related to security awareness and ownership and different methods used in security education. The second section will address the chosen method, action research, while the third section will address literature on how to measure security improvement in awareness and compliance.

This review is used to identify if similar projects had been implemented in different organizations and if they had been successful. The research performed in the information security awareness and compliance field is investigated to create knowledge and understanding for creating a successful method. To find relevant literature approved databases like IEEE, Springerlink, ISI Web of Knowledge, ScienceDirect, Elsevier and others are used. Because of the timeframe relevant literature can be missed out, but the identified literature has formed the research questions stated in chapter 3.

Information security awareness and ownership are the core concepts of this project. A study by Siponen and Oinas-Kukkonen revealed that information security traditionally has been dedicated to technical aspects and much more research on the non-technical aspects is needed [9]. Puhakainen examined thoroughly the majority of the awareness literature produced before 2006. His

8 European Network and Information Security Agency - www.enisa.europa.eu

dissertation provides a overview of the research and is used extensively on the research before 2006 [5].

Puhakainen's research question was to explore how IS[9] users' compliance towards IS security policies and instructions can be improved [5]. To solve this he divided the two steps where the first action was to review the existing literature and the second action was to develop design theories based on the shortcomings in the literature. Puhakainen reviewed the field of information security awareness as part of his PhD dissertation in 2005 [5]. Puhakainen's work is a recognized summary of the security awareness field. He found 59 papers on awareness and compliance submitted between 1985 and 2005. This is a small amount of published research taking into account a 20 year time frame and it shows that security awareness is an understudied field. The lack of empirical data in the identified literature is also important. Puhakainen revealed that the dominant research approach was conceptual analysis. 53 of the 59 papers were based on this approach and they did not present empirical evidence, hence the effectiveness of the programs was not investigated. The research of Puhakainen presented two main categories of awareness improvement methods. Cognitive methods and methods based on behavior.

Cognitive approaches consider the individual as an active processor of the information he receives and consequently, that his behavior is not changed unless he understands the information in a meaningful way [5]. In the existing IS security awareness research, cognitive approaches aim to improve users' behavior through (1) persuasive communication and (2) active participation in the design of IS security measures [5].

The cognitive methods were closely related to security training. Methods used for training in this period were lectures, personal discussion, videos, printed materials and web based systems amongst others [5]. Most of the studies presented security awareness training as a socio-technical approach. But the practitioners did not present their underlying theory and why they could improve compliance.

The methods that are used in today's security education are often cognitive methods. The core features that form the basis for a successful program are support from upper management for ensuring economical support and role models, the use of a theme or remainders for creating ownership towards security among the employees and to continuously improve the program [10, 11]. When having these aspects in place, the security team can choose different methods for reaching the employees.

The security team in Norsk Tipping use classroom education as one of their methods of their annual "security update" to their employees. This method is popular to use in companies because it can be used towards all of the employees, is relatively easy to implement and can be tailored to the companies security threats. By hiring security professionals to perform the education, the newest trends and attacks can also be revealed and they might improve the educational outcome. The method demands small amount of resources from the security team and the agenda is prearranged.

This form of education is often used as a reminder of important security aspects. But this method has limitations. The aspect that all the employees are educated with the same content will impact the effect of the method. Employees in large organizations are often on different security awareness levels. Because the content of the session must be tailored to the employees with the lowest

9 Information systems

awareness, it can decrease the motivation for the more aware employees and by that impact their awareness level. The content can often be presented on the general level. To create a dialogue and answer questions from the employees are also more difficult when using large groups of employees. The actual outcome to the employees can be difficult to measure, when using these large groups.

Another popular method to use when improving security awareness is to use web-based training programs. This is an individual approach, where the employees is presented to information and often answer questions related to a topic chosen by the security team. One of the strengths of the method is the ability to reach large sets of the employees and it is possible to adjust the content to different groups of employees, by using several modules. Aetna which is an American health insurance company is well-known for their use of the web-based education [12]. The security team in Aetna also used an interactive channel to distribute security information to the employees.

The important aspect of creating a security dialogue and the ability for the employees to ask questions to the security information provided, are difficult to achieve when using web-based education. The information is often on a general level to ease the amount of work for the security team. The outcome of the program can therefore be less interesting for the security aware employees.

The second method presented by Puhakainen was behavioral methods. They were based on manipulating variables in response to undesirable behavior, punishing the violations and rewarding compliance with security instructions[5]. The three papers with empirical evidence were in this section and based on deterrence. Puhakainen concluded that more theory-based security awareness approaches should be introduced and that the effectiveness of them should be explored [5].

Consequently, Puhakainen presented 3 design theories for improving IS awareness. These theories were (1) IS security awareness training, (2) IS security awareness campaigns and (3) reward and punishment [5]. Theory (1) was tested in two practical settings using action research and provides empirical information on the results of the intervention [5].

The first practical case was completed in a software company with an awareness training program. Interviews and observation were used to gather information. The IS security manager and seven of the employees claimed a positive effect by attending the awareness training where the aim was to improve the use of encrypted email [5]. Despite the positive results there were identified several areas for further improvement.

The second practical case was with a business unit in a large Finnish corporation. This was also an awareness training program with training session and e-learning package. An anonymous survey and group interviews were used in the evaluation. Both the methods were evaluated as positive and relevant by the employees [5]. In addition to the positive feedback critical opinions were identified among several employees.

To counteract towards the lack of participation, cogeneration of security knowledge and the ability to adjust the security content towards the employees, researchers have developed and tested new methods to improve the security education among employees.

Several methods are based on principles from action research (AR) where the researcher and the employees together forms the research and the main concepts of this method is to create participation and generate new knowledge

from the expertise of the researcher and the expertise of the employees. By using these methods the employees are more included in the security education and the content can be more adjusted to what the employees want to improve. The research is often performed with small group interventions where the different employees together provide the educational content.

Eirik Albrechtsen has done several single studies on improving awareness and compliance of employees. In 2006 Albrechtsen performed a qualitative survey on users' view on information security [3]. The main patterns of the study showed that (1) the users stated to be motivated for security, but they did not perform individual security actions, (2) high information security workload created a conflict between functionality and information security and (3) documented requirements of expected behavior had little effect on user behavior and awareness [3]. Albrechtsen used interviews with the employees in the two companies to collect the data. The results of the study cannot be generalized, but Albrechtsen discovered that the employees in the companies were aware that information security work is important, but that the actual behavior was not aligned with their awareness of this issue. There was a conflict between efficiency and functionality on one side and information security on the other side and the users perceived a user-involving approach as the most effective tool to improve awareness and behavior [3].

In 2008 Albrechtsen submitted his PhD dissertation. His aim was to explore the information security management of employees, by studying users' view on information security, measuring individual performance and information security management in practice [13]. Albrechtsen used four different research approaches. He used interviews with employees, interviews with security managers, and intervention study that is described in the section below and a survey on security measures [13]. The results from the thesis showed that education, training and information have best effect when employees and security professionals are interacting and are in dialogue. Employee participation was also evaluated to be the most effective process to improve individual information security performance [13].

In 2010 Albrechtsen and Hovden presented a paper on an intervention study performed in 2006 including six small-sized workshops aimed at improving security attitudes among the employees, and change work behavior relevant to information security at Brønnøysund Register Centre in Norway [6]. Each workshop included an introduction with motivation and objective, group work for discussing scenarios, plenary discussion of scenarios and an evaluation and summary of the workshop. To evaluate the intervention a quantitative survey was used and a qualitative approach with combined interviews, group conversation and observation [6]. A third survey was also used to measure the improvement over time. The interviews showed that the intervention was powerful enough to significantly change awareness and behavior among the participants. It demonstrated that employee participation, collective reflection, group processes, and knowledge creation at an organizational level create changes in information security awareness and behavior at an individual level [6]. This was one of the studies Albrechtsen did in his PhD thesis [13].

Puhakainen and Siponen performed an action research study based on improving employees' compliance through information systems security training in 2010 [14]. They presented a training program based on two theories; (1) universal constructive instructional theory that provided a framework for designing instructions that is customized for a certain learning and (2) elaboration likelihood model that helped practitioners understand why training is expected to work [14]. They used two research cycles where the first session

was implementation of a training program to improve compliance towards an e-mail policy, while the second cycle was based on incorporating a continuous IS security communication process [14]. One of the most important findings was to use training methods and ideas that enable learners' systematic cognitive processing of information. Moreover the learning tasks should have personal relevance to the learner and the previous knowledge of the learner should be taken into account [14]. Visible support from top management and security compliance communication are also necessary.

The provided literature on information security awareness show that there has been a lack of research on awareness and that it is a small amount of the literature that provides empirical data. Mostly there have been conceptual analyses with different scenarios. The literature also includes methods based on principles from action research that has become popular to use when educating employees. This trend addresses employee participation and cogeneration of knowledge. Several papers in the last years claim improvement in both security awareness and compliance. One important aspect of this research is that all of these are single studies. In order to generalize the results, more research must be performed on different organizations and in different scales.

Most of the security education methods that are used today are cognitive methods in Puhakainen's classification. Despite the fact that they often reach a large group of employees and this saves resources for the security team, they also have areas of improvement. The methods are not adjusted to the different roles of the employees and the content must be general in order to have an effect on most employees. Because of the participation and opportunity to adjust the content, researchers have had success with adopting principles from action research to improve security education [5, 6].

Because the success of Puhakainen and Albrechtsen, a method based on principles from action research was chosen for this project. The main goals of the project are also closely related with the advantages of action research, like improving the ownership towards security and the security awareness. In the following section action research is described.

2.3.1 Action research

Action research (AR) is defined as social research carried out by a team encompassing a professional action researcher and members of an organization or community seeking to improve their situation. AR promotes broad participation in the research process and supports action leading to a more just or satisfying situation for the stakeholders [15]. The researcher and the participants define the problems to be examined, cogenerate knowledge about them, learn and execute social research techniques, take actions, and interpret the results together [15].

AR rests on the belief that all people accumulate, organize and use complex knowledge constantly in everyday life [15]. The participants in the research are defined as professionals on their own role and a group including several different types of professionals is therefore likely to be used in action research.

The term action research was introduced by Kurt Levin, when he was a professor at MIT[10]. He used action research to answer if American housewives could be encouraged to use tripe instead of beef for family dinners, because beef was primarily for the troops in 1943 owing to the shortages imposed by World War II [4]. Action research has been used in organizational development and Levin conceptualized social change as a three-stage process: unfreezing, changing and

[10] http://web.mit.edu/

refreezing. This can be related to the planning, action and results phases which are core features of action research.

The planning process is where the researcher and the participants together define the problem. The second process is where the group together performs actions related to the defined problem. In this phase the co-generation and discussion is important concepts and to use the knowledge of the group as a unit to improve the situation. In the third phase the group evaluates the results and identify if something should be done differently to improve the results.

The most typical form of action research is the participatory method [16] and is often based on a five step cyclic process. Step (1) is diagnosing, that is to identify the primary problems. Step (2) is action planning, which are the organizational actions to improve the problem. Step (3) is action taking, which is an implementation of the planned action. Step (4) is evaluating, where the researchers and practitioners together evaluate the outcome. Step (5) is specifying learning and this is usually an ongoing process throughout the research [16]. In the participatory AR there is more responsibility on the actors than in the other sub-classes of action research. Researchers bring theoretical knowledge while the actors bring situated, practical theory to the process [16].

In 1993 Greenwood et al. analyzed participatory AR for organizational learning in three different organizations [17]. In all of the three cases the participatory method led to meaningful research discoveries and organizational change processes. The researchers are also struck that the open processes led the research to new insights about the organization and to useful action consequences [17]. Greenwood et al. states that completely realized participatory research are rare, because many research situations do not permit full-scale participation.

In 1996 Baskerville reviewed AR as method to use in information systems research [18]. After addressing the origins of the method together with a discussion of the method related in information systems, Baskerville concluded that AR is not widely used as a research method, but the method should have a growing role in the mainstream IS research and practice. Puhakainen reviewed this field in 2005 with the same results, but in the last few years several information security professionals have used this in security education [3, 5, 14].

Baskerville investigated different information systems with action research in 1997. He described that the term action research can refer to the general class of methods and also to a specific sub-class that distinguish from “participatory AR” and “action science” [16]. The four main characteristics of action research are; (1) aims at an increased understanding of an immediate social situation, (2) simultaneously assists in practical problem solving and expands scientific knowledge, (3) is preformed collaboratively and enhances the competencies of the actors and (4) is primarily applicable for the understanding of change processes in social systems [16].

Ottoson reviewed participatory action research in 2003 [19]. He states that traditional research demands that researchers should not be involved in the studied object in a way that could affect their objectivity. However Ottoson states that the researcher obeys modern scientific thinking when performing action research and is completely involved in the research [19]. Ottoson present several positive aspects of participatory AR; access to top management and employees, researcher obtain a very deep understanding of the process, the dialogue is the focus of action research and unspoken needs and demands can be discovered [19].

Dickens and Watkins reviewed the historical and contemporary definitions of AR, the process and the goals of AR [20]. Lewin argued for action research because of the limitations of studying social problems in a controlled laboratory environment. Rather than studying a single variable within a complex system, Lewin preferred to consider the entire system in its natural environment [20]. The action research participants begin with little knowledge in a specific situation and work collaboratively to observe, understand, and ultimately change the situation, while also reflecting on their own actions [20]. Dickens and Watkins states that action research has evolved from Lewin's ideas, but the evolved models follow the thread and connects back to Lewin.

The method of involving the employees is also used in other field of research with effective results. Levin and Klev stated that involvement of the users has been one of the most important tools for change [21]. It has also showed to be effective in the safety psychology, with the use of cross disciplinary group-based approaches [22]. In the risk research area the interaction between the experts and the employees create and improved understanding of risk and risk mitigation [3].

Because of the advantages of AR and the fact that Norsk Tipping wants to try a different method to improve security awareness and education, a method based on principles from AR is chosen in this project. The fact that researchers also has used such methods and achieved positive results strengthens the choice of an AR-based model. The fact that the method can be easily adjusted towards the employees makes this a preferred method because of the time and resource aspect of the project.

In order to define if the method based on principles from action research actually improves the security awareness and compliance, the method has to be evaluated. Measuring security is a difficult task because it is difficult to find suitable metrics. This following section will address the literature on security awareness measurement methods either completed through similar experiments or related to security measurement in general.

Puhakainen presented empirical data in his PhD dissertation. He used two different cases with companies in order to measure the improvement of an information security awareness program. The first case included all the seventeen employees in a software company and the entire intervention took place over an eleven-month period [5]. Puhakainen used three methods for collecting the research data; (1) interviews, (2) survey and (3) participatory observation. The survey contained open questions to explore employees' knowledge and skills while the interviews were both individual and in groups [5].The participatory observation was conducted in the eleven-month project where Puhakainen spent several weeks at the organization. These three methods were used to measure the improvement of security awareness, with the survey as a pre-test and the interviews and the observation as post-tests.

The second case was an intervention with a business unit in a large Finnish corporation. The intervention was conducted over a ten-month period with 37 employees [5]. In this case Puhakainen used an anonymous survey as a pre-test. This was used to gather relevant data. In addition he used group interviews to determine important information before he started the training. As post-tests Puhakainen used an anonymous survey and group interviews. Both the experiments of Puhakainen use a pre-test post-test method to measure the improvement of the participants.

Albrechtsen has performed several single studies over the last 6 years measuring security awareness improvement [3, 6]. In one study Albrechtsen performed a qualitative study on employees in two different companies, a bank and an IT-company. He used qualitative interviews on 19 employees in each company and the interview lasted about 1 hour [3]. By using these interviews Albrechtsen got the users experiences on information security related to their daily job. In another study Albrechtsen and Hovden created an education program with small sized workshops to improve security awareness and behavior. In this study the researchers used both a quantitative evaluation with three web-based questionnaires. Since not all of the employees participated in the education the researchers also had a control group that answered the questionnaires. The three surveys were conducted one month before the intervention, one month after the intervention and six months after the intervention [6]. In addition to the surveys the researchers used a qualitative evaluation. This was used to evaluate how the workshops influenced awareness and behavior. The approaches used were group-based discussions, observation, in-depth interview with security officers and data from the surveys [6]. The second method has many similarities with the methods used by Puhakainen, while the first method does not evaluate the actual behavior but it evaluate the impressions and feelings of the users.

Hagen investigated the effectiveness of implemented organization information security measures in her PhD dissertation [23]. Hagen suggested three practical methods to evaluate the effectiveness. A taxonomy was developed to evaluate the security practices, the use of Spearman Correlation Analysis with lagging indicators such as reported security breaches and economic performance indicators [23]. The thesis also presented how questionnaires and personal interviews can be used to measure employee compliance with security policies and security guidelines [23].

PricewaterhouseCoopers[11] did a survey for ENISA[12] in 2007 where they addressed what governments and private companies are currently doing for assessing the impact and success of awareness raising activities [8]. This report gives an indication of how large European organizations measure and improve information security awareness. The main findings of this survey were a variety of methods used to measure security, but the organizations found it very difficult to put effective metrics in place. In addition the audits of the organization were the most popular source of actual behavior. The most effective metrics presented was security incidents due to human behavior, audit findings, number of staff that completes training and qualitative feedback from staff among others. But the aspect of actual measuring the effect on an awareness training program or behavior toward the security policy is still difficult to achieve. Should it be used historical derogations or incidents, or should the actual behavior be measured with observation or penetration testing to get empirical data?

Thomsen and von Solms stated that to improve compliance, education and awareness campaigns can create a big impact on the employees [24]. They introduced a maturity model for information security competence in order to evaluate how well the information security is embedded in a corporate culture. There were 4 levels from unconscious incompetence to unconscious competence. The first stage is called unconscious incompetence. At this stage the employee is not aware of the tasks that must be performed and there is a deficiency in the skill needed to perform the task [24]. The second stage in the matrix is conscious incompetence. The employees are now aware of the existence and relevance of the task to be performed [24]. They know what actions are “right” and “wrong” but they do not know exactly how to perform these tasks.

[11] www.pwc.com
[12] The European Network and Information Security Agency

The third stage of the matrix is the conscious competence where the employees need to concentrate and think to be able to perform the task. The employee will not be able to perform the task unless thinking about it and making a mental effort, as the task has not become 'second nature' or part of the culture [24]. In order to reach the final stage employees must practice to become unconsciously competent. The unconsciously competent employee may even have difficulty in explaining how a task is done as the task has become mostly instinctual [24].

There are different methods used today to measure security. The report from ENISA concluded that the large corporations and governments in Europe used a variety of methods in order to measure the employees [8] . One way of measuring security is to use a model or matrix to define the security level of an employee. Examples of including models in the evaluations are Nonaka's "Spiral of Knowledge", Argyris' double-loop learning or Bloom's taxonomy [24-26].

The "Spiral of Knowledge" is a model created by Nonaka and Takeuchi. This model addresses the development of tacit and explicit knowledge in an organization. By alternating between these two modes, knowledge evolves from an individual level and moving up through expanding communities of interaction. The knowledge creation can cross sectional, departmental, divisional and organizational boundaries [26].This model relates to the development of a new product, but it has many similarities with action research and the development of tacit knowledge in an intervention. It can therefore be adopted to create security knowledge in an organization.

Another method is to use penetration tests. This is a method that Norsk Tipping has used to measure the effect of their annual security training. Penetration tests measure the actual behavior of the employees and do not directly measure improvements on awareness. The tests are often performed by security professional and can be an expensive alternative. In addition measuring security behavior is difficult, time-consuming and can have a negative impact on the corporate culture.

Questioners and interviews are also a popular method for measuring information security awareness. These are often a more economical method than penetration testing and can be used to measure improvement in security awareness and knowledge. Puhakainen and Albrechtsen use this form of measurement when doing experiments.

The report from ENISA presented security incidents due to human behavior, audit findings, number of staff complete training and qualitative feedback from staff among others to be the most popular used metrics in the large organizations [8].

In 1956 a team of educational scientists developed a classification of learning objectives within education. This work was led by Bloom and was published in "*The Taxonomy of Educational Objectives, The Classification of Educational Goals, Handbook I: Cognitive Domain*". This classification become known as Bloom's taxonomy and is regarded as a fundamental element within the educational community. The taxonomy is divided into 3 domains; (1) affective domain that addresses feelings and emotional areas (attitude), (2) cognitive domain that address mental skills (knowledge) and (3) psychomotor domain which address manual or physical skills. The categories are arranged from simple to complex and are built up as a cumulative hierarchy; all the lower degrees must be mastered.

The cognitive dimension of the taxonomy is closest to the different methods of measuring security awareness. Thomsen and von Solms used a maturity model

where the employees had to complete an awareness program and security training to reach the highest levels of maturity model [24]. The cognitive dimension is categorized into six categories that can be thought of as degrees of difficulty. The six categories are knowledge, comprehension, application, analysis, synthesis and evaluation.

In the mid 90's Anderson et al. revised the cognitive domain and updated this to the 21st century work [27]. The two most prominent changes were the change of the nouns to verbs in Bloom's taxonomy and change the order of the two most complex steps. This work resulted in a two-dimensional table named the taxonomy table. The table is presented in Table 1.

The Knowledge dimension	The cognitive Process Dimension					
	1. Remember	2. Understand	3. Apply	4. Analyze	5. Evaluate	6. Create
A. Factual knowledge						
B. Conceptual Knowledge						
C. Procedural Knowledge						
D. Meta-Cognitive Knowledge						

Table 1 - Taxonomy table

In 2005 Anderson discussed the major differences between the original taxonomy and the taxonomy table, the way the table could be used to improve quality of assessment and instruction and how the table could be used to provide more accurate estimates [28]. One of the major differences is that the taxonomy table has two dimensions. This multidimensional aspect is consistent with other frameworks that have evolved since Bloom's taxonomy. A knowledge dimension has been added and is build on different amount of knowledge [28]. These are factual, conceptual, procedural and meta-cognitive knowledge. This dimension made it easier to place the learning objectives in the table. Anderson concluded that the table promotes shared understanding and meaningful communication. It can improve assessment, instruction, and the essential link between them [28].

Athanassiou et al. reviewed Bloom's taxonomy as a learning tool in 2003 [29]. They present growing awareness of the taxonomy's usefulness and richness among educators. Their way of improving education is to encourage students to develop responsibility for their learning and self-assess the quality of their work and contributions in lectures [29]. The taxonomy has received criticism that the levels are not always distinct, it is not strictly hierarchical and developed at the behavioral level and not a theoretical level. Athanassiou et al. also performed an empirical experiment to improve the students' critical-thinking skills. Most students improved their skills and reported the taxonomy tool useful [29].

Amer presented a critical review of both the original and the revised taxonomy [30]. The original taxonomy had the assumption that the cognitive processes are ordered on a single dimension from easy-to-complex behavior. In addition there has evolved several theories and approaches to organizational learning [30]. The

revised taxonomy has included these new approaches. The most notable change of the revised taxonomy is the move from one to two dimensions.

Results of the chapter:

- Description of Norsk Tipping
- Presentation of the main problem in the project
- Violations to the security policy in Norsk Tipping
- Increase ownership towards security
- Description of different methods to improve awareness and compliance
- Choice of improvement method

3 Hypothesis and research questions

Content of the chapter:

- Presentation of hypothesis
- Presentation of research questions
- Hypothesis in P'HAPI

This chapter includes the description of the research questions related to the project. The hypothesis and the research questions are developed and composed from the literature review and also the initial meetings with the problem owner. The research questions are used as guidelines for the project and define the context of the project.

Despite information security awareness education when employed followed by an annual security update, security test implemented by the security team in Norsk Tipping still reveals that employees violate the guidelines stated in the overall security policy. Norsk Tipping is interested in improving the security education and wants to try an additional method for teaching security to their employees. The literature review showed that there was a small amount of research with empirical data on security awareness, but in the latest years several researcher have performed single studies that has improved security awareness. Some of these researchers have used different methods based on action research. The main hypothesis for this project is that a method based on action research can improve security awareness amongst the employees. In order to check the validity of the hypothesis, the following research questions must be answered.

- Can a method based on principles from action research increase the knowledge and understanding of security to the employees in Norsk Tipping?

The two additional research questions are related to the measurement of the method. They are stated for validating the method and to find out if the method are successful and can be used as an additional method for improving the security awareness and compliance among the employees in Norsk Tipping.

- Did the employees find this method positive and effective for improving information security awareness and compliance?
    - What do they think of the process of the education and did the method improve their ownership towards security?

Another feature of the participatory model is that it is not only the employees that can get an outcome of such a process, but the security department will also be able to improve their knowledge on security information on different roles in the organization. By using discussion between the employees which are experts in their job role and the security department which is expert in security, the cogeneration of knowledge can improve the knowledge to the security team. This learning objective should also be investigated in the project.

- Can a participatory method based on principles from action research improve the security team's knowledge of specific security aspects for the employees?
    - Does the security team find this process effective and can it be used in the future?

The literature review reveals different characteristics that have showed to be successful in improving the awareness in single studies. The cogeneration of knowledge has been tested, but this is only tested in single studies and this may not fit the organization of Norsk Tipping. In addition to the cogeneration of knowledge, the security department might also be able to improve their knowledge on different security aspects in the company, when they get a closer dialogue with the employees.

3.1 Choice of method

There are several different techniques and methods for improving information security awareness and compliance. The most used methods today are web-based awareness programs and classroom education provided by the security team or security professionals. These methods have the advantages that they can reach out to many employees, with little use of resources from the security team. A web-based education program can be purchased from a vendor and modules that are important can be chosen. For classroom education the same content can be used on a large group of the employees. These programs can also provide a form of security measurement when web-based programs can include questions after a module or within the program and the classroom education can include a questioner at the end of the session. This can measure an effect of the improvement and provide the security team with statistics, but it is difficult to measure successfully, when people can answer what they think is best for the security team.

The advantages of the two educational programs can also have a negative effect on the information security awareness and compliance improvement. In large companies there are often different level of skill when it comes to IT and information security. When all the employees are exposed for the same security content, this has to be on a general level, in order to have an effect on the least knowledgeable employees. This can therefore have a negative effect on the employees that have more knowledge. These employees can see the sessions as boring and have negative effect on their security culture. It can be more difficult to create an important security dialogue and many employees can be too afraid to ask important questions in a large group.

When using a web-based program too general content is also a problem for the employees. This method has many similarities with the classroom education described above. These programs address general security topics and important security aspects of the different roles in a company may never be addressed. A web-based program can be tailored to special group of employees, but this requires resources when rearranging the different modules to suitable content.

The first implications of a functional method were discussed on a meeting with the problem owner spring 2010. The terms security awareness and compliance had been discussed earlier and the first discussions on a participatory method was introduced. These early discussions were important in order to identify the requirements stated by Norsk Tipping.

After several discussions with the problem owner and identification of similar research-studies completed within other companies, a participatory method was chosen. This type of awareness training seems promising and is different from the dominant class-room and intranet-based approaches. Because of the use of employee participation and the aspect of ownership, this method could be adjusted for Norsk Tipping's demands. Several single studies with empirical evidence have been presented by researchers and the guidelines from the security department in Norsk Tipping could be attained. There has also been a trend in the latest years where participation and small group interventions are used to address security awareness and compliance with positive results. That makes a participatory AR method particular interesting to test.

Results of the chapter:

- Description the research questions related to information security awareness and compliance improvement
- Foundation of the following design and test implementation of the participatory method

4 Design of method

Content of the chapter:

- Presentation of the participatory method design
- Presentation of the implementation of the participatory method Documentation of the group interventions with the participants
- Analysis in P'HAPI

In this chapter the design of the participatory method is described. This design is created from the provided literature, discussions with the problem owner and is based on the research questions stated in chapter 3. The description of the participatory method is provided in this chapter including the security adjustments to the revised taxonomy, description of the interventions included in the method and an evaluation of the method design.

After several discussions with the problem owner, the key aspects of the method were identified. The main goal of the project was to design and test a method for improving the information security awareness and ownership among a group of employees in Norsk Tipping. The project report should also be used as a foundation for further work and improvement of the method, so recommendations for measurement and additional features should also be included. The project process was initiated with an identification of the organizational structure and the security documentation of Norsk Tipping. This information was used as background information to adjust the method and meet the requirements provided by Norsk Tipping.

A model based on AR has several strengths when it comes to information security awareness and compliance. In this project the employees are experts on not just the security aspects, but also the non-security aspects of their job-function, while the security team and the researcher are experts on security and the AR framework. AR is a method that captures the important tacit knowledge and can change this to explicit or documented knowledge. The abilities to adjust the security content towards the employees and improve ownership towards security are strengths in this method. The employees help to shape the research and are responsible, together with the security team, to address the most important security aspects. This might improve the ownership to the employees who attends the session. AR is often based on small group interventions where the researcher participates as a facilitator or has special responsibility for guiding the sessions.

A method based on principles from AR will use time and resources of the security team. The design of the method and all the requirements of the group intervention must be planned. Such a framework should be designed in order to meet the requirements of as much of the employees as possible. In an organization with many employees and different level of knowledge, the employees can be categorized in order to improve the awareness education. When these groups of employees are identified, adjusted security education can

be provided to several groups despite that the roles of the employees are different. By implementing such a mapping of the employees, the security team can tailor the security education toward the employees.

Despite the amount of resources a method based on AR is chosen as the additional method to improve information security awareness and compliance in Norsk Tipping. This method will be significantly different from the educational approaches used today and the important aspects of participation and ownership might have a larger role with such a method.

Another aspect that was discussed on the meetings with the problem owner was the ability to measure the improvement of the employees. This was a feature that Norsk Tipping wanted as a result for evaluating the participatory method. Measuring actual security awareness improvement and improvement of behavior is very difficult and complex. It is difficult to find the suitable method and the corresponding security metrics.

In order to evaluate the participatory method and group interventions with the employees, qualitative interviews were chosen as the preferred method. Because the participants are active in the research the training also work as a mapping of security in the different job-roles, a pretest/posttest was decided to not be functional. This type of measurement was used in the singles studies identified in the literature review, but because the lack of time and resources in this project it was decided to use qualitative interviews as evaluation of the group interventions.

One important issue with only using an interview at the end of the test phase is that the actual improvement of the participants is not measured. The results of this interview are the feelings and experiences the participants have after the session. The impressions of the participants are important indications for the security department when deciding if the method is suitable for Norsk Tipping. The method is a proof of concept and can be seen as the first phase of a continuous improvement of the security awareness of the employees. A measurement of the employees after the group intervention should be completed in order to investigate the possible improvement of the participants in the future.

4.1 Description of the content

The core feature in the participatory method is the small group intervention with the employees. This is where the identification of tacit knowledge and co-generation of knowledge is completed and it is vital that this intervention is positive for the participants for improving awareness and ownership. The employees are included as experts on their job role and are important for the outcome of the intervention. In the planning phase of the project important concepts that should be included in the intervention were identified.

The first important action was to define the content of the intervention. The content had to cover the security documentation of Norsk Tipping, which is the basis for all security training in the organization. After reviewing the security policy, the security handbook and the ISO/IEC 27001 standard it was decided that the different security categories in the standard covered the responsibilities of the employees. By including these categories the lifetime of the method would be increased, because the standard is the core document for security in Norsk Tipping.

Some of the security categories were more suitable to awareness training than others. It was important that the categories were easy to understand for the participants and that it was possible to relate the content to situations that affected the employees. Eleven security categories were chosen as the framework of group intervention.

After the definition of the content it was investigated how the employees should be categorized. The literature review had identified research that used classification of the employees. For this project Bloom's revised taxonomy was chosen. By adjusting the table towards security and by using a method based on AR, the employees in Norsk Tipping can together with the security department define their own level of awareness towards security based on this classification. When placing an employee in this table on different aspects of security, the security team can get an overview of what level the different departments is located at. This may lead to more adjusted security training in the future. The decision of where the employees should be in their job role can be a task for the department manager. This can create ownership and attention to security on the manager level.

The reasons for choosing the scale based on Bloom's revised taxonomy are the popularity and diffusion of the taxonomy and the amount of resources available in the project. By translating the levels to security the strengths of the process dimension is attained. Another aspect is that the model should be easy to understand and use and by adopting a model which is thoroughly documented and explained the resources can be used on adjusting the model instead of developing a new model for Norsk Tipping. In the following section the different cognitive level are explained. This documentation is from the book by Anderson et al. [27]

Level 1 - Remember

The first level of the taxonomy is called remember. Remember is the only phase that promotes retention[13]. The other five levels promote transfer of knowledge. Remembering involves retrieving relevant knowledge from long-term memory. This is often realized by addressing the knowledge in the same conditions as it was taught. Remembering is an essential foundation for meaningful learning, problem solving and the ability to accomplish more complex cases.

There are two cognitive processes in the category. These are *recognizing* and *recalling*. The cognitive process *recognizing* means to search the long-term memory for information that is identical or extremely similar to the presented information. *Recalling* is to bring the relevant literature to the working memory where it can be processed. These aspects have to do with identifying, locating and retrieving the relevant knowledge in the long-term memory. Examples can be to retrieve important names or dates from a historical event.

This level can be closely mapped to the security handbook of Norsk Tipping. The document presents the security guidelines defined by the security team and all the employees have to read the handbook and sign that they have understood the material. The relation to the taxonomy is that the employees are able to recall the different guidelines stated in the handbook. A question in this phase can be stated as; "What are you supposed to do if your computer is infected with a virus?" This is the level that all the employees in Norsk Tipping should manage.

Level 2 - Understand

Understand is the second level of the cognitive process and the first phase to promote transfer of knowledge. The transfer of knowledge is the ability to use

13 Retention – the ability to retain facts and figures in memory

what is learned to solve new problems or answering new questions. When a person understands he is able to construct meaning from instructional messages whether it is from oral, written or graphical communication. When an employee builds a connection from their prior knowledge to the "new" knowledge, he understands.

There are seven cognitive processes in this category. *Interpreting* is the first process and occurs when the employee is able to convert the information from one representational form to another. An example can be to convert pictures to words. The second process is *exemplifying* where the employee gives a specific example or instance of a general concept or principle. The third process is *classifying* where the employee recognize that something belongs to a category. This can be to identify relevant features or patterns of a concept. *Summarizing* is the fourth process and occurs when an employee abstract a general theme or create a single statement of presented information. Process five is *inferring* and involves finding a pattern in series of examples. *Comparing* is process six and involves detecting similarities and differences between to objects. The last process is *explaining* and it occurs if an employee is able to construct a cause-and-effect model of a system.

When it comes to the security perspective understand is the first phase where the employees link "new" knowledge to their prior knowledge and meaningful knowledge is created. When adjusting the category to security, some of the processes are easier than others. Exemplifying and comparing are two processes that can be easily adjusted to security. Questions like; "Can you give an example on a secure password?", "what are the differences between the different classification levels for documentation?" and "what are the differences between worms and viruses?" are questions where the employees show understanding when answering.

Level 3 - Apply

Apply is the third level in the participatory model. It involves using procedures to perform exercises or solve problems. Exercise referrers to a familiar task where the employee knows the procedure to use. A problem is defined as an unfamiliar task where the employee must use his knowledge to choose the correct procedure to use.

Executing is another name for performing exercises. The situation often provides several clues to guide the employee to the most appropriate procedure. This method is often associated with using skills or algorithms to solve the case. They often consist of a sequence of steps and in a fixed order. *Implementing* is the term used when the task is unfamiliar. When implementing an employee must understand the problem and also the variety of the different procedures available in order to solve the problem. A procedure may also need modifications in order to solve the problem.

For applying to the third level of the participatory method, the employees must be able to follow defined guidelines and procedures stated by the security department. When a problem is rising, the employee must use his knowledge and choose the most appropriate procedure, maybe with modifications, and solve the problem. Questions; "What do you do if you meet a person without identification in the hall?" "How do you define the classification of a document?"

Level 4 - Analyze

The fourth level of the model is to analyze. Analyze involves breaking material into parts and determining how they are related to one another. There are three cognitive processes in analyze; differentiating which is learning to determine the

relevance of important pieces of a message, organizing, the way pieces of information is organized and attributing to determine the underlying purpose of the message.

Differentiating involves discriminating relevant information from irrelevant information and import information from unimportant information. This differs from the cognitive category understand because it involves structural organization and determine how parts fit into an overall structure. One example of differentiation is to identify main steps of a complex procedure. *Organizing* is the second cognitive process and involves identifying elements in a situation and recognizes have they fit into a coherent structure. An employee must be able to identify relationships among elements in order to fulfill the demands of the level. *Attributing* occurs when the employee is able to ascertain the point of view, biases, values or intention of underlying communications.

Identifying security related aspects similar to the analyze level the differentiating and organizing are important aspects. One example of analyzing a security aspect is to identify major points why Norsk Tipping has a security handbook and what are the main messages.

Level 5 - Evaluate

The fifth level in the participatory model is to evaluate. Evaluate is to make judgments based on criteria and standards. Examples of criteria can be quality, effectiveness, efficiency and consistency. There are two cognitive processes at this level, checking and critiquing.

Checking involves testing for internal inconsistencies or fallacies in an operation or a product. Operations like detecting and monitoring can be used in the evaluation of a system. *Critiquing* is based on judging a product based on external criteria and standards. One example of this is to identify positive and negative features of a system and based on those make a judgment.

In security the ability to evaluate can be important for employees that have business critical functions. When an employee has the ability to evaluate a security system he must have a deep understanding of the system together with the relationships towards its related systems. A question for this level can be; “List the pros and cons for the mail system at Norsk Tipping?”

Level 6 - Create

Create is the highest level of the model. On this level the employees should be able to put elements together to create a functional whole. This can be done by using different known elements but it requires modification in the process. There are three cognitive processes related to the create level.

Generating is the first process which involves representation of a problem and arriving at alternatives or hypotheses that meets certain criteria. This is often realized through suggesting different solutions to a problem where this process often is called creative thinking. *Planning* is the second cognitive process and involves the solution method that meets a problem’s criteria. In other words create a plan for solving the problem. One method is to establish subgoals or break the problem into several sub-problems. The last cognitive process is *producing*. This involves carrying out the chosen plan for solving the problem. It may include uniqueness and originality but this is not a requirement in the taxonomy.

When adjusted to security, this last level demands that an employee is able to generate alternative solutions for a problem, create a plan and carry out the plan in order to improve the situation.

The use of security categories and Bloom's revised taxonomy resulted in a table that was used in the different group interventions. This document included the different security questions in each category and also the cognitive levels by Bloom. The table was used to identify the expected and actual cognitive levels of the employees. By marking the defined level with an x for the expected level and a star for the actual level, it was easy to identify the special security considerations for the employees and the potential gaps of the employees. In Table 2 the framework for the interventions is visualized.

ISO/IEC 27001 – security categories	Questions	1	2	3	4	5	6
A4 – Risk assessment	On what level should employees know risk assessment and risk analysis?						
A5 – Security documentation	On what level should employees know the security policy?						
	On what level should employees know the security handbook?						
A6 – Organization of information security	On what level should employees know the non-disclosure agreement?						
	On what level should employees know the core concepts of information security; confidentiality, integrity and availability						
A7 – Asset management	On what level should employees know the guidelines on portable assets?						
	On what level should employees know the classification guidelines?						
A9 – Physical/environmental security	On what level should employees know the physical guidelines in Norsk Tipping?						
A10 – Communication and operation management	On what level should employees know handling and protection against mobile code?						
A11 – Access control	On what level should employees know the guidelines for password handling in Norsk Tipping?						
	On what level should employees know the handling of unattended equipment and clear desk philosophy?						
A12 – Information systems acquisition and maintenance	On what level should employees know social engineering and information leakage?						
A13 – Incident management	On what level should employees know the guidelines on incident handling?						
A14 - Business continuity management	On what level should employees know the business continuity plans in Norsk Tipping?						
A15 – Security documentation compliance	On what level should employees comply with the security documentation in Norsk Tipping?						

Table 2 - Framework for interventions

4.2 Description of interventions

The main part of the participatory model is divided into two interventions. The first intervention is a meeting with the line manager of the employees who will attend the group-based intervention. The aim of this intervention is to present the basic ideas of the framework for the second intervention. This meeting is used as a preparation for the manager and gives him the opportunity to think of the group session before the main intervention. This may improve the discussions and the outcome of the second intervention. The second intervention is the group-based intervention with both the line manager and his employees. This is the main intervention and is where principles from action research are introduced and the ownership towards security can be improved. The interventions are described in the following section.

Intervention 1 – Meeting with manager

The first intervention is the meeting with the line manager of the group of employees who is attending the second intervention. In Norsk Tipping the manager has the responsibility for addressing security to his employees, so in order to improve awareness and ownership towards security, the line manager is important. In this intervention Figure 2 is presented together with the main goals of the second intervention. The main reason for having this intervention is to prepare the line manager for the following session. The line manager can then identify important aspects that he wants to include and prepare statements for the desired cognitive levels.

This session can help to define what level of security the employees should have in the different categories and it can also improve the ownership towards security for the manager. In addition this session can identify new aspects of security that the security department did not know which is important for the group of employees.

The introduction to the meeting is an explanation of the goals for the intervention together with an extensive explanation of Figure 2. It is important to assure that the manager understands the purpose of the intervention and how the model is constructed. Explanations of the different cognitive levels and their differences are also important for the outcome of the intervention. The managers are suggested to study the model and its explanations before the group intervention.

Intervention 2 – Group intervention with the employees and the line manager

The second intervention in the participatory method is the session with the small group of employees including the line manager. This intervention is the core of the participatory method and is where the principles from action research are introduced. The method is tested with two groups of employees that are defined as business critical and two groups that are not defined as business critical.

The intervention starts with an explanation of the main goals of the session and the participatory model. The extensive explanation is provided for creating a mutual understanding of the model for the employees and the manager. Important aspects like discussion, participation, cogeneration of knowledge and improvement of ownership towards security are explained in this phase of the session. It is important that the employees understands the model and the goals of the group session in order to create a functional method for improving the security awareness and ownership.

After the introduction, the main task of the session is introduced. This is the discussion between the security department, employees and the line managers

where the aim is to define the cognitive levels of the employees in the different security categories in the model. In this discussion it is important to address the actual role of the employees and try to identify situations and examples related to the security categories. With the help of these examples and situations the group should be able to agree on the expected cognitive level of the employees. It is important that all the participants have the opportunity to present their meaning on the different categories and the cognitive levels. If there is a disagreement on the expected level, it is important to identify the reason and try to find a solution to the problem. The security department should take an active role if it is identified disagreements in the categories. The discussion on the different security categories is important in order to improve the ownership to security for the employees. The employees are included in the definition of their security requirements and can help to shape the security education.

In addition to define the expected cognitive of level the employees, the group also evaluates the employees in the different security categories. This is done by asking control questions and discussion within the group. When defining the security performance of the employees, it is important that the employees are honest and try to give a realistic view on the employees. This evaluation is important for the security department because the potential gaps and potential risks are identified. When this is done together with the employees the thoughts and feelings of the employees are included and this can improve the security overview for the security department. The security department can get an overview of the different groups of employees and choose to address education to a large audience, or address specific and more critical gaps in the model.

To answer research question 2 and 3 the intervention must be evaluated. Because the employees participate in defining the security levels and the timeframe of the project, the measurement of the method will be based on qualitative interviews with the participants of the group session. These interviews will be based on feedback from the employees on the group session. Because the actual security level cannot be measured in the project, it is important to see if a method based on participation can be introduced in Norsk Tipping and if the employees found it positive and interesting. The results can then be used by the security department to decide if they want to adopt this method for additional security education.

Figure 2 visualizes a possible outcome of a group intervention. On the right side of the model eleven security categories is presented. These categories are adopted from the ISO/IEC 27001 standard. On the left side of the diagram the cognitive levels adopted from Bloom's revised taxonomy is visualized. The different columns in the middle visualize the expected cognitive levels of a particular job role. Figure 2 represents a fictitious department.

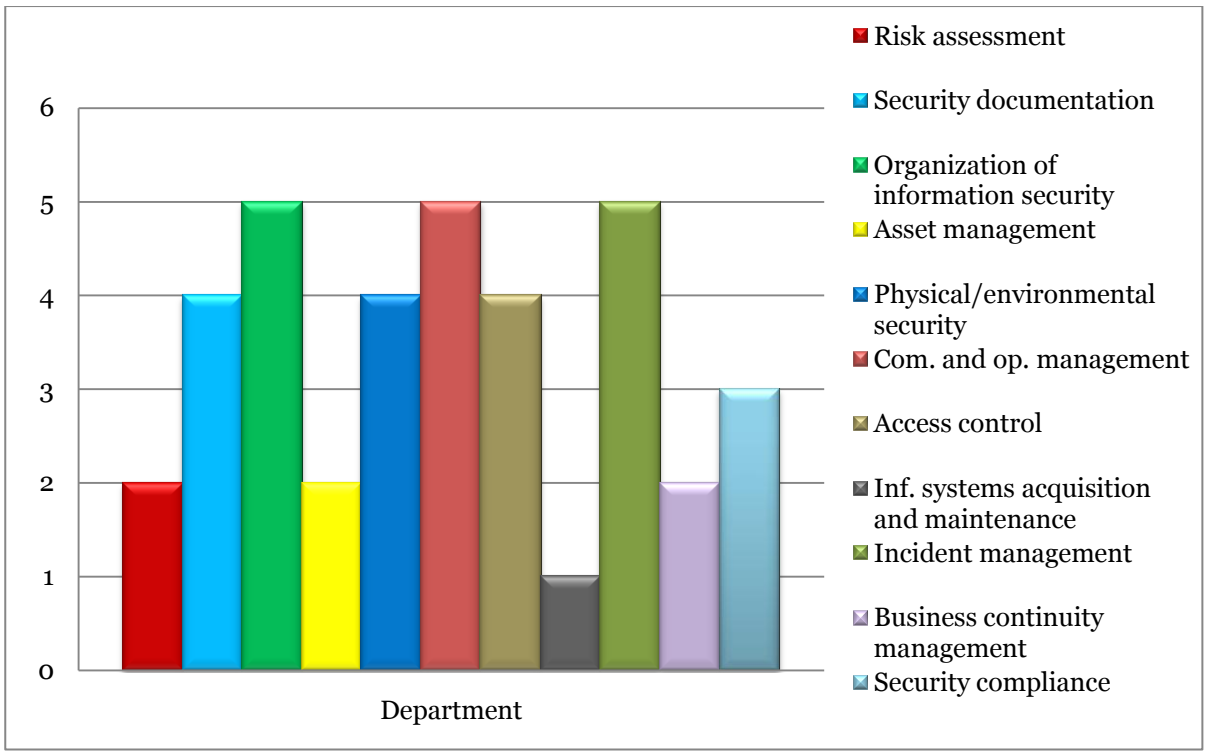


Figure 2 - Fictitious model

One of the strength of this type of model is its ability to adjust to different groups of employees. Because the method addresses dialogue and cogeneration of knowledge, one main goal in the intervention is to identify special security considerations for the group of employees. This issue may be more important for some groups of employees (the business critical functions), but the opportunity for identifying special categories is available for all the groups. This identification is important for the security department because it can reveal special considerations that the security department was not familiar with. These aspects can also be a major security threat for the company. In this project the security categories that are defined to be level 5 or higher, organization of information security, com. and op. management and incident management in Figure 2 is defined special security considerations.

Evaluation of the method

The fictitious model was used in different ways in the group interventions. It was used in the explanation of the intervention process in order to make the employees understand their tasks. In addition the model was used as a basis for the discussion in the group intervention. The different security categories adopted from the ISO/IEC standard were used to address the different security areas of the employees. The main function of the model was as a measurement tool of the employees in the group intervention. When the employees defined the expected and actual level the model was used to identify the gaps between the cognitive levels. This makes it easier for the security department if they use these diagrams for mapping the different job-roles in the organization.

By including this model in the participatory method was easier to explain to the participants in the test phase. Adopting the cognitive classification from Bloom's revised taxonomy improved the method with clear distinctions between the cognitive levels that made it easier for the employees to find a suitable level in

the different security categories. Adopting the relevant security categories from the ISO/IEC standard made it easier to cover the important areas for security.

Because the model was adopted from an educational environment, there were challenges to adjust the cognitive levels to security. The lowest categories were easy, but it was more difficult to define security related examples in the highest categories. This should therefore be modified in the future in order to create a more solid model, either with more examples or adjust the classification.

Results of the chapter:

- Designed a method based on action research
- Designed a model as a measurement tool and basis for discussion in the intervention

5 Implementation of the participatory method

Content of the chapter:

- Documentation of the meetings with the line managers
- Documentation of the group interventions
- Evaluation of the group interventions
- Analysis in P'HAPI

This section addresses the implementation of the participatory method. The documentation is based on the different interventions that have been completed; the interventions with the line managers and the main intervention with all the employees from the different departments. The process is described and analyzed and the results are provided in the next chapter. The group interventions were completed with particular groups of employees and their managers in the different departments. The name of the departments is used for protection of privacy for the participants.

Meeting with line manager in games production
The line manager in games production has the responsibility for one group of employees in the department. The meeting was held to prepare the line manager for the following group intervention. This department has responsibility for the operations for the organization and it important to address the identification of special security considerations that could be important for the security department.

The meeting started with a short introduction of the researcher and the main goals of the project, followed by the explanation of the security categories in the fictitious model. The line manager had a deep understanding of the standard because the department is also complying with the standard and has to perform revisions together with the security department. The manager had no objections for the choice of the security categories.

The cognitive levels of the model were described to the manager together with the goals of the meeting. Because the employees are part of an operative department, the manager informed that the employees had to be on standby under the group session. Because of this responsibility, we might lose one of the employees. This will impact the results of the group session because we may only have on opinion from the employees and it will impact the discussion. The employees work shifts and that was the reason for having only two employees.

The manager had created a solid understanding of the model and the cognitive levels before the meeting. The manager expressed that the employees had several security considerations that should be addressed in addition to the security categories. These are important to identify in order to create a functional result that corresponds to the business functions of the department.

Overall, the manager was positive to the method and agreed on the benefits of adjustable security education, increased security awareness and ownership. The method was an exciting and different way of addressing security.

Before the group session with the employees, the researcher and the security department discussed the fictitious model and suggested placement for the employees in the different security categories. This meeting was used to get an impression of the employees and discuss if it could be specific security aspects that should be discussed.

Group intervention games production

The first group session was conducted with the employees together with their manager. It was scheduled for 1 hour and 30 minutes and it were two employees present. The group session was conducted on March 28th.

The group session started with an introduction of the researcher and the main goals of the project. This was provided in order to create an overview over the session and as an explanation to why the group was assembled. After the short overview an explanation of the following process was given. The two main objectives for the group session were explained; (1) the definition of the expected cognitive levels of the employees, (2) the evaluation of the employees and on what level they actually were on. The special security considerations were identified in the two phases when the group discussed the security levels in the different categories. The participants gave the impression of understanding the objectives.

In the next phase of the session the participatory model was introduced to the employees. Some of the different security categories were explained including a few examples and the link towards the ISO/IEC standard was explained. After the short description of the security categories the cognitive table was introduced. Each of the levels was explained and links to examples were provided.

After the introduction part of the session, the first objective was started. This was to define the expected cognitive level of the employees. The first security category in the model was risk management. Because it was the first category, the security department provided examples and explained what risk management meant in Norsk Tipping. After this discussion and explanation of the security terms, the group defined that the employees should be at level 5 when handling risk. The employees did not use the terms stated by the policy, but they evaluated incidents when they were identified and this was an important task for the employees.

The second category is the security documentation in Norsk Tipping. The employees were now more familiar to the model and it was easier to define the expected level. When it comes to the security policy in Norsk Tipping, the group agreed on level 3 – use. This was the same level as the security team had suggested and is reached if the employees understand the security principals and follow the guidelines that are derived from it.

The following question in the category was directed at the security handbook. The security handbook includes the guidelines for the employees and is a living document in Norsk Tipping. The group agreed that the employees should be above the use-level and be able to analyze (level 4) the requirements. This means that the employees have decided a higher cognitive level for the security handbook than the security policy.

Security category three is organization of information security. The first question was about the importance of the non-disclosure agreement for the employees. The employees have critical knowledge about systems in Norsk Tipping and have access to important IT-systems, so the cognitive level should reflect this and the group defined the expected level t be level 5 – evaluation. Next question was

directed at the important concepts of information security; confidentiality, integrity and availability. The employees were not familiar with the terms, but when they were linked to examples the employees understood the importance. The group defined level 5 for the important concepts.

Asset management was the fourth security category. The first action was to define the expected level for handling assets and assets guidelines. The employees suggested that following the guidelines as a level 3 was a minimum and because of their handling of critical systems, they should be on a level 4 – analyzing. The security team and the manager agreed on this assumption. The following questions were based on document handling. When the group was discussing these aspects, one of the employees had to leave the intervention to deal with an incident. The rest of the intervention was completed with one employee. The employees did not create much information themselves, but they handled sensitive information. The group decided that the employees should be able to understand and follow the guidelines in the security handbook, a level 3 – use when it was classification of information. To label information is a concept in the security handbook and the group defined the same cognitive level for labeling of information.

Physical and environmental security was the next security category. There are described physical guidelines in the security handbook and the employees suggested that they should be on a high cognitive level in physical security. Level 5 – evaluation was defined by the group. The second question in this category was towards social engineering. Because the employees have access to critical systems and have important information about the systems, the consequence of a successful social engineering attack is big. Because of this risk the employees should be able to detect and evaluate these attacks in order to act securely towards Norsk Tipping. The group decided that level 5 should be the expected level.

Communications and operations management is the next category in the model. Within this category protection against mobile code[14] and management of removable media is covered. For knowledge and protection against mobile code the employees suggested being above average among the employees. They suggested being able to analyze the code and being on level 4. The employees have special access control to their location, but despite the technical defenses, the employees should treat removable media carefully. The group defined because of the criticality of the business function that the employees should be on level 4 on handling removable media.

The seventh category in the participatory model is access control. The handling and knowledge of passwords is an important security feature for Norsk Tipping. The employees suggested that the expected level should exceed a use – level and perhaps higher. After some examples the group defined the expected level to be evaluation – level 5. Unattended equipment is also covered in this category. The employees explained that had special access to their location and did not have extensive use of equipment outside this perimeter. But they stored important information on their laptops, so a level 4 was defined by the group for unattended equipment. Clear desk policy is the last question in this category. The group defined, based on the amount of sensitive information, that the employees should follow the guidelines and be able to analyze why this guideline is described in the security handbook.

[14] Virus, worms and malicious software

Information systems acquisition, development and maintenance are the next security category in the model. In this category the knowledge of information leakage is investigated. The employees might be a target for social engineering because of their access privileges and their knowledge to the systems. The group defined that the employees should be at level – 5, evaluation in order to withstand such attacks.

Category nine is information security incident management. The employees are one of the departments that have to deal with change and security incidents frequently. Because this is one of their main tasks, it is important that they are on a high cognitive level when handling these incidents. The group agreed on the evaluation level (level 5) in the model.

Category ten addresses business continuity management. Business continuity plans are important documentation that must be reviewed and updated regularly. The employees suggested that they should be at a high level in the model because they develop continuity plans and have to be able to evaluate the risk on new incidents. The group defined the expected level to be 5 for the employees.

The final security category is about compliance to the security documentation and guidelines developed in Norsk Tipping. This category is a general measure of the compliance of the employees. The group defined that the employees should follow the guidelines and procedures that are defined in the security handbook. If they do comply, the risk to the organization is manageable, but the employees have several high placements in the model and this should be monitored.

The second phase of the group intervention was to evaluate where the employees actually were in relation to the expected level defined in phase one. This was done to identify if there were any gaps that could be a security risks for Norsk Tipping. It was important that the employees were honest in the evaluation and gave reasonable explanations to the different categories.

In the risk management category the employees performed risk assessment when a new incident was identified. Even though the employees rarely used the same terms for the activities, they had routines for handling new incidents and were doing this automatically. Because of this the group defined that the employees met the expected level, level 5.

In the second category security documentation, the employees suggested that they met the requirements on the knowledge on the security policy and followed the guidelines and were familiar with the security handbook. Their manager supported the suggestion and agreed on the cognitive levels in the category.

The organization of information security was the third category and the group decided that the employees met the expected level defined in the first phase of the group session. The employees were familiar with the terms in information security and knew the non-disclosure agreement.

The first gap identified in the group session came in the asset management. Both the manager and the employees agreed that they did not meet the requirement on labeling documents. There expected level was level 3 – use, but they suggested that the employees were on a level 2. On the other questions in the category the employees meet the requirements defined in the first phase.

In physical security the employees set the expected level to be at level 5 on the security guidelines in Norsk Tipping. Because they worked in a special zone in the location, with additional access control, they should be at a high cognitive

level and both the manager and employees decided that they met the requirements. In the second question in this category, regarding social engineering, the employees did not meet the expected level. It was the second gap of the session and the employees defined level 3 – use, and the expected level was level 5 – evaluate.

When the group discussed the physical security, the manager had to respond to the same incident that the other employee had to check out. This meant that the manager had to leave the session and we only had one employee to evaluate the rest of the categories. When the manager disappeared and with only one employee, the core features of this method was lost. The group discussed the rest of the categories, but with a small amount of discussion and no manager, the results may not be correct. The researcher and the security department decided to complete the intervention on a later stage with the employees and the manager.

Evaluation of the group session with games production

The first group session resulted in an amputated session, but it identified several points of improvement that should be implemented to the model. Because the employees had an operative responsibility, we were prepared that we may lose one of the employees if an incident occurred. But the incident also required the manager, so without these two the important aspects were not fulfilled in the last phase of the session. Because of this incident, the researcher and the security team decided to schedule a new session with the games production department.

The session identified several possible improvements to the security categories and the evaluation of the employees. One of the improvements was to merge some of the questions, because they addressed similar aspects for the employees. This would decrease the number of questions and increase the time for discussion and evaluation.

Despite that the session was slightly amputated, we got some important results. During the discussion on the security categories it was discovered a difference in the use of terminology. The employees did not use the same terms for risk management as stated in the security documentation. It could be beneficial for Norsk Tipping to use the same terms in every department to increase the understanding and avoid misunderstanding in project across the departments.

To increase the security awareness was also a goal for the session and this was identified in the implementation. Despite the difference in terms, the employees performed risk management often without thinking “security”. With examples and discussion the employees showed an improved awareness on this category. The employees increased the participation throughout the session when they were more familiar with the model and the method.

Second group intervention games production

Because the complications in the first group intervention, it was decided that the second phase of intervention should be completed with a second intervention. The main focus in this intervention was to define the actual cognitive level of the employees and identify potential security gaps in the cognitive dimension. The session was completed with the manager and one of the employees that had participated in the first intervention. The other employee did not have the opportunity to participate. The meeting was scheduled to 1 hour.

In the first intervention the group defined that the employees should be on a level 5 in risk management. This is one of the important roles to the employees and is frequently performed. The expected level of the employees was suggested

to be a level 3. Despite that they do this regularly, the manager and the employee explained that there should be more awareness and education related to the templates that is used throughout Norsk Tipping. This will help the employees when they are participating in project across the departments.

The second category is security documentation and the first question is related to the security policy. In the first intervention the group defined that the employees should be able to understand and follow the policy, level 3. Whit the control questions and examples on the policy the group defined that the employees was on level 0. The manager suggested increasing the awareness towards the policy. The security handbook was the following question and the expected level of the employees was defined as level 4. The group defined that the employees met this requirement based on examples provided in the intervention.

In the third category the non-disclosure agreement is addressed and in the first intervention the expected level was set to level 5. The employees handle sensitive information and it is important that they are familiar with the agreement. This was an important area for the manager and the group defined that the employees meet this requirement, level 5. In the following question the core concepts of information was addressed. The group defined the expected level to be level 5 in the first intervention and identified a gap in intervention two. The employees did not use the same notion as the security department, so the group decided that they needed awareness and explanation of these terms. The actual level of the employees was defined as level 3.

Asset management was the following category in the model and the expected level was defined as level 4 regarding portable assets. The employees shared the work place and with the technical defenses like encrypted hard drive and use of VPN[15] the employees suggested to meet the requirement. The manager and the rest of the group agreed. Question two in the category addressed the classification of information in Norsk Tipping. In the first intervention the group defined the expected level to be level 3 and in the second intervention the group defined the actual level to be level 2. The gap in this category was based on lack of awareness to classification and the different level stated in the security handbook.

Regarding the physical security the group defined that the expected level was level 5. The group defined that this requirement was met by the employees. The following question addressed mobile code and the expected level was level 4. The employees must have an extensive knowledge in computing and the group defined that they met this requirement.

The seventh security category was access control. The group defined that the expected level regarding the guidelines and the handling of passwords should be level 5. Because of the complexity in the systems the employees must handle several passwords on a daily basis. This is an important task for the employees and the group defined that they met the requirement. The following question in the category addressed handling of unattended equipment and clear desk philosophy. Because the amount of sensitive information the expected level was defined level 4. The actual level of the employees was defined to be level 4 based on the explanations of the manager and the employees.

Gap number five was identified in the question addressing information leakage and social engineering. The expected level was defined to be level 5 in the first intervention, but the actual cognitive level was defined to be level 3. The lack of

15 VPN - Virtual private network

awareness and the fact that this threat should be addressed often because of its popularity were reasons for defining this level. In the following category the business continuity plans were addressed. The employees could be included if a crisis occur and the expected level was level 5. The documentation on the plans was revised and updated and if large cases occurred they could be included in the documentation. The actual level of the employees was defined to be level 5; they met the requirement stated in the first intervention.

The last security category addresses the compliance towards the security documentation in Norsk Tipping. In the first intervention the group defined that the employees should understand and follow the security guidelines and the expected level was level 3. The security culture and the knowledge of the employees showed that they met this requirement, but there were categories that needed attention to improve the security awareness. In Table 3 the results from the intervention are visualized. The x represents the expected cognitive level and the star represents the actual cognitive level.

ISO/IEC 27001 – security categories	Questions	1	2	3	4	5	6
A4 – Risk assessment	On what level should employees know risk assessment and risk analysis?			☆		x	
A5 – Security documentation	On what level should employees know the security policy?	☆		x			
	On what level should employees know the security handbook?				x ☆		
A6 – Organization of information security	On what level should employees know the non-disclosure agreement?					x ☆	
	On what level should employees know the core concepts of information security; confidentiality, integrity and availability?			☆		x	
A7 – Asset management	On what level should employees know the guidelines on portable assets?				x ☆		
	On what level should employees know the classification guidelines?		☆	x			
A9 – Physical/environmental security	On what level should employees know the physical guidelines in Norsk Tipping?					x ☆	
A10 – Communication and operation management	On what level should employees know handling and protection against mobile code?				x ☆		
A11 – Access control	On what level should employees know the guidelines for password handling in Norsk Tipping?					x ☆	
	On what level should employees know the handling of unattended equipment and clear desk philosophy?				x ☆		
A12 – Information systems acquisition and maintenance	On what level should employees know social engineering and information leakage?			☆		x	
A13 – Incident management	On what level should employees know the guidelines on incident handling?					x ☆	
A14 - Business continuity management	On what level should employees know the business continuity plans in Norsk Tipping?					x ☆	
A15 – Security documentation compliance	On what level should employees comply with the security documentation in Norsk Tipping?			x ☆			

Table 3 - Results games production

Evaluation of the second group session with games production

The second intervention with games production was conducted with one employee and the line manager. Despite the lack of members the session had interesting discussion in different security categories and the group was able to identify several issues that should be improved.

In five of the eleven security categories gaps were identified. All of the gaps were related to lack of awareness. In order to improve the situation for the employees

a security awareness program could be adjusted to the identified security categories. It was a positive tone in the intervention and the participants shared examples and situations to the discussion.

Development of control questions

To improve the evaluation part of the method, a set of questions was created for each category. These questions were used in addition to examples and discussion in each category in order to define the actual level of the employees. The questions are a mix of open and more targeted questions. They were used as spot-tests to identify if the employees met the cognitive levels that were defined in the groups. The questions were used in addition to the discussion of examples and situation and it was not enough time to ask all of the questions.

The questions have the same scale as the table used in the group intervention. This is adopted from the ISO/IEC 27001 standard and makes it easy to link the different categories to the standard. The questions were made short and easy to understand in order to function as spot-tests. The control questions are listed below.

A4

- Can you explain how a risk assessment should be conducted?
- How is a risk assessment constructed?
- What methods are used to handle risk?
- Why do we conduct risk assessment?
- What are important elements in a risk evaluation?

A5

- Can you repeat one of the security principles stated in the security policy?
- Can you give a short explanation of the distribution of responsibility described in the policy?
- What are your duties as an employee stated in the security policy?
- How does the classification of a document take place?

A6

- Can you repeat one of the statements in the non-disclosure agreement?
- What are the consequences of breaking the non-disclosure agreement?
- Can you explain the concepts confidentiality, integrity and availability?

A7

- What are the guidelines on handling electronic equipment outside Norsk Tipping's facility?
- How are you supposed to act if you lose electronic assets?
- How is the classification of information divided in Norsk Tipping?
- What are the differences between the different classification levels?
- Can you classify a document?

A9

- How should you act if you meet a person without visible identification?
- How should you act if you have a visitor during work hours in Norsk Tipping?
- What guidelines are defined for visitors in Norsk Tipping?

A10

- How should you act if you have suspicion of malware on your computer?
- What are characteristics of an infected PC?

A11

- Name three criterions of a strong password
- How should you store password?
- What are you suppose to do if you find an USB-stick?

A12

- Can you explain the term social engineering?
- What methods can an attacker use in a social engineering attack?
- How are you supposed to act if you think you are exposed to a social engineering attack?

A13

- How do you act if you identify a security incident in Norsk Tipping?
- How do you report a security incident in Norsk Tipping?
- Can you give three examples of security incidents?

A14

- Are you familiar with the continuity plans in your department?
- Have your department developed continuity plans? Are they revised?

A15

- Are you aware of security in your daily job?

Meeting with line manager retail and brands

In order to prepare the manager of the employees, it was held a short meeting for introduction. It started with an introduction of the researcher and the main goals of the project. This was done to explain the context and create an overview of the method.

After the introduction of the project the participatory method was explained. The security categories were discussed and the reason for choosing them provided. There was also presented examples to some of the categories. After discussing the security categories the cognitive levels were explained extensively.

Retail and brands has groups with different configuration than the other departments, including team leaders for some employees. Because of this configuration we had a discussion on who should attend the group session. We ended up with the line manager, one team leader and two employees from the department. With this configuration the responsibility for security was fulfilled and we got examples and discussion.

The line manager in retail and brands was positive to the group session. He wanted to have clear examples in the different categories and a description of the model to give to the team leader before the group intervention.

Group intervention trade and brand management

The group intervention with retail and brands was completed on Wednesday 30th of March. In addition to the manager, one team leader and two employees represented retail and brands in the group. The session lasted for 1 hour and 30 minutes and was completed with the modifications from the version used on the employees from operation management. This included fewer questions in the categories and control questions to the measurement of the employees.

The group session started with a presentation of the researcher and a description of the main goals of the project. This was provided to the employees in order to link the group session to the goals of the project. After the introduction the participatory model was presented.

The security categories were described to the employees briefly. The cognitive dimensions of the model were more thoroughly described in order to define the expected levels correctly and create a correct “picture” of the employees retail and brands.

Objective one was started after the explanation of the cognitive levels. This was to define the expected level of the employees in the different categories based on

discussion in the group. The first category was risk management and the group used extra time on examples and explanation of the different cognitive levels related to risk management, in order to learn the model and the process of the following categories. In risk management the group defined the expected level to be level 4 – analysis. The employees presented examples where they often had to use risk assessment in relation to customers.

The following category was security documentation. The employees explained that they knew about the security policy and read it when a new version was released (annually). The group defined that the expected level for the employees should be level 2 – understand, because it was important that the employees understood the principles and responsibilities stated in the policy. The group decided that the employees should be able to use of follow the security handbook. This indicates level 3 and the employees stated that they should not need more knowledge than an average employee.

Security category number 3 is organization of information security. The first question in this category was related to the non-disclosure agreement in Norsk Tipping. Because the employees were handling customers the non-disclosure agreement is an important document for the employees. The group defined that the expected cognitive level for the employees should be level 5 – evaluation. The important concepts of information security were not used by the employees on a daily business, but the groups defined that the employees should understand the different concepts and satisfy level 2 in the model.

In category four, asset management, the first question was about the rules for employees' assets. In retail and brands the employees has stationary computers that is used by different employees. Because of this guideline, the do not need special considerations for handling assets. The group defined expected level to be level 3 – use, where the employees follow the guidelines described in the security handbook. Question two in the category was about classification of information. The employees did not need to classify information often. The group decided that the expected level on classification of information should be level 2; employees should understand the principles of classify information in Norsk Tipping.

Physical security was the next category and the employees did not have special considerations about physical guidelines. The group defined the expected level to be 3; the employees should be able to understand and follow the procedures defined in the security handbook.

Protection against mobile code is the question in communication and operations management category. The employees suggested that they should be able to analyze mobile code and be familiar with the guidelines regarding mobile code. The group decided that the cognitive level 4 – analysis should be appropriate for the employees in trade and brand management.

In category seven, access control, the group defined that the employees should be at level 3 – use when it comes to passwords knowledge. The employees should be able to understand and follow the guidelines presented in the security handbook. When it comes to handling of unattended equipment, the expected level should also be a level 3. This is because there are stationary computers in the work area and the employees are not more exposed to threats than other departments.

The questions asked in the eight security category are about information leakage and social engineering. These concepts are important for the employees in trade and brand management and the group defined the expected level to be level 5 –

evaluation. This was mainly because the employees are often in contact with customers and they handle sensitive information that outsiders often want to get. To avoid being a large risk for Norsk Tipping it is important that the employees can evaluate the situations and incidents that occur and are able to handle these in a secure manner.

Category nine is security incidents. Employees in the department must often deal with incidents, because they are the connection to the customers. They often experience incidents and must be at a high cognitive level. The group defined together that the expected level should be level 5 – evaluation. One employee described an example where he had to evaluate the situation in order to deal with it securely.

The following question was in the business continuity category and the employees suggested that they should be able to follow the business continuity plans that are used in Norsk Tipping. The department did not have any additional continuity plans, but the employees must know there special responsibility if they have any. The group defined that in category ten the expected level should be a level 3 – use.

The final category in the model is compliance towards the security documentation. This category reflects the expected levels above and if the employees have special security considerations that are important. These are the categories where the employees should have a high cognitive level. In this category the group agreed that a level 4 – analysis is the correct level for the department. They should be able to analyze situations that occur and they have areas that are important to the security team.

Objective two in the group session is to define what cognitive level the employees in the department are at. Because the group had used time on examples and discussion in the first phase, the group did not define all the categories in phase two. The group did manage to ask some of the questions and we also touched the objective in phase one when defining the expected level.

In the risk management category the employees suggested that they were on a level 3. Even though they did use risk assessment they wanted more introductions on risk management. In the second category the expected level for the employees was level 2. When asking the control questions, the employees were not able to repeat the policy so on this question they were on a level zero. When it comes to the security handbook, the employees were more familiar with this and were able to describe the procedures documented and they met the expected level which is level 3.

The non-disclosure agreement was a very important document for the employees and was often discussed in the department. The expected level for the employees was level 5 – evaluation. Because this was one of the key documents for the employees, they explained that all of the employees were trained in this evaluation and they meant that they met this requirement. The following question in the category was the important concepts in information security. The employees had some thoughts of the concepts but did not meet the requirement for level 2. This is an area for improvement.

When it comes to the asset management the employees did not have any special requirements or responsibility. The expected level was level 3 for portable assets and level 2 for classification of information. The group agreed that the employees in the department meet the expected cognitive levels. The following categories were defined based on the discussion in phase one and by the researcher and the security team. The reason was lack of time. The answers can

be more unbiased, but after the session the security member and the researcher felt confident to define the actual level of the employees.

Based on the explanations of the employees, the employees met their requirement for physical guidelines. The employees had a stationary environment where the employees rotated. The expected level was defined to be level 3, and the employees met this requirement. In the next category the question was related to mobile code. The group defined the expected level to be level 4, and the employees suggested that they met the requirement. The researcher suggests that mobile code should be involved in an awareness program because the trend shows that this type of attack is increasing.

On access control defined the group that they should follow the guidelines stated in the security handbook. The employees had provided different examples in this category and showed a high level of understanding. The group defined that the employees met the expected cognitive level.

Category eight and nine dealt with information leakage and incident handling. In both categories the expected level of the employees was defined as level 5 – evaluation. These are key features for an employee in the department. In both categories the employees meant that they met the requirements. Inside the department it was focus on security and the employees had extensive training in the different roles in order to perform securely.

In the last two categories the group decided that the expected level on business continuity planning was level 3 and compliance to security documentation was level 4. The employees meant that they met these levels also because they had a security discussion going among the employees and the documented routines that they had. The results are visualized in Table 4. The x represents the expected cognitive level and the star represents the actual cognitive level.

ISO/IEC 27001 – security categories	Questions	1	2	3	4	5	6
A4 – Risk assessment	On what level should employees know risk assessment and risk analysis?			☆	x		
A5 – Security documentation	On what level should employees know the security policy? ☆		x				
	On what level should employees know the security handbook?			x ☆			
A6 – Organization of information security	On what level should employees know the non-disclosure agreement?					x ☆	
	On what level should employees know the core concepts of information security; confidentiality, integrity and availability?		x ☆				
A7 – Asset management	On what level should employees know the guidelines on portable assets?			x ☆			
	On what level should employees know the classification guidelines?		x ☆				
A9 – Physical/environmental security	On what level should employees know the physical guidelines in Norsk Tipping?			x ☆			
A10 – Communication and operation management	On what level should employees know handling and protection against mobile code?			☆	x		
A11 – Access control	On what level should employees know the guidelines for password handling in Norsk Tipping?			x ☆			
	On what level should employees know the handling of unattended equipment and clear desk philosophy?			x ☆			
A12 – Information systems acquisition and maintenance	On what level should employees know social engineering and information leakage?					x ☆	
A13 – Incident management	On what level should employees know the guidelines on incident handling?					x ☆	
A14 - Business continuity management	On what level should employees know the business continuity plans in Norsk Tipping?			x ☆			
A15 – Security documentation compliance	On what level should employees comply with the security documentation in Norsk Tipping?				x ☆		

Table 4 - Results with retail and brands

Evaluation of the group session with retail and brands

The group session with retail and brands was the second implementation of the participatory method. It was the first intervention with the control questions and the facilitator had more experience. The intervention was an improvement from the previous session. The questions in the security categories were better linked to each other and the control questions helped defining the actual level of the employees.

The employees seemed interested and motivated for presenting their experience through examples and situations from the work environment and the manager and the team leader gave the session their viewpoints related to security. After the introduction the employees understood the fictitious model fast and they did not need excessive explanation. The employees where experienced in their job role and was familiar with the guidelines from the security department and their own department.

It was a positive atmosphere in the session and the employees seemed relaxed and eager to talk about security. This made the discussion easier and helped the group to define the expected cognitive level. There were no disagreements between the manager and the employees when defining the levels. This might be that the employees are afraid to disagree with the manager or the manager and the employees have the same view on the different categories.

The improvement action derived from this session is to decrease the time used in phase one, so the group are able to define the actual cognitive levels in all the security categories. In this session the group ran out of time half way into the second phase so this can affect the results.

Meeting with line manager communication and community relations

The third line manager that was introduced for the participatory method was a line manager in the communication and community relations department. The meeting started with an introduction of the researcher and the main goals of the participatory method. The method was described including the security categories and the cognitive levels. The manager was not as familiar with the ISO/IEC standard as the line manager in operation management, so a few examples were provided for describing the categories.

The different cognitive levels were explained in detail to create a solid understanding of the model. When the manager had been explained the model, we discussed the future work and the possible implementation of the method. The manager understood the core elements in the method, to use participation and discussion to improve both the ownership and security awareness among the employees. He expressed excitement to the method and was positive to the following group session.

Group intervention communication and community relations

The group session with the communication and community relations department was the third session with employees. The employees play an important role in handling media. The group session was scheduled to 1 hour and 30 minutes and was based on the same set of categories as the previous session. There were 3 employees present in addition to their line manager.

The session started with an introduction of the researcher and the main goals of the project. An explanation of what had been done prior to the group session was also provided to the employees. This was done to link the group session with the project and to give a solid understanding of the method to the employees.

After the short introduction the participatory method was explained to the group. During the presentation of the security categories, the group discussed the different roles of the employees. Because the employees have several roles it was important to define what role they should be in the intervention. After a short discussion the group agreed that they should include the roles and participate as the employee and the different roles they had. The line manager and the employees were not familiar with the ISO/IEC standard and its content, but they were familiar with the security documentation that was developed in Norsk Tipping.

The cognitive dimension of the model was thoroughly explained including examples, to create a solid understanding. The employees gave the impression that they understood the participatory model and the objectives of the group session.

After the description of the participatory model the first objective of the group session was started. This was to define the expected cognitive level for the employees in the different security categories in the model. The first security category was risk management. The employees have to perform risk assessment on a regular basis. This was a task where the employees had to able to evaluate an incident. One example was that an employee had to know what to say if media wanted a response. If the employees made a wrong decision it could damage the reputation to the company. Both the manager and all the employees agreed that the expected level for risk management should be level 5 – evaluation.

Category two is the security documentation that is provided in Norsk Tipping. The employees suggested that they should be able to understand and explain the important parts of the security policy. Because the policy did not have guidelines or procedures they did not need to be on a level 3. The group defined that level 2 should be the expected level for the employees. Questions two in this category was related to the security handbook. This documentation includes guidelines and procedures that the employees must follow. The employees and the manager suggested that they should be able to evaluate these guidelines and incidents related to the guidelines. Level 5 – evaluation was defined by the group.

In the following category, organization of information security, the first question was towards the non-disclosure agreement. This document is essential to the employees because they have the responsibility for talking with the media and the document provides guidelines for the employees. The group defined that the expected level for employees would be level 6 – make. When it comes to the important concepts in information security the employees suggested that they should be on level 2 – understand. They should be able to understand the concepts, but they did not need any deeper cognitive level for the concepts.

Category four was administration of assets. Because the employees handled sensitive information the group agreed that they should be on level 4 – analysis on handling portable assets. It may also be visitors in the office environment and with sensitive information in circulation it might be a risk for Norsk Tipping. The following question in the category was towards classification of information. In Norsk Tipping they have decided four types of classification based on the sensitivity of the content. The group agreed that the employees should be on a level 5, be able to evaluate and judge a document.

In physical and environmental security the employees suggested that they should follow the security guidelines as a minimum. Because of the amount of sensitive information the group defined that the expected level for an employee

should be level 4 – analyze. In the following category the mobile code is aspect and the employees suggested that they should be able to follow the guidelines provided by the security department. If they followed these guidelines they know how to handle mobile code and are able to reduce the risk of impact. The group defined level 3 as the expected level.

Access control was the following security category and first question was on password handling. The manager suggested that the employees should be on level 3 as a minimum. After a short discussion the group ended up on level 4 – analyze because the employees should be able to analyze their passwords and have a better understanding than many of the employees. Unattended assets and clear desk were also important concepts to the employees. They have many similarities with the previous question and the group defined the same expected level for the employees.

Category nine was addressing social engineering and information leakage. These concepts are crucial for the employees and the group agreed that the expected level was level 6 – make. If an employee did not meet this requirement it could impact the company's reputation or economical loss. In the following category incident handling was the subject and this is a task which affects the employees. This results in an expected level 5 – evaluation for the employees.

Business continuity planning and completion of these are the following category and this is also a task that is important for the employees. If something happens during the lotteries, each employee must be able to deal with the situation. There have been developed guidelines to some situations, but an employee must be able to improvise in some situations. The employees suggested the expected level to be level 5 – evaluation and the rest of the group agreed.

The final category address compliance towards the security documentation developed in Norsk Tipping and can be looked at as a summary of the categories defined earlier. In this category the group defined that the employees should be on level 4 – analyze. The employees have several categories where they have a high cognitive level and this implies that they should be above the average employee when it comes to information security.

After finishing the first phase of the group session phase two was started. Phase two is the evaluation of the employees and to identify potential gaps that can be security risks for Norsk Tipping. This is the phase were the employees has to opportunity to define the actual level of security awareness and security knowledge.

In the first category the group defined that the expected level of the employees should be level 5. This category was targeting risk management and the employees and the manager suggested that they met this requirement. The department has experienced employees and this is a task that is often needed for the employees.

Category number two is the security documentation in Norsk Tipping. The employees defined in objective one that they should understand the principles and responsibilities in the security policy. None of the employees were able to repeat the policy so the actual level of the employees was level 0. The employees admitted that they did not reach the expected level for the security handbook. The expected level on the security handbook was level 5, but the employees suggested that they were on a level 2. They suggested that they needed more awareness on different aspects of security, especially towards e-mail attacks and information leakage.

On the non-disclosure agreement the employees answered that they met the requirement which was level 6. This was one of their main tasks and every employee had to deal with situations that used these guidelines. Because this is one of the crucial documents, the employees had it always in their mind. The second question in the category was based on the important concepts in information security. In phase one the group defined that the employees should understand the concepts and the group agreed that this requirement was met.

In both the question in asset management the employees defined that they did not meet the requirements. The first question were related to the portable assets where the employees agreed that they were to sloppy with the assets and should improve the awareness. When it comes to the classification of the information the group defined that the expected level was level 5. The employees defined their actual level to be level 0. This was because they meant that the classification of information was too difficult and wanted new templates and guidelines for classification. If this is identified as a trend, it should be addressed to the management in order to improve the situation for the employees.

When it comes to the physical security and system administration the expected level defined in the first phase was level 4 and level 3. The employees defined that they met both these requirements. They also mentioned that to address these aspects in a security education could raise the awareness even further.

In the category access control the first question was on password security. The group had defined the expected level to be level 4 – analyze and the employees agreed that they met this requirement. Question two in this category is on unattended equipment and clear desk. The expected level defined in phase one was level four and the employees suggested a level two on the actual cognitive level. They did not meet the requirement and the employees suggested a reminder of these aspects for improved awareness.

The following category addresses social engineering and information leakage. This is two of the most central tasks to the employees and the expected level was defined to be a level 6. The employees presented several examples on situations where they did not meet the requirement. They suggested that they were on level 3 and lacked awareness for the two concepts. Because this is one of the most important tasks this should be improved to avoid possible attacks to important people in Norsk Tipping.

In the category on incident handling the expected level was defined to be level 5. This task was something the employees had to deal with regularly and they explained that they met this requirement. In addition to documented guidelines it was discussed how to deal with incidents between the employees. The group defined that the employees were on level 5.

The business continuity plans was also an important task for the employees. In phase one the group defined the expected level to be level 5. The employees explained that they were on level 1, but they were in the middle of the process of improving this aspect inside this department. The gap will be registered but the improvement process is ongoing and will improve this result.

In the last category the expected cognitive level for the employees was defined as level 4. Despite that the employees had several gaps in the previous categories the group agreed that the employees met this requirement. The results are visualized in Table 5. The x represents the expected cognitive level and the star represents the actual cognitive level.

ISO/IEC 27001 – security categories	Questions	1	2	3	4	5	6
A4 – Risk assessment	On what level should employees know risk assessment and risk analysis?					x ☆	
A5 – Security documentation	On what level should employees know the security policy?		x ☆				
	On what level should employees know the security handbook?		☆			x	
A6 – Organization of information security	On what level should employees know the non-disclosure agreement?						x ☆
	On what level should employees know the core concepts of information security; confidentiality, integrity and availability?		x ☆				
A7 – Asset management	On what level should employees know the guidelines on portable assets?		☆		x		
	On what level should employees know the classification guidelines?		☆			x	
A9 – Physical/environmental security	On what level should employees know the physical guidelines in Norsk Tipping?				x ☆		
A10 – Communication and operation management	On what level should employees know handling and protection against mobile code?			x ☆			
A11 – Access control	On what level should employees know the guidelines for password handling in Norsk Tipping?				x ☆		
	On what level should employees know the handling of unattended equipment and clear desk philosophy?		☆		x		
A12 – Information systems acquisition and maintenance	On what level should employees know social engineering and information leakage?			☆			x
A13 – Incident management	On what level should employees know the guidelines on incident handling?					x ☆	
A14 - Business continuity management	On what level should employees know the business continuity plans in Norsk Tipping?		☆			x	
A15 – Security documentation compliance	On what level should employees comply with the security documentation in Norsk Tipping?				x ☆		

Table 5 - Results communication and community relations

Evaluation of the group session with communication and community relations

The group session with the with communication and community relations was successful. It was three employees together with their manager and each of them was interested in their job role and participated in the discussion with examples from their work environment. The group had discussions on several topics where there was disagreement between the members, but the group did manage to

reach consensus on every question. The employees were able to reflect on their job role and identified different situations that were discussed.

After the explanation of the group used some additional discussion of the first category in order to understand the process and the employees understood the cognitive table quickly. The atmosphere in the group was informal and the impression from the session is that all participants took it seriously and was honest on their own level and skill in the security categories.

The results of the group session were that employees play an important role in Norsk Tipping and need a high cognitive level in order to operate securely in their business environment and towards media and people outside the company. In the session the group identified seven security gaps between the expected and actual level of the employees, with suggestions on how these gaps can be decreased. The session also identified two level six areas and five level 5 areas that should be identified as special considerations and should be taken into account when the security department is defining security education for the employees in the future.

Meeting with line manager projects

The first meeting in the project was a short introduction meeting with the line manager in projects. Project management represents one of the four groups of employees which are attending the test-phase of the participatory method. The meeting was scheduled at March 25th and lasted 15 minutes.

The meeting was opened with a short introduction of the researcher and the background of the project. The main goals of the project were presented together with the participatory method. When presenting the security categories that is derived from the security documentation in Norsk Tipping, the manager questioned the number of categories. He had the impression that it could be too many categories and this might be difficult for the employees to understand. The manager agreed on the reasons for choosing the ISO/IEC standard as the reference document. This is mainly because the standard is based on best practices when it comes to security and the ability to be included in the security education in Norsk Tipping in the future.

Another question that was raised when the security category was discussed was that the manager wanted an explanation on the different categories with examples in the group session. This should be introduced to ensure that the employees understood the meaning of each category and had some references when they should define the security levels. When introducing the cognitive levels of the model, the line manager understood the classification but wanted more examples on the different levels.

After discussing the cognitive levels the goals of the session were presented. This was to prepare the manager for the following group session and give him the opportunity to ask questions about the method. The manager expressed that he was positive to the completion of the method and the method had many similarities with methods that he used in appraisal interviews. He agreed that adjusting the security education, increasing the security awareness and ownership were important actions for improving the overall security in Norsk Tipping.

Group intervention projects

The fourth group session was with projects. This group of employees was chosen because they might have interesting contribution and thoughts related to

security. There were three employees present in addition to their manager and the group session was scheduled to 1 hour and 30 minutes.

The group session started with an introduction of the researcher and the goals of the process. This was done to give the employees an understanding of the participatory method and to place the group intervention into the project. After the introduction of the project, the participatory method was explained. The security categories were briefly explained because they were the core in the rest of the intervention. The cognitive dimension was more explained and discussed in the group to create a solid understanding and to be able to separate the different levels.

After the introduction of the model, the first objective was initiated. This was to define the expected level for the employees in the different security categories. The first security category is risk management. Since this was the first category the group discussed it thoroughly and provided several examples related to the use of risk management in Norsk Tipping. In this category the group also discussed the different cognitive levels and compared the examples provided by the employees to the examples stated in the cognitive table. The group defined that the expected level for employees should be level 5 – evaluation.

In the second category the security documentation in Norsk Tipping is addressed. The first question was addressing the security policy and the group defined that employees should understand the important chapters in the policy and follows the guidelines that are derived from the policy. The expected level was defined as level 3 – use. In the following question the security handbook is addressed and the group defined with help from examples that the expected level should level 4 – analyze.

Category number three addresses the organization of information security and the first question in the category address the non-disclosure agreement. The employees were often in contact with consultants and customer and had to remember the non-disclosure agreement. Because of these relations the group defined that the expected level should be level 4. In the following question the core concepts in information security were discussed. For the employees these terms were defined as crucial. The group defined that the employees should be on level 6, because they created software that is used in the company.

The following category addresses asset management. For handling portable assets the employees suggested that the expected level should be level 4. They often had consultants in their work environment and they also handled some sensitive information, so the employees should be a step above following the security guidelines. The second question in this category addressed the classification of information and the employees did not classify much information. The group defined the expected level to be level 2 – understand. Employees should understand the principles for classification, but did not need more knowledge on the topic.

In the category physical security the group defined the expected level to be level 4. Because their environment often had consultants the employees should be able to analyze their situation regarding the guidelines. The employees should also follow the procedures documented in the security handbook. The following category addresses mobile code. The employees explained that they did not need any additional requirements then the security guidelines documented in the security handbook. They were not more exposed to mobile code than other employees so they suggested level 3. The rest of the group agreed on this suggestion.

Access control is the following security category and the first question address the handling of passwords. The group defined that the employees should be able to analyze their own password. The documentation in the security handbook is short and the group defined that should understand how a good password is created and the value of a solid password. The employees have an open office environment and have occasionally sensitive information on their desks. The security handbook requires that the employees must clear their desk before they leave for the day. The group defined that the employees must be able to follow these guidelines and procedures, so the expected was level 3 – use.

In the next category information leakage and social engineering is addressed. The employees are not as vulnerable for information leakage as the communication or operation management. Even though they do have consultants in their environment, the group defined the expected level to be level 3; following the security guidelines in the security handbook. The following category addresses handling of security incidents. The employees are not a part of the usual detection part of the company. The group therefore defined that the expected level should be level 3 - where they followed the procedures for notifying the correct department.

The final two categories address the business continuity plan and the overall compliance towards the security documentation in Norsk Tipping. The employees did not have any special contingency plans within the department, but they were affected by the overall contingency plans in the company. The group defined that the expected level should be level 3. When it comes to the compliance category the employees suggested that the expected level should be level 4. They had several security categories above the average level in the model. The rest of the group agreed on this suggestion and the first objective of the group intervention was completed.

The second objective in the group session is to define where the employees are on the cognitive scale. This action is important for identifying potential risks for Norsk Tipping and to discuss possible countermeasures to decrease the gap. In the first category, risk management, the group had defined that the expected level was level 5 – evaluate. After a discussion with examples from the employees, the group agreed that they did not meet the requirement. There is not a common vocabulary in the organization when it comes to risk management. The employees defined that they were on a level 4 in this category and wanted a clarification on the different risk concepts. This could also lead to a better understanding for the employees when they worked in project with different departments.

In category number two the security documentation is the concept. When it comes to the security policy, the group defined that the expected level should be level 3 – use, but the employees were not familiar with policy. The actual level of the employees was level 0. This is a gap that the security department should be aware of, but this might not affect the actual security if the employees follow the guidelines in the security handbook. But the policy is the backbone document and the employees have a responsibility to know several sections of the policy. The security handbook is the following question and the group defined that the employees should be able to follow the guidelines and also analyze special considerations that can happen. The group defined that employees meet the requirement of level 4 – analyze.

Organization of information security is the third category and the group defined in phase one that the employees should comply with the non-disclosure agreement and be able to analyze and selecting the important concepts. This was

a document that the employees where familiar with because they used it in their contact with consultants and customers. The employees suggested that they met the requirement of level 4 because the usage of the document. The next question in this category relates to the core principles of information security. The group defined in phase one that the expected level was level 6, but the employees suggested that they were on a level 3. The employees point out that there is a lack of formality in the documentation for the employees. They might also need more awareness on these concepts to increase their understanding.

In the category handling of assets the group defined that the expected level for the employees to be level 4. The employees worked in an environment where consultants may appear and they were familiar with the guidelines. The group defined that the employees meet the requirement on portable assets. Classification of information was the next question and this was not a task that the employees needed to do often. In phase one the group defined that the expected level was level 2 and the group defined that the employees met this requirement.

The physical security requirement for the employees was defined at level 4 – analyze in objective one. This was chosen because the aspect of consultants in the work environment. The employees suggested that they met this requirement. In the following category the mobile code was addressed. The expected level of the employees was level 3 – that they followed the guidelines in the security handbook. After a short discussion the group defined that the employees were satisfying the requirement set in objective one.

The first question in category seven is addressing passwords. In the first phase of intervention the group defined that the employees should be on a level 4 – that they should be able to analyze their own passwords and create safe passwords. The group defined that the employees met this requirement after the security department has used resources on the aspect in the security education. When it comes to clear desk and unattended equipment, the group defined the expected level to be level 3. The group agreed that the employees meet this requirement and complied with the security handbook.

In category on social engineering and information leakage the next gap was identified. The group had defined the expected level to be level 3, because the employees were not a primary channel to the outside world, but because of lack of awareness the actual level of the employees were defined as level 2. The employees are not one of the main channels for reporting security incidents. In phase one the group defined that the expected level was level 3 – use, and the group agreed that the employees meet this requirement and were able to follow the guidelines in the security handbook.

When it comes to business continuity planning the expected level for the employees was defined to be level 3. They suggested that they met this requirement because they were familiar with the documented plans and did not have any additional guidelines. The group agreed that they met the expectations. In the last security category the compliance towards the security documentation is addressed. This category is also related to the previous categories in the model. The expected level was defined as level 4, because in some of the categories the employees was high on the scale (above level 3) and the group agreed that the employees met this requirement despite the gaps identified. The results are visualized in Table 6. The x represents the expected cognitive level and the star represents the actual cognitive level.

ISO/IEC 27001 – security categories	Questions	1	2	3	4	5	6
A4 – Risk assessment	On what level should employees know risk assessment and risk analysis?				☆	x	
A5 – Security documentation	On what level should employees know the security policy?		☆	x			
	On what level should employees know the security handbook?				x ☆		
A6 – Organization of information security	On what level should employees know the non-disclosure agreement?				x ☆		
	On what level should employees know the core concepts of information security; confidentiality, integrity and availability?			☆			x
A7 – Asset management	On what level should employees know the guidelines on portable assets?				x ☆		
	On what level should employees know the classification guidelines?		☆	x			
A9 – Physical/environmental security	On what level should employees know the physical guidelines in Norsk Tipping?				x ☆		
A10 – Communication and operation management	On what level should employees know handling and protection against mobile code?			x ☆			
A11 – Access control	On what level should employees know the guidelines for password handling in Norsk Tipping?				x ☆		
	On what level should employees know the handling of unattended equipment and clear desk philosophy?			x ☆			
A12 – Information systems acquisition and maintenance	On what level should employees know social engineering and information leakage?		☆	x			
A13 – Incident management	On what level should employees know the guidelines on incident handling?			x ☆			
A14 - Business continuity management	On what level should employees know the business continuity plans in Norsk Tipping?			x ☆			
A15 – Security documentation compliance	On what level should employees comply with the security documentation in Norsk Tipping?				x ☆		

Table 6 - Results projects

Evaluation of the group session with projects

The group session with projects was the fourth session with employees. In the group session four gaps were identified and the trend showed that the employees were above average in seven of the security categories. This can imply that all departments can have special considerations that are important to identify to improve the security education.

The group had extensive discussions in the first categories in order to understand the difference between the different cognitive levels in the model. There was initial disagreement on the placement in the model but with discussion and examples of situations the group did manage to agree on in the different security categories. The employees were active and provided examples when necessary.

Results of the chapter:

- Completed four meetings with line managers from the different departments
- Completed five group interventions with employees
- Identified eleven potential risks in the different interventions

6 Results

Content of the chapter:

- Documentation of the qualitative interviews
- Documentation of the interview with the security department
- Analysis of the results in the interviews
- Analysis in P'HAPI

The method that was chosen for evaluating the participatory method was qualitative interviews. This was chosen because the method is based on that the employees participate in the measuring of them and also participate in defining what to measure. When choosing such a method, a pre-/post-test option is not functional. The evaluation is based on 14 interviews with the participants in Norsk Tipping. The answers are categorized if possible and when there are differences in the answering, it is described below. The answers that have similar meaning are emphasized in order to identify trends among the participants.

6.1 Framework for the qualitative interview

The qualitative interview was chosen as the preferred method for evaluating the group interventions. In order to secure that the interviews satisfy the demands of research and to get the correct results, a framework was chosen. This framework was based on suggestions made by Kvale and Brinkmann [31]. Since the test phase of the project included four different groups of employees, two business-critical and two non-critical groups, the decision of interviewing all the participants was made. This resulted in 14 interviews with the employees who participated in the interventions, both managers and regular employees.

Kvale presents several quality criteria for an interview. Three of the most important criteria are (1) that the interview is interpreted while it is ongoing, (2) the interviewer verifies his own interpretations throughout the interview and (3) that the interview is "self-communicated", it does not need additional comments or explanations [31]. These three criteria were used as a foundation of the interviews.

The interview was based on a structured approach with eight questions, but without strict limits and where the participants had opportunity to give explanations in each answer. The researcher had also opportunity to ask control questions or for more explanation to the different answers. Because the interviewer was familiar with the participants, a friendly tone was chosen so the participants were comfortable and able to give honest answers on the questions. All the interviews were started with a short explanation of the setting and the main goals of the interview. Since all the employees had been participating in sessions prior to the interview, they were familiar with the educational method and the group intervention.

There were two main goals of the interview. The first goal was to evaluate the participatory method from the employees' view. This is related to the hypothesis and the research questions and is the method used to evaluate the participatory method itself. In addition to the questions based on the first goal, there are also questions related to the completion of the group intervention itself. These questions are used to ensure that the group intervention followed the principles from action research and they help to support the questions related to the first goal. The questions to the two main goals are mixed in order to identify inconsistencies in answers provided by the employees. The eight questions are described below.

1) How did you experience the process in the group intervention?

The first question targeted the group intervention. This was an open question for the participants used to help them remember the group intervention and how it elapsed. In addition the question revealed if the participants got an understanding of the main goals of the intervention and if the model was too difficult for the employees. When interviewing the managers the first short introduction meeting was included in this question.

2) What do you think of being able to shape your own security education?

This second question aims towards the main goal of the project. The question is used to investigate what the participants think about adjusted security education and also to get an impression on if the participants think the group intervention was a positive method. Since most of the education in Norsk Tipping has been to a general audience, the employees related adjusted education to the group intervention.

3) Have you become more engaged in security after the group intervention?

The third question is closely related to the first research question. This question identifies if the employees feel an improvement of their awareness or ownership towards security by participating in the group intervention. This is the impression that the employees have after the intervention.

4) Do you feel that your viewpoints were considered and affected the results in the group intervention?

Question number 4 is related to the facilitator role of the researcher. The facilitator has the responsibility to include all the participants in the discussion and that no one feel afraid to contribute. This is one of the important aspects of action research where all the participants are able to share examples and situations with the group.

5) Do you think a method based on adjusted security education can improve the security awareness and security ownership among the employees?

This question is closely related to the second research question. In this question the employees evaluate the method in relation to security education and also give feedback on what they thought of the method. The employees also evaluate if adjusted security education can improve the security awareness and ownership of the participants. This is an open question where the employees can give an extensive explanation of the method.

6) Did you get new knowledge about security related to your job role in Norsk Tipping?

This question is closely related to question 3 but also include if new knowledge was identified in the group intervention by the participants. This is one of the main goals of a session based on action research and it is important to identify if the group intervention actually improved knowledge by discussion situations and examples in the group.

7) Is there anything that should have been done differently or was missing in the group session?

This question was used as an evaluation of the group session. This was an open question where the employees were able to evaluate the possible shortcomings of the group intervention and identify possible improvements for developing the method further.

8) Do you think a method based on adjustable security education should be implemented in Norsk Tipping?

This last question address if the employees found this method positive and interesting. The employees have the opportunity to explain why or why not they think that the participatory method should be introduced to the remaining departments in Norsk Tipping. In addition they can also explain what to include in the sessions in order to get the best outcome of the interventions.

6.2 Interview with participants

1) How did you experience the process in the group intervention?
The trend in the answers provided by the participants was that the fictitious model, with the security categories and the cognitive dimension, was easy to understand and intuitive. This made it easy to understand the different phases in the group intervention when defining both the expected and actual cognitive level. The employees did not have any knowledge about the intervention prior to the group meeting and it was vital that the model was easy to understand. Most of the employees were positive to the process and agreed that the model was easy to understand.

Despite that most of the employees had positive experiences there was also identified areas of improvement. A couple of employees answered that there had been problems with understanding the differences between the cognitive layers and because of that used much time to explain and decide the different levels. This made the intervention more difficult and affected the outcome of the intervention. There was also one employee that explained difficulties in separating the expected level and the actual cognitive level in the intervention. This resulted in discussions and explanations and made the intervention more complex. In addition one manager had difficulties with expectations to himself and the employees, who had the responsibility for defining the levels in the group intervention, but this issue was resolved in the beginning of the group intervention by discussion.

Analysis: The evaluation by the participants show that an extensive part of the employees found the group intervention positive, tidy and intuitive. Most of the employees described that the description of the model was functional and the model itself was easy to understand. This result was also identified during the interventions, when the employees showed understanding and came with suggestions on the levels and situations from their job role. In addition to the positive feedback, some employees meant that the model needed some explanation and the cognitive levels were difficult to define. The trend in these answers is that the participatory model was intuitive and easy to understand, but

it is important to clarify the different cognitive levels and use more time and explanation on the first categories in phase one in order to teach the employees the model. This will improve the outcome of the intervention and might improve the awareness and ownership to the participants.

2) What do you think of being able to shape your own security education?

The results from this question are positive. The participants find a method where they are active and can provide their own examples to be a better for improving security awareness. By discussing security terms that is familiar to the employees, they explain that the content was more understandable and the outcome was better. In addition employees explain by discussing the different security categories they also improved awareness on the different sections. It was also positive that the security department could share their experiences to the group in order to be a part of the discussion. Several participants explained that this method should be used on all of the employees in Norsk Tipping, because they learned security that was important for their job role. One employee explained that this method was more relevant because the security handbook was guidelines that were too general and therefore not as important for him. By participating in the security discussion the employees can address what is important for them in their daily work and thereby improve the most important categories. The departmental differences should also be included in future security education. One employee suggested that interventions could be used as reminders in the future to maintain or improve the security awareness.

Analysis: All the employees were positive to participate in their security education. The fact that the content became more understandable and the ability to discuss security with the security department were positive actions described by the employees. The possibility to relate the security discussion to situations from their daily job was also a positive effect with the method. The results show that the employees that participated in the group intervention had a positive impression by the group interventions and the possibility to discuss situations with the security department. They liked the idea with including the employees on a larger scale in the education.

3) Have you become more engaged in security after the group intervention?

This question was used to evaluate if the group intervention had an effect on the participants. This question will not identify if the group intervention had an actual effect, but if the participants believe that they focus more on security or think more on security after the session. The results on this question can be divided into two groups. The first group is the employees that explain that the group intervention had improved the security awareness. This was either related to an example or a topic that was discussed in the group intervention, or that the session was positive and made the employees more interested. Several employees also explain that they have improved their knowledge in categories where the group identified gaps in the group intervention. This can imply that the employees are interested in security and eager to improve their own awareness and knowledge in the different categories.

The other group of employees was the ones that did not feel more engaged after the session. Several of the employees explained that they had several years of experience and was familiar the security issues that were discussed in the session. They meant that the session could improve the awareness on different security aspects as a reminder, but they did not feel more engaged. In addition there were employees that have had a security session prior to the group

intervention, so they explained that this might have an impact on the outcome of the intervention.

Analysis: The participants were divided into two groups. One group of the employees had improved their engagement towards security by participating in the group intervention. They explained that by discussing relevant situations from their daily jobs, the content was more interesting for them and by that had improved awareness. There were examples where the group had discussed situations that happened between the intervention and the interview, where employees had used the knowledge from the intervention to solve the incident. The other group of employees explained that the group intervention did not increase the engagement. There were different reasons why intervention did not improve the engagement, with recently security education in the department and a high personnel interest in security as reasons. Despite that the employees was not more engaged, they did find the intervention informative and helpful to keep interest in security.

4) Do you feel that your viewpoints were considered and affected the results in the group intervention?

This question was used to identify if the participants felt that they was neglected in the intervention and did not participate because they did not feel comfortable. This is one of the main tasks for the facilitator and this could impact the discussion in the group and thereby impact the results of the overall intervention. It is therefore important to identify if the participants were uncomfortable under the intervention. All the participants stated that they did not feel uncomfortable or neglected in the session. They explained that they could bring up examples for discussion and it was a positive tone in the group intervention. Several of the employees explained that they are positive to discuss security in groups with colleagues.

Analysis: All of the employees explained that they were comfortable in the group interventions and that they felt as a contributor to the group. By including several employees in a group and arrange for discussion, different meanings can surface and improve the co-generation of knowledge. It is important for the evaluation of the model that the employees feel that they are important in the group intervention in order to improve the outcome of the interventions. The completion of the interventions shows that there is a functional security culture in Norsk Tipping. Without this security culture, the intervention could be more difficult to achieve.

5) Do you think a method based on adjusted security education can improve the security awareness and security ownership among the employees?

This question is closely related to the second research question. In order to answer this research question the employees evaluate the method that is used throughout the project. All of the employees answered that they were positive to target the security education to the different departments and job roles. This can increase the understanding of the content, make the content more interesting, and by that improve both the awareness and the ownership towards security. Suggestions that came from the employees were that the interventions should be done to all of the employees, where the results could be compared, and that the method should include follow-ups in reasonable time to maximize the outcome and preservation of knowledge. Some of the employees mentioned that the security handbook included guidelines that were to general and that this affected the curiosity of the employees. One employee explained that the principle of subsidiary was important in security education. When the employees were able to actively participate in the education they could also improve the ownership.

Analysis: The results from the interviews showed that all of the participants were positive to the method introduced in the group interventions. The advantages described by the employees are that the content is more understandable, it is more interesting when they participate in the education themselves, the education can be more targeted in the future and have a better effect than general education. Several mentioned that they believed more on dialogue than on one-way communication in security education. Employees described that the participatory method could be adjusted to different roles for the employees and not only towards security. The cognitive levels and the definition of expected and actual level can be retained and other categories can be included.

6) Did you get new knowledge about security related to your job role in Norsk Tipping?

In the answers provided by the employees there were two trends. One was the employees that did not get new knowledge by participating on the group intervention. There were several reasons for not improving the knowledge with experience in the job role, internal security education prior to the intervention and some of the employees did not remember getting new knowledge. This could be dependent on the group intervention and how this was completed.

The second group of answers was from the employees that gained new knowledge by participating on the group interventions. Several employees explained that the categories addressed security areas that surrounded the core elements of their job role and was important for the employees. Employees explained that the knowledge on the relation between the job role and security was improved by seeing the "whole" picture by the security categories.

Analysis: The answers were divided into two groups. One group of the employees answered that they did not get new knowledge from participating on the group interventions while some of the employees described an increase in knowledge by participating. The possible increase in knowledge is not measured, but the answers may be the results of a positive intervention for the employees. It is not likely that all the participants will gain new knowledge because it is individual preferences in the group. Some of the members can be experienced and comfortable in discussing in groups, while others can find this difficult. But the positive answers can be an implication where the participants find the method interesting and that the group intervention addressed security issues that was new to some of the employees.

7) Is there anything that should have been done differently or was missing in the group intervention?

This question was asked to identify possible modifications to improve the outcome of the session. Several participants suggested that it should be handed out information prior to the group intervention, so the participants had the opportunity to prepare themselves. This was only done with the introduction meetings with the managers. Other participants explained that because the participatory model was easy to understand they did not need information prior to the intervention, the participants were divided into two groups. One of the employees suggested including the security handbook in the intervention and using this as a basis for the discussion. Another employee explained that the model had too much security categories and this should be improved in order to avoid rushing at the end of the intervention.

Analysis: There were two main trends in the answers where one trend was that participants wanted information before the intervention in order to prepare themselves. The other trend was the employees that did not identify particular

improvements before the interventions. The choice of only preparing the managers was made to avoid that the participants could discuss situations before the group session. By helping the employees in the session to explain situations and examples from their daily job, the researcher hoped to get a better discussion and outcome of the group intervention. If employees could discuss the situations prior to the intervention this might affect the discussion phase of the intervention. It is positive that many of the participants found the model intuitive and that they did not need information before the session. One employee also mentioned that an additional group of employees should complete the intervention and the results from the two interventions compared, in order to get a more satisfactory result. This will demand much resources of the security department.

8) Do you think a method based on adjustable security education should be implemented in Norsk Tipping?
This last question in the interview is used to identify if the participants find this method positive and if they recommend this as an additional method for security education in Norsk Tipping. The trend shows that all of the employees find this method positive and think that it should be adopted by the security team. They base their conclusions on the understanding of content, better adjusted to the employees, opportunity for dialogue and not only education by professionals and that it was an exciting method. One employee explained that this method should be used to improve the principle of subsidiary in relation to security. By keeping the general security education and use this method to improve specific security issues for the employees.

Analysis: The employees were positive to the method used in the group intervention. Both the managers and the employees explained that the method was educational, interesting, smart and easy to understand. Methods based on small group interventions have been tested in other companies and positive results have been made. The participatory method included security categories from the ISO/IEC 27001 and a cognitive dimension from Bloom. This was used to increase the functionality and duration of the model.

Despite that this is only an evaluation provided by the employees it is important results that they find the method interesting and that the employees explain that it improves the awareness. They explain that the method was positive because they were included in the education and had the opportunity to influence the intervention.

6.3 Framework for interview with the security department

In addition to the qualitative interview with the participants an interview with the security department was also conducted for evaluating the method and the interventions from their point of view. The interview has some similar questions to the interview with the participants, but it is also modified for evaluating the method. The security department has experts on security and might have different experiences on the method and the group interventions. Since the security department is defined as the problem owner in this project, it is important that they also evaluate the participatory method. The questions are described below.

1) How did you experience the process from the start-up to today's situation?

In this question the security department evaluates the progress from the early meetings to the situation after the group interventions with the employees and their evaluation of the method. This is an open question where the security officer has an opportunity to share his thoughts on how the design and implementation phase has been.

2) Can the security department learn from the group interventions? If yes, what can it learn?

This second question is used as an evaluation on the different group interventions and if the security department has identified positive effects by completing the interventions. The security department has participated in the design phase of the method and has deep knowledge before the implementation of the group interventions.

3) Are there advantages by adjusting the security education to the employees? If yes, which are the biggest advantages?

The third questions address the advantages that the security department has identified by completing the group interventions and adjustable education in general. Norsk Tipping has used a method related to classroom education and wanted to test a different approach for the annual security education. The question is structured for identifying possible advantages and to explain how they can have a positive effect on the employees.

4) Are there disadvantages by adjusting the security education to the employees? If yes, which are the biggest disadvantages?

Question four addresses the disadvantages of adjustable education. The reason for choosing to identify the disadvantages is to determine whether such a method is possible to use in a large organization and to evaluate if the method has elements that must be identified in order to have a successful method.

5) Is there anything that should have been done differently in the group session?

This question addresses how the security department evaluated the group interventions and if the method should have been modified in order to improve the result. There can be issues that are not included in the method because this is a proof of concept and the method with security categories and a cognitive dimension is not used extensively in security education.

6) Which experiences has the security department after the completion of the group interventions?

Question six evaluates the participatory method and the group interventions. This evaluation is used to identify the trends revealed in the group interventions and also the impressions of the employees that have participated in the test phase. The question is open in order to include the different results and what the security department has experienced with this method.

7) Do you think a method based on adjusted security education can improve the security awareness and security ownership among the employees?

This question is the same as question five in the interview with the participants. It is asked to the security department to identify if they believe in the method from a security perspective. The evaluation of the method is provided by the participants in the group sessions and an expert evaluation provided by the security department.

8) Do you think a method based on adjustable security education should be implemented in Norsk Tipping?

The last question in the interview with the security department addresses their thoughts on including the participatory method as a method for improving the security education in Norsk Tipping. It is important to identify if the security department will adopt this method and if they will use the model in the future.

6.4 Interview with security department

In addition to the evaluation of the participants in the group interventions a member of the security department was interviewed. This interview was made to identify the viewpoints from the security department on the design of the participatory method, completion of the meetings with the managers and the group interventions with the employees. This interview is modified from the interview to the participants. It is an evaluation of the project process and is based on a security perspective. The evaluation is done by a member of the security department so the answers are documented with an analysis at the end of the section.

1) How did you experience the process from the start-up to today's situation?
This question is used to as an evaluation of the entire project, from the initial meeting to the qualitative interviews with the participants in the interventions. The security expert states that he is pleased with the progress. After creating the project plan for the participatory method, the progression has been on track. A risk analysis was made in the project plan and the potential risks have been decreased in several revisions throughout the project.

2) Can the security department learn from the group interventions? If yes, what can it learn?
The security expert believes that the security department can learn several things from the interventions. The security department gets feedback from departments on where the employees are in the different security categories, the status for the department and what level they want to achieve. The security department also gets an interaction with the participants and this is an ideal method for teaching security, with small groups and the ability to talk to the employees. This is a good method for defining what the security department wants to include in the security education and for the participants to share their feelings on different categories.

3) Are there advantages by adjusting the security education to the employees? If yes, which are the biggest advantages?
The biggest advantages are the utilization of the resources for the security department and that we are able to cover the security requirements in the different departments. In addition we are able to prioritize the important issues for the employees and can use a more risk-based educational method. The employees that have critical roles in Norsk Tipping can be educated and prioritized where the risks are most critical. We have also the opportunity to use larger group of employees on the more basic educational issues.

4) Are there disadvantages by adjusting the security education to the employees? If yes, which are the biggest disadvantages?
This method requires more resources from the security department when it comes to the planning phase. When we take over the method it will demand resources to get a functional method and adjust this to Norsk Tipping. But we use time on the annual security education and if we use that time on this method it can be beneficial for the company. There are also challenges related to communication of the new method that must be addressed to the organization in the right way.

5) Is there anything that should have been done differently in the group session?
Gaining experience improves the results and was visualized throughout the interventions. We did improve the interventions by adding control questions and learned from that experience. The participants gave positive feedback and one of the main goals where that the session was used to improve awareness in addition to define the cognitive levels. I think that we have chosen a correct approach and we learned how to ask the control questions in order to define the levels. We also got honest answers from the participants

6) Which experiences has the security department after the completion of the group interventions?
The group interventions identified areas where the security department has to invest resources in order to improve the situation. Especially the security policy and what is important for the employees when it comes to security education. We are also back at the core elements of why doing security education. It is important that we learn how the employees experience the security education.

7) Do you think a method based on adjusted security education can improve the security awareness and security ownership among the employees?
I am 100 percent certain that adjustable security education can improve both the security awareness and ownership. With adjustable education we are able to decompose the education to where it is most important and the security department will also get a better understanding of the requirements for education in the different departments in Norsk Tipping. The security department has been thinking of such a method, but has not had the resources to start the process. It was luck that the schedule fitted like it did because it requires resources to design such a method and complete the test phase.

8) Do you think a method based on adjustable security education should be implemented in Norsk Tipping?
It is determined that the method will be adopted by the security department. The uncertainty lies in how the method is adopted based on your report and assessments on how to implement this method. We will then improve the method and adjust it to fit the organization. So in the autumn we must continue this process and use your work for implementing the method.

Analysis: The interview with the security department was used to identify the experiences from a security The interview addressed both the project process and evaluated the participatory method and the group interventions. The overall impression is that the security department is satisfied with project and how this was carried out. It has been a close relationship between the researcher and the security department in order to develop a method that can be adopted in the organization and used in the future.

The impression made by the security expert was that the security department was satisfied with the design of the method. The security categories were adopted by the ISO/IEC 27001 to increase the operating time of the method. In addition the security expert was satisfied with the experiences from the group intervention, where challenges were identified and the security department learned more about the individual adaption in the different departments. Overall the security department is pleased with the outcome and that is showed by the decision of adopting the method after the summer.

Results of the chapter:

- The qualitative interviews revealed positive feedback from the participants
- Several employees explained that the content was much easier to understand
- The method was intuitive, smart and easy to use
- Employees explained that they had learned new security aspects
- The supervisor from the security department was satisfied with the method
- The method will be modified and adopted by the security department this autumn

7 Discussion and conclusion

Content of the chapter:

- Discussion and conclusion of the project
- Policy in P'HAPI

In this chapter the entire process in the project is evaluated. This includes phase one that was the literature study and the documentation of Norsk Tipping, the second phase that was the design of participatory method, the third phase that was the test phase and the final phase that included the evaluation of the method.

The first phase was used to investigate the organizational structure of Norsk Tipping. This was done to understand how the organization worked and also identify the security documentation and how security education had been done in the previous years. This was completed with guidance from the security department who provided the documentation.

The project aimed at designing an additional method for security awareness training for the use in Norsk Tipping. The guidelines from the security department were that the method should be different from the annual security training by the employees. This had been completed with a classroom-education with large groups of employees, so the security department wanted more active employees in the education. After reviewing the literature the hypothesis and research questions were defined. The main hypothesis for this project is that a method based on action research can improve security awareness amongst the employees. In order to investigate if that is correct three research questions were defined. They are discussed below.

Can a method based on principles from action research increase the knowledge and understanding of security to the employees in Norsk Tipping? Security awareness is composed of different concepts. In order to be a security aware employee, the employee must have a level of knowledge, understand why this knowledge is important and be able to see the large security picture. Why is security important? The literature review identified methods that were suitable to Norsk Tipping's demands. Methods based on principles from action research had provided results in similar research so it was a possibility for improving the knowledge and understanding of the employees. The evaluation done by the employees identified that several employees felt an increase in knowledge towards security by participating. This has not been measured because of lack of time and resources and the completion of the method, so there are no results that show actual improvement of the employees. Despite this fact it is an important indication that employees explain that the group discussed topics in the group intervention that "open the eyes" to the employees.

Several of the employees also explained that the content of the group intervention was easier to understand because they were able to provide examples and situations from their own job role. When discussing the different security categories the employees had the opportunity to relate the categories to their environment and this could improve the understanding for the employees. Because the evaluation of the group interventions were interviews the actual

improvement of understanding security is not measured. This functionality is part of the future work of the method that should be implemented in order to improve the method. Based on the results the actual improvement in knowledge and behavior is not measured, but there are indications that some employees have improved their knowledge towards security.

Did the employees find this method positive and effective for improving information security awareness and compliance? Important criterions for a successful educational method are that the method is positive and interesting for the participants. If the employees dislike the way of educating security it is difficult to improve their security awareness. The evaluation of the group interventions revealed that all of the participants found the method positive. They explained that the method was intuitive and by building the intervention on discussion the employees were able to address their own meanings on security. This made the content more understandable and the intervention more interesting. *What do they think of the process of the education and did the method improve their ownership towards security?* The employees were positive to the setting of the awareness training. One of the key concepts of the participatory method was that by including the employees in the education, the ownership towards security could be improved. This was realized by defining the expected and actual cognitive level in the interventions. When defining these levels the employees identifies that there are gaps that should be decreased and also suggests countermeasure. When the employees are able to perform this evaluation in the group intervention, it shows that the security culture in Norsk Tipping is in place and that the employees are able to evaluate their own job role. It is important for this thesis that there is a security culture and that the employees are aware of their responsibility for meeting the security guidelines. Without this security culture the discussion in the group intervention would be more difficult and the outcome of the session could be of lower quality. Because this security culture, the communication in all of the interventions were good and we were able to create a positive atmosphere during the test phase of the method.

Can a participatory method based on principles from action research improve the security team's knowledge of specific security aspects for the employees? One of the concepts that were discussed during the design of the participatory method was the ability for the security department to gain valuable knowledge from the group interventions. Since the action research in this case is based on small group interventions where the participants are defined as experts on their own role, the security department should be able to improve their knowledge on the different job roles in the company. The evaluation with the security department identified that they did get new information about the different departments. When defining the expected and actual level of the employees the group also identified special security considerations of the job role. The categories where the group defined the expected level to be level 5 or level 6 was determined to be special security considerations. These were the most important categories for the employees and they should be emphasized in future security education of the employees. In the four group interventions twenty categories were defined as special considerations. In addition to the security considerations the security department can also learn from the situations and examples provided by the employees. The employees in Norsk Tipping are eager to explain situations regarding the security categories and the security department should pay attention to these explanations. The employees can explain concepts that make their job more difficult and it is important that the security department help the employees from a security point of view. *Does the security team find this process effective and can it be used in the future?* The security team is satisfied with the design and implementation of the participatory method. They

were active in the design phase in order to provide their thoughts on how the method should be designed to fit the organization and their requirements. The in house supervisor attended all of the group interventions and was the representative from the security department. He participated in the group interventions when necessary and was following the entire project process. The evaluation of the interventions shows that the security department wants to adjust this method and include it in their security training of the employees. Based on the evaluation and respond from the participants the security department wants to use this type of education and improve the participatory method to improve the outcome of the awareness training.

Despite that the evaluation and the feedback from the participants were positive the participatory method did not include a measurement of the outcome of the interventions. Because the employees participated in the definition of the expected and actual cognitive levels, it was not possible to use a pretest/posttest design for measuring the actual impact of the interventions. Since the definitions were made in the actual implementation phase the pretest and the posttest would include different content and the data could not be sufficient. In addition the lack of time and resources made it difficult to complete this measurement. The measurement of the method is a crucial part of it functionality. It is therefore important that this is included in the future for evaluating the employees in Norsk Tipping. The first round of the interventions can be the identification and definitions of the cognitive levels that is the basis for the measurement on a later stage. The expected levels that are defined in the group intervention are the content that should be measured in the future. If the measuring show gaps from the expected levels, countermeasures should be implemented to improve the situation.

The project resulted in an intuitive, interesting and functional method that has co-generation and discussion as main features for improving the security awareness. The security department improved their knowledge to the different roles in the organization and should use the results to adjust the security education in the future. The method was designed based on research literature and guidelines from the security department in order to be functional. The method was tested with four group interventions with employees where the group discussed eleven security categories adopted from the ISO/IEC 27001 standard. After this test phase 15 qualitative interviews were conducted to evaluate the effect of the participatory method. It is important to remember that four departments were chosen for the test phase and that the results from the interventions may not be a correct picture of the situation in Norsk Tipping.

Results of the chapter:

- The qualitative interviews indicate that the participants find the method intuitive and interesting
- Several employees explain that the content was more understandable
- All group interventions revealed special security considerations
- The security department is satisfied with the method and will develop this further in the future

8 Future work

Content of the chapter:

- Nine recommendations to develop the method further
- Implementation in P'HAPI

In this chapter the recommendations for improving the participatory method is described. These recommendations are based on the results from the group interventions, the interview with the participants and the shortcomings of the method. The shortcomings are related to measurement of the cognitive dimensions where the participants defined themselves with help from the security department. This action does not measure the actual behavior and awareness of the employees, so in the future measurement of the actual cognitive method should be introduced. The following recommendations are based on the results from the group interventions and qualitative interviews so this might affect the outcome of the recommendations.

1) Review the security categories and cognitive classification

Based on the completion of the method the researcher recommends that the security department evaluates the eleven security categories that were used in the group interventions. It may be important categories that have been left out of the method and it can be categories that should be merged or modified in order to reach all of the employees in Norsk Tipping. The fifteen questions that were used to address different categories in the group interventions should also be revised. They follow the same template and there might have been important aspects that have been left out of the session. The security department has created the security documentation so they should define the best suitable questions. One example of a modification is to exclude the last category. This was difficult to decide in the interventions because it is not directed to the security documentation. In addition should question number six and question number eleven be merged because they address similar aspects.

Another action that the researcher recommends is to evaluate the use of Bloom's taxonomy. During the group interventions there were difficulties when separating the different cognitive levels. There can be a similar classification in use in other education in Norsk Tipping, so the security department should decide on what classification that should be used in the organization. The researcher suggests that it is used one cognitive classification in different types of education throughout the organization. It is advantages and disadvantages with Bloom's taxonomy, but creating clear distinctions between the cognitive levels should improve the use of the taxonomy and make a functional classification. This should be possible to export to other educational purposes in Norsk Tipping. It is important that the security categories and cognitive classification is adjusted to the organization before the second recommendation is initiated.

2) Complete group interventions with each department/important job role

To complete the group interventions with all the departments in Norsk Tipping is the second recommendation. The reason for include all departments in the

organization is to identify possible trends among the employees and improve knowledge to the different departments in the security department. Group interventions can be used to improve the security awareness and ownership, but also to identify the special security considerations in the different departments. If the group intervention is completed throughout the organization, the security department will have a more accurate picture of the organization and the risks it faces. The researcher recommends that one unit from each department is a minimum of employees. The security department should also complete group interventions with units that have an important or special responsibility in the organization.

By completing the group interventions with the different units the security department should improve their knowledge to the different job roles in Norsk Tipping. In addition the data collected in the intervention will be more accurate. The completion may also identify new or reinforce the identified trends from the project that should be used as a foundation for future security education in Norsk Tipping.

3) Improving the awareness to the security policy among the employees

One of the trends that were identified in the four group interventions was the lack of knowledge towards the security policy in Norsk Tipping. This is the steering document and includes the security goals and the responsibilities for the employees in Norsk Tipping. The interventions revealed that employees did not know the overall security policy document, but were familiar with the security handbook that includes security guidelines. To improve ownership and awareness it is important that the employees are familiar to the core concepts of the security documentation. If they only rely on the guidelines and do not know why these guidelines are defined, it could impact the understanding. There are several methods to improve the awareness to the policy.

One option is to make the policy to a more living document. This can be to address the policy in the security education and it can be distributed regularly to the employees, maybe in a readable version that is easy to understand. To link the education to the overall security goals of the organization and include the responsibilities more actively can also improve the awareness among the employees. Despite that it was identified a gap in the knowledge to the policy the employees were more familiar with the security handbook. This addresses the security guidelines and is more directed to the employees.

Another option is to create a new security policy. The challenge with a security policy is that it has to include the general level of security and can be more difficult to understand for the employees. If the security team decides to create a new policy, it should be addressed more regularly to the employees. It is important that the employees are familiar with the core concepts of security in Norsk Tipping.

4) Improving risk assessment and risk management in the organization

Another gap identified in the group interventions were in the first category, risk assessment. This is one of the categories from the ISO/IEC 27001 standard and in 3 of the interventions a gap was identified. The explanation on the gap is regarding the use of different terms and understanding of a risk assessment. This is an activity that is often used in projects and many of the employees must perform risk assessment weekly. The recommendation is to define a standard, or set of terms that is used throughout the company in order to improve the understanding of the process. This should help the employees when dealing with

risk in project or if they must define the risk in an incident. The security department should review/modify the templates for accomplish a risk assessment and include this in the security education in the organization.

5) Increase awareness on social engineering and information leakage

A trend identified in the group interventions was lack of awareness on social engineering and information leakage. This is a risk that has evolved together with the importance of information and often addresses the employees in an organization. For any large organization with effective technical defenses, attackers can choose to use this type of targeted attacks in order to get the right information. The security department has addressed social engineering in the annual security education and also tested these skills. It is important that the education and increasing awareness are also important in the future. Many of the employees in Norsk Tipping handle customers and media and it is important that they have the knowledge and the awareness to identify and deal with these attacks in the future.

To improve the knowledge and awareness the security department should invest resources in addressing this when they have the opportunity. In the annual security education this should be addressed, it is important that social engineering and information leakage is continuously described to the employees. When large cases of social engineering is described in the media, like the attack on the Norwegian defense in 2011, the security department should store this cases for use in future education. One possibility is to have a small section on the intranet where the security department can link to examples of social engineering. It is also important that they teach the employees how these attacks can be launched, what they include and how to act if the employees are suspicious.

6) Review the classification guidelines in Norsk Tipping

Several employees experience that the classification guidelines needs a revision. They expressed that they found it difficult to classify documents today and revised guidelines or modified templates should be created. This is something that the security department should have in mind if they continue the group interventions with the remaining department. If several employees suggest changing or revising the guidelines, the security department should investigate the usage of the classification guidelines in the departments and the ability to modify them to make them more useful.

By improving the classification guidelines the usage of the classification can be improved. This will include the entire organization and requires resources from different departments. But it important to adjust the classification if employees find this difficult and to avoid that future information is classified wrong or not at all.

7) Improve the awareness on the core concept of information security

Confidentiality, integrity and availability are core concepts in information security. They are the concepts that the security education in Norsk Tipping is built on and where the security documentation has its origin. To address why security is important and why they need to have a relationship to security in today's society is important to the ownership towards security. If the employees do not understand why they need to think security, it is difficult to improve the knowledge and the behavior. By including the core concepts of information security in education and to thoroughly explain why they are important can improve the more specific situations in the security education.

8) Follow up the other indications identified in the group interventions

In addition to the five trends, gaps including two or more groups, there were identified 5 additional gaps in the interventions. If the security department chooses to complete the interventions with the remaining departments, they should pay attention to the additional gaps that are identified. These gaps can indicate important trends that should be addressed in future education or in adjusted education to group of employees.

9) Develop measurement tool for the cognitive dimension of the employees

This task is one of the most important actions to complete in order to get a functional method. Because of the lack of time and resources and that the employees must participate in one group intervention to define the expected levels, the actual measurement of the method was done with qualitative interviews. The participants had the opportunity to evaluate the group session, but with that method the behavior was not measured. The actual level is suggested by the participants and the group decides the final level.

When doing security education it is important to measure the effect of the education. If education is completed without measuring the effects, the results cannot be evaluated and the outcome of the education is uncertain. It is difficult to improve the education, the knowledge and behavior of the participants without a proper measurement tool. The security measurement metrics are difficult to define and it is difficult to perform proper security measurement.

A pretest/posttest method is used to measure security. The pretest can be used to create an initial state of employees, performed before an intervention or educational setting. In the participatory method the group intervention can be used as a pretest. The group defines the actual levels and the result can be used as a basis for the future measurements. Despite that the levels are evaluated, not measured. The security department needs to develop a post-test that measures the behavior to the employees and compare this to the defined cognitive levels.

The researcher recommends using a questionnaire to address the three first cognitive levels from Bloom's revised taxonomy. This includes remember, understand and apply level. The employees meet the requirements by knowing how to perform the procedures stated in the security handbook and why these are used. These levels should be regarded as requirements for most of the employees. The control questions that are developed to the group interventions can be used as a starting point for a questionnaire.

In addition to these questions new questions should be developed to address the security documentation. It is important that these questions target the different cognitive levels and not only address retention and repeat knowledge. Questions that identifies if the employees understand the concept and what he or she think is important, can be used to identify potential risks for the company. More complex questions like "in your opinion, what are the most common ways malicious software get into Norsk Tipping's network?" can indicate the knowledge and understanding of an employee. If the expected level of an employee is defined to be level 4 – analyze, he should be able to give a reasonable answer to such questions.

The method also identified several special security considerations is important areas for the employees. It may be difficult to create questions that are able to measure if the employees meet these special considerations. The researcher recommends test cases that address these considerations. One example can be to

create a social engineering case that is addressed to the communication department and the reception. These units have a special responsibility to the customers and social engineering can be launched to one of these units. The test cases can be adjusted with different content and be targeted to one or more department.

Penetration testing is also a method that can be used to measure the employees as a post-test. This can be completed with professionals and be used on large group of employees all smaller groups that have a similar cognitive levels. These penetration tests can be used on a general level and low cognitive levels or be adjusted to selected units.

10) Divide employees in groups for education

If the security department completes the interventions with the remaining departments it will get an accurate picture of the organization. Most of the employees are not defined as business critical and many of the groups could end up on level two and three in the participatory model. These levels indicate that the employees must understand and follow the guidelines provided by the security department. Based on the resources to the security department it should be performed classroom education to these groups of employees, if there are identified gaps between the actual behavior and the expected level. By using this method the security department reaches out to a large group of employees and it has the opportunity to adjust the content to the employees.

The reason for choosing this method is based on that the employees have similar demands towards security and that the method can be used to address many employees with a small amount of resources. The security department should use their annual security education on these employees, with issues that has been identified in the group interventions. By giving the employees this general education should be effective based on the demands of security. Then the security department can provide adjustable education for the business critical functions, in order to improve the security for the organization.

Results of the chapter:

- Review the security categories and cognitive classification
- Complete the interventions with the other departments
- Improve the categories where it was identified gaps during the test phase of the method
- Develop measurement tool for method
- Perform targeted security education to different groups of employees

9 Bibliography

1. Hagen, J.M., E. Albrechtsen, and J. Hovden, *Implementation and effectiveness of organizational information security measures*. Information Management \& Computer Security, 2008. **16**: p. 377 - 397.
2. Schneier, B., *Secrets & Lies: Digital Security in a Networked World*. 1st ed. 2000, New York, NY, USA: John Wiley \& Sons, Inc.
3. Albrechtsen, E., *A qualitative study of users' view on information security*. Computers \& Security, 2007. **26**(4): p. 276 - 289.
4. Levin, M. and D.J. Grennwood, *Introduction to Action Research*, ed. C.D. Laughton. 1998: SAGE Publications.
5. Puhakainen, P., *A Design Theory For Information Security Awareness*. 2006, University of Oulo.
6. Albrechtsen, E. and J. Hovden, *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study*. Computers \& Security, 2010. **29**(4): p. 432 - 445.
7. Jaziar, R. and J.G. Jose. *Understanding Hidden Information Security Threats: The Vulnerability Black Market*. in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. 2007.
8. PricewaterhouseCoopers, *Current practice and the measurement of success*. 2007, European Network and Information Security Agency.
9. Siponen, M.T. and H. Oinas-Kukkonen, *A review of information security issues and respective research contributions*. SIGMIS Database, 2007. **38**(1): p. 60-80.
10. Wright, M. and J. Kakalik, *Information security: contemporary cases*. 2007: Jones and Bartlett.
11. Lacey, D., *Managing the Human Factor in Information Security: How to Win Over Staff and Influence Business Managers*. 2009: Wiley.
12. Wright, M. and J. Kakalik, *Information Security: Contemporary Cases*, ed. T. Anderson. 2007: Jones and Bartlett Publishers. 187-207.
13. Albrechtsen, E., *Friend or foe? Information security management of employees*. 2008, Norwegian University of Science and Technology: Trondheim. p. 2008:101.
14. Puhakainen, P. and M. Siponen, *Improving Employees' Compliance through Information Systems Security training: An action reserach study*. Mis Quarterly, 2010. **34**(4): p. 757-778.
15. Greenwood, D.J. and M. Levin, *Introduction to action research: social research for social change*. 1998: Sage Publications.
16. Baskerville, R.L., *Investigating information systems with action research*. Commun. AIS, 1999. **2**.
17. Greenwood, D.J., W.F. Whyte, and I. Harkavy, *Participatory Action Research as a Process and as a Goal.* Human Relations, 1993. **46**(2): p. 175-192.
18. Baskerville, R.L. and A.T. WoodHarper, *A critical perspective on action research as a method for information systems research*. Journal of Information Technology, 1996. **11**(3): p. 235-246.
19. Ottosson, S., *Participation action research - A key to improved knowledge of management*. 2003.
20. Dickens, L. and K. Watkins, *Action Research: Rethinking Lewin*. Management Learning, 1999. **30**(2): p. 127-140.
21. Levin, M. and R. Klev, *Forandring som praksis. Læring og utvikling i organisasjoner*. 2002: Fagbokforlaget.

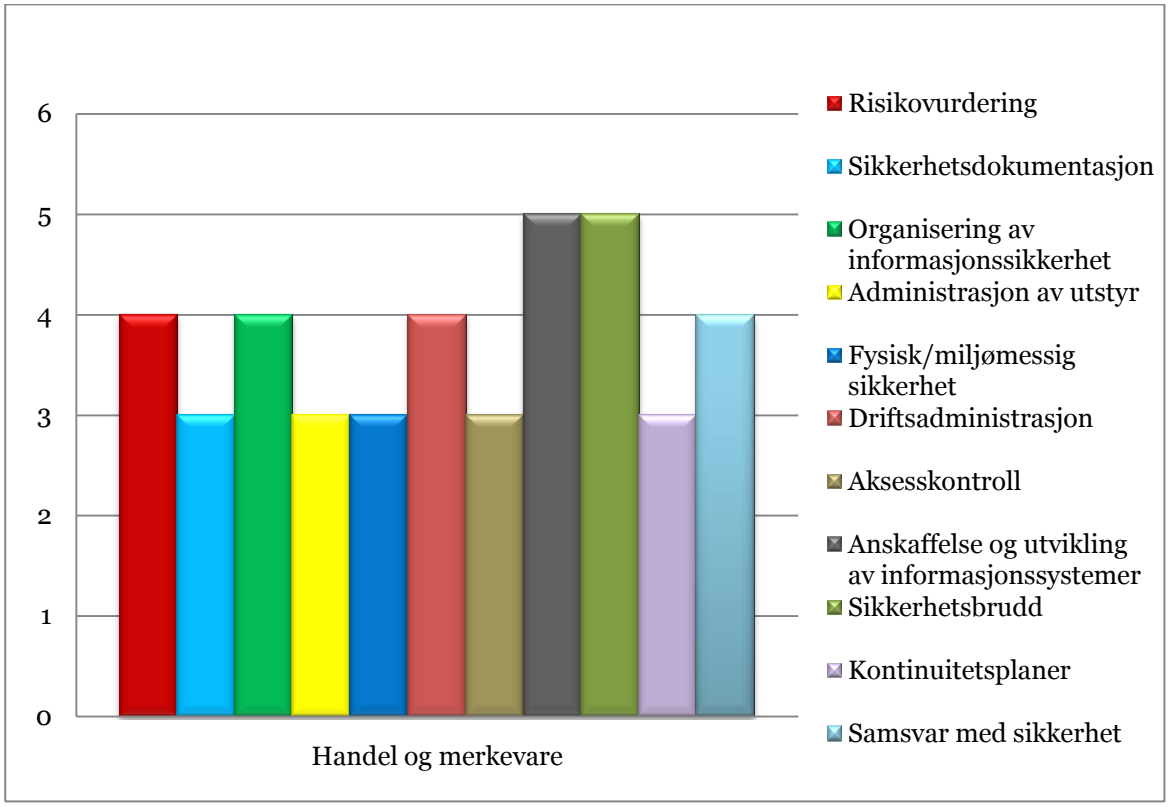
22. Lund, J. and L.E. Aarø, *Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors.* Safety Science, 2004. **42**(4): p. 271 - 324.
23. Hagen, J.M., *The Human Factor behind the Security Perimeter*. 2009, University of Oslo: Oslo.
24. Thomson, K.-L. and R. von Solms, *Towards an Information Security Competence Maturity Model.* Computer Fraud \& Security, 2006. **2006**(5): p. 11 - 15.
25. Schein, E.H., *Organizational culture and leadership*. 3rd ed, ed. J.W. Sons. 2004: Jossey-Bass. 437.
26. Nonaka, I. and H. Takeuchi, *The knowledge-creating company: how Japanese companies create the dynamics of innovation*. 1995: Oxford University Press.
27. Anderson, L.W., et al., *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Abridged Edition*. 2 ed. 2000: Allyn \& Bacon.
28. Anderson, L.W., *Objectives, evaluation, and the improvement of education*. Studies In Educational Evaluation, 2005. **31**(2-3): p. 102-113.
29. Athanassiou, N., J.M. McNett, and C. Harvey, *Critical Thinking in the Management Classroom: Bloom's Taxonomy as a Learning Tool.* Journal of Management Education, 2003. **27**(5): p. 533-555.
30. Amer, A., *Reflections on Bloom's Revised Taxonomy*. Electronic Journal of Research in Educational Psychology, 2006. **4**: p. 213 - 230.
31. Kvale, S.a.B., Svend, *Det kvalitative forskningsintervju*. Vol. 2. 2009: Gyldendal akademisk.

Appendix A

Group interventions

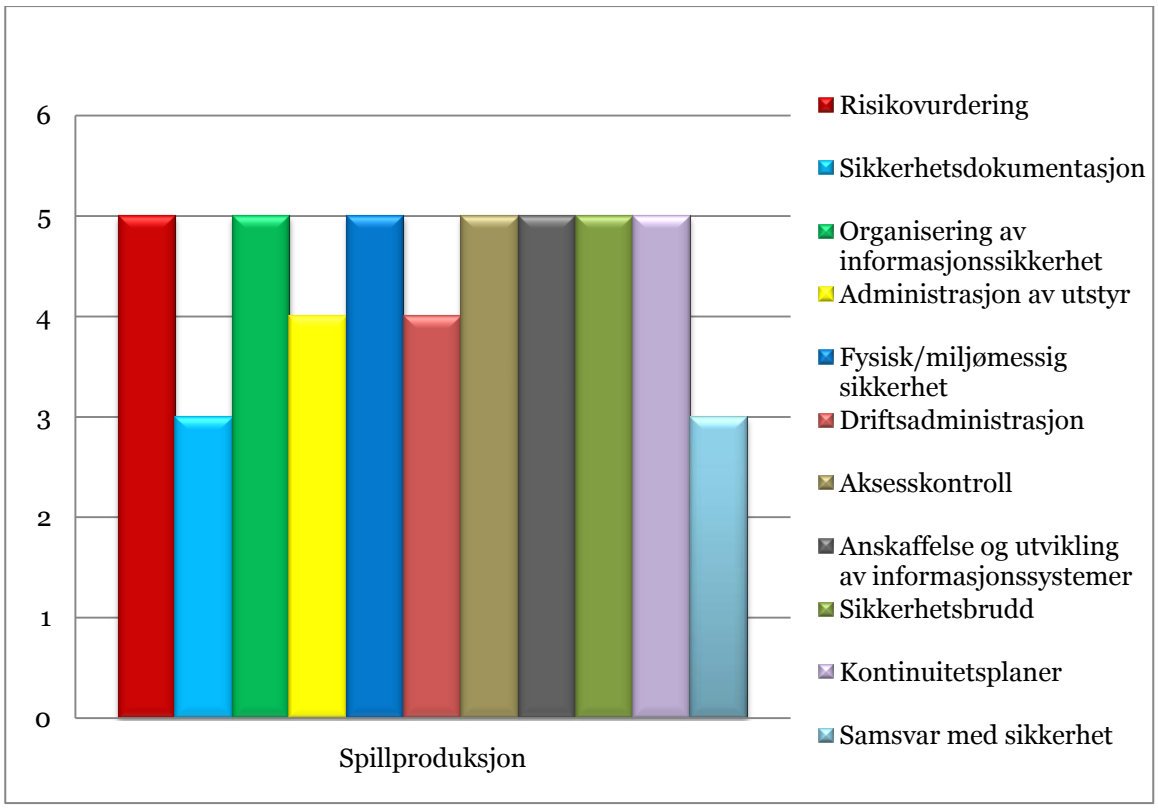
Sikkerhetskategorier – handel og merkevare

ISO/IEC 27001 - sikkerhetsinstruks	Spørsmål	1	2	3	4	5	6
A4 – Risikovurdering	På hvilket nivå bør de ansatte kjenne til risikovurdering og gjennomføring av dette?			☆	x		
A5 – Sikkerhetsdokumentasjon	På hvilket nivå bør de ansatte kjenne til sikkerhetspolicy? ☆		x				
	På hvilket nivå bør de ansatte kjenne til sikkerhetsinstruksen?			x ☆			
A6 – Organisering av informasjonssikkerhet	Hvor godt bør de ansatte kjenne til taushetsplikten?					x ☆	
	På hvilket nivå bør de ansatte kjenne til konfidensialitet, integritet og tilgjengelighet?		x ☆				
A7 – Administrasjon av utstyr	Hvor godt bør de ansatte kjenne til reglene for bruk av bærbart utstyr?			x ☆			
	På hvilket nivå bør de ansatte være når det gjelder klassifisering av informasjon?		x ☆				
A9 – Fysisk/miljømessig sikkerhet	På hvilket nivå bør de ansatte kjenne de fysiske retningslinjene i Norsk Tipping?			x ☆			
A10 – Driftsadministrasjon	På hvilket nivå bør de ansatte kjenne til håndtering av og beskyttelse mot mobil kode?			☆	x		
A11 – Aksesskontroll	På hvilket nivå bør de ansatte kjenne til passordbestemmelsene og håndtering av egne passord?			x ☆			
	Hvilket nivå bør de ansatte være på ved håndtering av ubevoktet utstyr og clear desk filosofi?			x ☆			
A12 – Anskaffelse og utvikling av informasjonssystemer	På hvilket nivå bør de ansatte kjenne til social engineering og informasjonslekkasje?					x ☆	
A13 – Sikkerhetsbrudd	På hvilket nivå bør de ansatte være i forhold til rapportering av sikkerhetshendelser?					x ☆	
A14 - Kontinuitetsplaner	På hvilket nivå bør de ansatte kjenne til kontinuitetsplanene og gjennomføringen av disse?			x ☆			
A15 – Samsvar med sikkerhet	På hvilket nivå bør de ansatte være på når det gjelder samsvar med sikkerhetspolicy og standarder?				x ☆		


6
5
4
3
2
1
0
Handel og merkevare
Risikovurdering
Sikkerhetsdokumentasjon
Organisering av informasjonssikkerhet
Administrasjon av utstyr
Fysisk/miljømessig sikkerhet
Driftsadministrasjon
Aksesskontroll
Anskaffelse og utvikling av informasjonssystemer
Sikkerhetsbrudd
Kontinuitetsplaner
Samsvar med sikkerhet

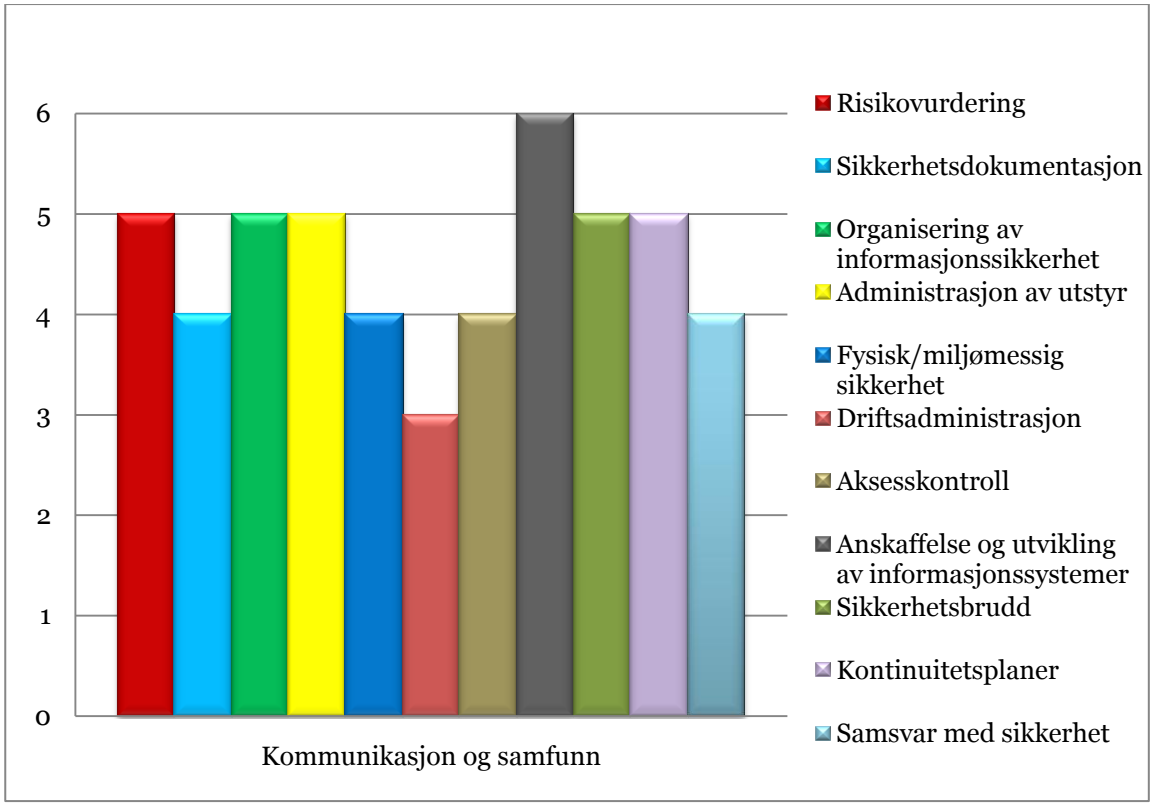
Sikkerhetskategorier - spillproduksjon

ISO/IEC 27001 - sikkerhetsinstruks	Spørsmål	1	2	3	4	5	6
A4 – Risikovurdering og risikohåndtering	På hvilket nivå bør de ansatte kjenne til risikovurdering og gjennomføring av dette?			☆		x	
A5 – Sikkerhetspolicy	På hvilket nivå bør de ansatte kjenne til sikkerhetspolicy?		☆	x			
	På hvilket nivå bør de ansatte kjenne til sikkerhetsinstruksen?				x ☆		
A6 – Organisering av informasjonssikkerhet	Hvor godt bør de ansatte kjenne til taushetsplikten?					x ☆	
	På hvilket nivå bør de ansatte kjenne til konfidensialitet, integritet og tilgjengelighet?			☆		x	
A7 – Administrasjon av aktiva	Hvor godt bør de ansatte kjenne til reglene for bruk av bærbart utstyr?				x ☆		
	På hvilket nivå bør de ansatte være når det gjelder klassifisering av informasjon?		☆	x			
A9 – Fysisk og miljømessig sikkerhet	På hvilket nivå bør de ansatte kjenne de fysiske retningslinjene i Norsk Tipping?					x ☆	
A10 – Kommunikasjons- og driftsadministrasjon	På hvilket nivå bør de ansatte kjenne retningslinjer for beskyttelse mot mobil kode?				x ☆		
A11 – Aksesskontroll	På hvilket nivå bør de ansatte kjenne til passordbestemmelsene og håndtering av egne passord?					x ☆	
	Hvilket nivå bør de ansatte være på ved håndtering av ubevoktet utstyr og clear desk filosofi?				x ☆		
A12 – Anskaffelse, utvikling og vedlikehold av informasjonssystemer	På hvilket nivå bør de ansatte kjenne til social engineering og informasjonslekkasje?			☆		x	
A13 – Sikkerhetsbrudd	På hvilket kognitivt nivå bør de ansatte være i forhold til rapportering av sikkerhetshendelser?					x ☆	
A14 - Kontinuitetsplanlegging	På hvilket nivå bør de ansatte kjenne til kontinuitetsplanene og gjennomføringen av disse?					x ☆	
A15 – Samsvar	På hvilket nivå bør de ansatte være på når det gjelder samsvar med sikkerhetspolicy og standarder?			x ☆			


6
5
4
3
2
1
0
Spillproduksjon
Risikovurdering
Sikkerhetsdokumentasjon
Organisering av informasjonssikkerhet
Administrasjon av utstyr
Fysisk/miljømessig sikkerhet
Driftsadministrasjon
Aksesskontroll
Anskaffelse og utvikling av informasjonssystemer
Sikkerhetsbrudd
Kontinuitetsplaner
Samsvar med sikkerhet

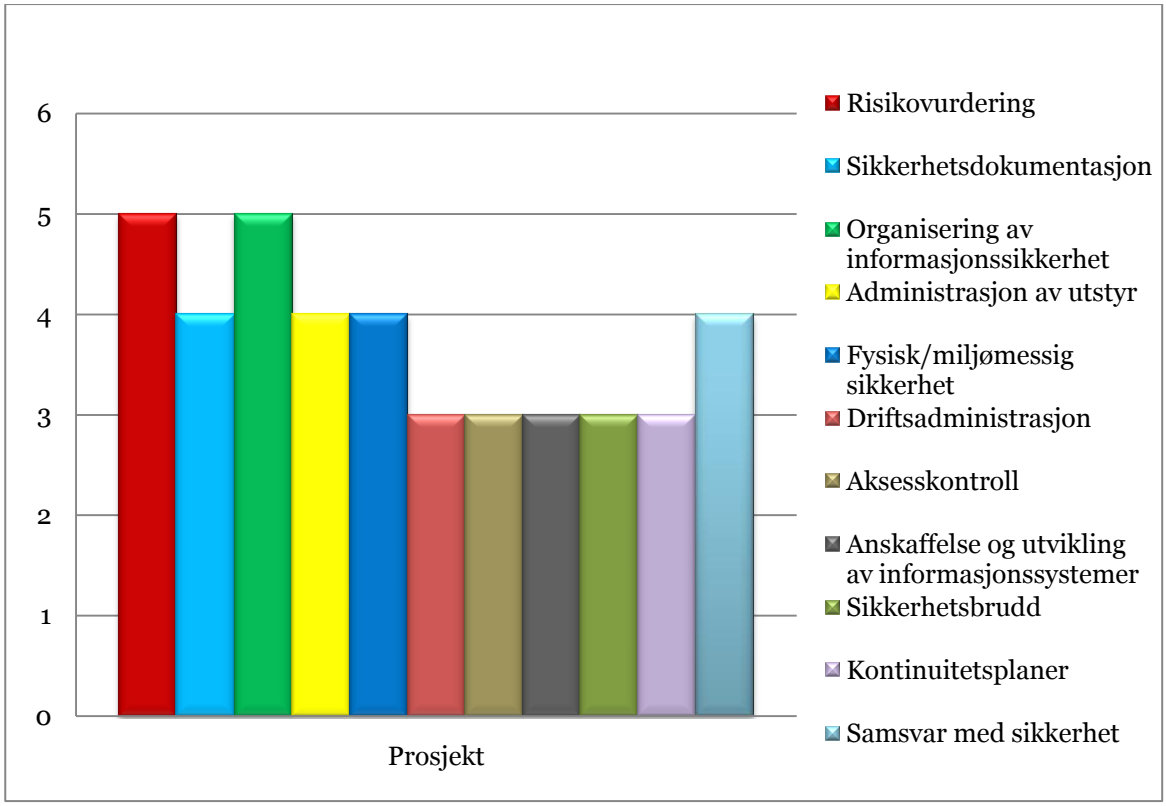
Sikkerhetskategorier – kommunikasjon og samfunn

ISO/IEC 27001 - sikkerhetsinstruks	Spørsmål	1	2	3	4	5	6
A4 – Risikovurdering	På hvilket nivå bør de ansatte kjenne til risikovurdering og gjennomføring av dette?					x	
A5 – Sikkerhetsdokumentasjon	På hvilket nivå bør de ansatte kjenne til sikkerhetspolicy?		x				
	På hvilket nivå bør de ansatte kjenne til sikkerhetsinstruksen?					x	
A6 – Organisering av informasjonssikkerhet	Hvor godt bør de ansatte kjenne til taushetsplikten?						x
	På hvilket nivå bør de ansatte kjenne til konfidensialitet, integritet og tilgjengelighet?		x				
A7 – Administrasjon av utstyr	Hvor godt bør de ansatte kjenne til reglene for bruk av bærbart utstyr?				x		
	På hvilket nivå bør de ansatte være når det gjelder klassifisering av informasjon?					x	
A9 – Fysisk/miljømessig sikkerhet	På hvilket nivå bør de ansatte kjenne de fysiske retningslinjene i Norsk Tipping?				x		
A10 – Driftsadministrasjon	På hvilket nivå bør de ansatte kjenne til håndtering av og beskyttelse mot mobil kode?			x			
A11 – Aksesskontroll	På hvilket nivå bør de ansatte kjenne til passordbestemmelsene og håndtering av egne passord?				x		
	Hvilket nivå bør de ansatte være på ved håndtering av ubevoktet utstyr og clear desk filosofi?				x		
A12 – Anskaffelse og utvikling av informasjonssystemer	På hvilket nivå bør de ansatte kjenne til social engineering og informasjonslekkasje?						x
A13 – Sikkerhetsbrudd	På hvilket nivå bør de ansatte være i forhold til rapportering av sikkerhetshendelser?					x	
A14 - Kontinuitetsplaner	På hvilket nivå bør de ansatte kjenne til kontinuitetsplanene og gjennomføringen av disse?					x	
A15 – Samsvar med sikkerhet	På hvilket nivå bør de ansatte være på når det gjelder samsvar med sikkerhetspolicy og standarder?				x		


6
5
4
3
2
1
0
Kommunikasjon og samfunn
Risikovurdering
Sikkerhetsdokumentasjon
Organisering av informasjonssikkerhet
Administrasjon av utstyr
Fysisk/miljømessig sikkerhet
Driftsadministrasjon
Aksesskontroll
Anskaffelse og utvikling av informasjonssystemer
Sikkerhetsbrudd
Kontinuitetsplaner
Samsvar med sikkerhet

Sikkerhetskategorier - prosjekt

ISO/IEC 27001 - sikkerhetsinstruks	Spørsmål	1	2	3	4	5	6
A4 – Risikovurdering	På hvilket nivå bør de ansatte kjenne til risikovurdering og gjennomføring av dette?				☆	x	
A5 – Sikkerhetsdokumentasjon	På hvilket nivå bør de ansatte kjenne til sikkerhetspolicy? ☆			x			
	På hvilket nivå bør de ansatte kjenne til sikkerhetsinstruksen?				x ☆		
A6 – Organisering av informasjonssikkerhet	Hvor godt bør de ansatte kjenne til taushetsplikten?				x ☆		
	På hvilket nivå bør de ansatte kjenne til konfidensialitet, integritet og tilgjengelighet?			☆			x
A7 – Administrasjon av utstyr	Hvor godt bør de ansatte kjenne til reglene for bruk av bærbart utstyr?				x ☆		
	På hvilket nivå bør de ansatte være når det gjelder klassifisering av informasjon?		☆	x			
A9 – Fysisk/miljømessig sikkerhet	På hvilket nivå bør de ansatte kjenne de fysiske retningslinjene i Norsk Tipping?				x ☆		
A10 – Driftsadministrasjon	På hvilket nivå bør de ansatte kjenne til håndtering av og beskyttelse mot mobil kode?			x ☆			
A11 – Aksesskontroll	På hvilket nivå bør de ansatte kjenne til passordbestemmelsene og håndtering av egne passord?				x ☆		
	Hvilket nivå bør de ansatte være på ved håndtering av ubevoktet utstyr og clear desk filosofi?			x ☆			
A12 – Anskaffelse og utvikling av informasjonssystemer	På hvilket nivå bør de ansatte kjenne til social engineering og informasjonslekkasje?		☆	x			
A13 – Sikkerhetsbrudd	På hvilket nivå bør de ansatte være i forhold til rapportering av sikkerhetshendelser?			x ☆			
A14 - Kontinuitetsplaner	På hvilket nivå bør de ansatte kjenne til kontinuitetsplanene og gjennomføringen av disse?			x ☆			
A15 – Samsvar med sikkerhet	På hvilket nivå bør de ansatte være på når det gjelder samsvar med sikkerhetspolicy og standarder?				x ☆		


6
5
4
3
2
1
0
Prosjekt
Risikovurdering
Sikkerhetsdokumentasjon
Organisering av informasjonssikkerhet
Administrasjon av utstyr
Fysisk/miljømessig sikkerhet
Driftsadministrasjon
Aksesskontroll
Anskaffelse og utvikling av informasjonssystemer
Sikkerhetsbrudd
Kontinuitetsplaner
Samsvar med sikkerhet

Appendix B

Spørsmål til kategoriene

A4

- Kan du forklare hvordan en risikovurdering bør gjennomføres?
- Hvordan er en risikovurdering bygget opp?
- Hvilke metoder brukes for å håndtere risiko?
- Hvorfor gjennomfører vi risikovurderinger?
- Hva er viktige elementer i en risikovurdering?

A5

- Kan du gjengi ett av sikkerhetsprinsippene som står beskrevet i sikkerhetspolicyen?
- Kan du gi en kort forklaring på ansvarsfordelingen som er beskrevet i policyen?
- Hva er Norsk Tippings sikkerhetsmål?
- Hva plikter du å gjøre som ansatt ifølge sikkerhetspolicyen?
- Hvordan foregår klassifiseringen av et dokument?(nivå 3 – bruke)

A6

- Kan du gjengi et at punktene i taushetserklæringen?
- Hva kan brudd på taushetsplikten medføre?
- Kan du forklare begrepene konfidensialitet/integritet/ tilgjengelighet?

A7

- Hva skal du passe på hvis du disponerer elektronisk utstyr utenfor Norsk Tippings lokaler?
- Hva skal du gjøre hvis du mister elektronisk utstyr?
- Hvordan er klassifiseringen av informasjonen inndelt i Norsk Tipping?
- Kjenner du til forskjellene mellom de ulike klassifiseringene?
- Kan du klassifisere et dokument?

A9

- Hva skal du gjøre hvis du møter en person uten synlig adgangsbevis?
- Hva skal du gjøre hvis du får besøk i arbeidstiden?
- Hvilke regler gjelder for besøkende hos Norsk Tipping?

A10

- Hva skal du gjøre hvis du får mistanke om virus på din personlige PC?
- Hva kan være kjennetegn på en infisert PC?

A11

- Nevn tre kjennetegn på et sterkt passord
- Hvordan bør man lagre passord?
- Hva skal du gjøre hvis du finner en usb-key?

A12

- Kan du forklare begrepet social engineering?
- Hvilke metoder kan en angriper benytte innenfor social engineering?
- Hva skal du gjøre hvis du tror du blir utsatt for et SE angrep?

A13

- Hva gjør du hvis du opptager en sikkerhetshendelse på jobb?
- Hvordan skal du rapportere en sikkerhetshendelse?
- Kan du nevne tre eksempler på sikkerhetshendelser?

A14

- Kjenner du til beredskapsplanene som gjelder din avdeling?
- Har dere utviklet egne beredskapsplaner? Er disse oppdatert?

A15

- Er du bevisst på sikkerhet i det daglige arbeidet?

Appendix C

Qualitative interviews with participants

Deltager A

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Ja. Klar og grei. Absolutt ikke problemer med å skjønne den.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Positiv til dette. Avdelingen samarbeider mye med sikkerhet. Vi må følge mange rutiner og bør kunne disse.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Ikke mer. Lå høyt i utgangspunktet. Driver med sikkerhet hver dag og har hatt rutiner lenge. Oppstår det saker så snakker vi sammen.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Konstruktiv og bra metode. Jeg føler at jeg ble hørt og det gjelder samtlige som deltok.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det synes jeg absolutt. Synes metoden virker veldig nyttig.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Husker ingen spesiell episode. Men fikk frisket opp mye. Nyttig og gå gjennom hver kategori. Innholdet sitter bedre ved deltagelsen.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Nei. Nytt og spennende konsept. Bra med diskusjon og relevante tema.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Jeg synes det var veldig bra. Engasjerende at vi kan påvirke å få delta. Oppfrisking er et pluss. Ufarlig metode, snakker sammen på en god måte.

Deltager B

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Positivt med utsendt informasjon på forhånd. Hadde lest igjennom og fått en forståelse. Bra forklart i gruppesesjonen

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Veldig bra å kunne forme selv. Da kan man sette fokus på det som er viktig, ikke all læring er like relevant.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Ja. Har sett på sikkerhetspolicyen en gang til. Positivt sett i forhold til instruksen.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Føler at jeg ikke ble overkjørt. Prøvde å holde litt igjen fordi jeg kan sitte med min oppfatning frem til de andre fikk sagt sitt.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det tror jeg helt sikkert.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Nei det gjorde jeg ikke.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Nei i utgangspunktet ikke. Kunne vært interessant og satt scorene opp mot hverandre.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Bør kanskje være tilpasset til noen grupper. Mange ansatte kan kjøre felles opplæring. Vi har høyt fokus (er med på sikkerhetsmøter etc).

Deltager C

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Den virket noe komplisert. Vanskelig å skille de forskjellige kognitive nivåene fra hverandre.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Det høres veldig riktig ut. Mer rettet mot bruker og ikke bare generell informasjon.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Har kikket litt igjennom policyen. Tenkt litt mer på. Men "slapper" nok av mer etter hvert og glemmer en del?

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Det synes jeg gikk veldig fint, når jeg ble enig med meg selv.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det tror jeg.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Vanskelig å si. Gjør ikke noe annerledes etter intervensjonen. Man vet hva man ikke skal gjøre.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Kunne gått igjennom instruksen og spurt noen spørsmål. Gått igjennom retningslinjene fordi mange mener nok at de følger dem, uten helt å vite hva det innebærer.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Jeg synes det. Dette burde kunne fungere.

Deltager D

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Veldig ryddig og kategorisert. I 1. møte var skalaen beskrivende og lett og relatere til. Beskrivende lett og bra.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Man kan bli fartsblind av konsekvensene ved å definere nivå. Men synliggjøring av sikkerhetsrutiner og jevnlige remindere kan være nyttig.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Nei. Blir litt seminareffekt. Man husker det en liten stund.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Ja det var greit. Alle fikk si sine meninger.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det tror jeg. Gjerne en generell del hvor man deretter krydrer med bevissthetsgjøring (nærhetsprinsippet).

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Fungerte som en reminder.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Mange spørsmål og kategorier. Men klarte etter hvert å diskutere skillene.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Jeg synes at det bør prøve. Det kan øke nærhetsprinsippet til sikkerhet. Beholde den generelle delen og krydre bevissthet.

Deltager E

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Skjønte prosessen. Fint å kunne diskutere de forskjellige kategoriene. Ikke vanskelig å forstå.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Veldig positivt. Da kan man mene noe om hvor man bør være og kunne påvirke dette, istedenfor å få tredd en instruks nedover hodet.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Nei. Har et høyt fokus på sikkerhet i utgangspunktet. Veldig opptatt av sikkerhet.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Ble hørt bra. Kunne diskutere oss frem sammen i gruppa. Veldig bra.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Blir lagt inn på et nivå så ja. Instruksen er bare en instruks, dette må være tilpasset brukeren.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Vanskelig å svare på. Dukket sikkert opp en del ting rundt plasseringen i de forskjellige kategoriene.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Hatt litt bedre tid. Ble ganske intensivt. Kunne hatt 2 bolker hvor man sammenlignet en annen gruppe med samme rolle. Burde blitt kjørt med hele gruppa.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ja. Mye av sikkerhet er funnet opp av sikkerhetsfolk som sitter og bestemmer. Man får dermed ikke eierskap til instruksen. Mer tilpasset og mer skreddersydd instruks og økt eierskap.

Deltager F

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Skjønte modellen, intuitiv.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Positivt. Kunne relatere til arbeidsoppgaver. Bør trenes mer opp mot caser i praksis.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Endret adferd – nei, men ja diskusjon kan bedre bevissthet.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

God tone og god dialog.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja, men det må forandre hos mange, gå bredt ut i bedriften.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Nei. Mye er godt innarbeidet og tenkt igjennom det meste tidligere.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Virket godt forberedt. Man diskuterer seg varm, bare viktig å sette av nok tid til gjennomføringen.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Det hjelper sikkerhetsavdelingen, positive for de som er med på opplæringen (ringvirkninger). Må ned på konkrete ting, ikke for overordnet innhold.

Deltager G

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Skjønte modellen. Var en veldig sunn prosess. Man tenker igjennom det man gjør← bra. Flere er med å hjelpe hverandre.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Veldig lurt å kunne definere et eget sikkerhetsnivå. Da tar man mer eierskap og etterlever det i større grad. Gjør det mer aktuelt for personen.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Helt klart, på flere områder.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Følte meg ikke overkjørt. Jeg hadde klare synspunkter, men dette ble tatt til etterretning.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Tror absolutt at dette lønner seg. Individuelle tiltak. Hva er risiko for oss og hva anser vi som risikomomenter.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Belyste en del ting. Får snakket gjennom og kan øke bevisstheten på større områder.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Be at noen tenker over ting før de kommer. Fin framgangsmåte som var bra tematisert. Ikke ha større grupper, bør engasjere alle.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ja absolutt noe å ta med videre. Er en form som passer selskapet. Mer fokus på sikkerhet, den generelle sikkerhetsbiten ←mange ansatte har mye å gå på. Dialog med sikkerhetsavdelingen kan være viktig. Smart måte.

Deltager H

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Veldig greit med det første møtet. Litt uklart hvilke forventninger det var til meg kontra mine ansatte.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Veldig mye fokus på området. Leder blir også utfordret på sikkerhet som er viktig. Kan ta ting som ikke er daglig/operativt.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Har ikke blitt mindre. Møte var interessant og nyttig.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Ja det var helt i orden. Fin seanse.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det kan gi større bevissthet og eierskap. I større grad bevissthet som kan være viktigere for mange av de ansatte.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Betryggende og vite at de ansatte var dyktige på sikkerhet. Føler meg også veldig trygg på sikkerhetsavdelingen.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Ikke noe som jeg husker så da mener jeg nei.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ser ikke bort fra det. Selv har vi god kontakt med sikkerhet. Ingen sterke meninger om ja eller nei. Noen grensesnitt mellom avdelingen bør kanskje friskes opp.

Deltager I

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Skjønte poenget. Lett forståelig og enkelt satt opp.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Veldig fornuftig. Nå er det slik alle skal igjennom det samme. Blir større tilknytning blant de ansatte.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Nei. Satt friskt i minnet fordi vi har drevet med sikkerhetsbevissthet i det siste. Ikke noe nytt.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Jeg synes at de ble ivaretatt. Gruppa endte opp på et felles nivå.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja absolutt veldig fornuftig. Kan gjelde andre områder også, ikke bare sikkerhet.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Ingen nye aha-opplevelser. Hadde fokus fra tidligere og det blir et samtaleemne i avdelingen når det er ferskt. Men kunne fått aha-opplevelser hvis det ikke var tilfellet.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Noe i forkant kunne vært lurt, men opplegget var lett forståelig.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ja jeg synes at det var positivt/og metode. Kan fungere som en tilleggssak til den vanlige opplæringen. Får det i sin egen gate og det skaper mer interesse.

Deltager J

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Veldig grei. Greit forklart og lett og forstå.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Kjempefint. Nyttig med avdelingsrettede sikkerhetsrutiner og instrukser.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Ja har faktisk tenkt mer sikkerhet i etterkant.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Jeg var enig med det som vi kom frem til og ble absolutt hørt.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det tror jeg. Særlig på avdelingsnivå i forhold til generelt i Norsk Tipping.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Nei, egentlig ikke.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Nei i grunn ikke.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Som en tilleggsak for avdelingen. Kan bidra mer på avdelingsnivå.

Deltager K

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Forberedende runde var veldig klar. Nyttig og lærerikt. Vanskelig å skille mellom hvor vi burde være/er i gruppesesjonen.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Opplegget var bra. Var bevisstgjøring i sesjonen. Eierskapet og bevissthet økes – det er en bra kombo.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Ingen nye caser. Har jobbet med sikkerhetsstrategi fortløpende.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Ja ikke noe problem. Mer opptatt av å begrense meg for at de andre i gruppa skal kunne bli hørt.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja. Bra opplegg og bra tilnærming. Sikkerhet er kanskje ikke hovedfokus og det mest spennende vi driver med. Opplegget krever oppfølging innen rimelig tid.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Det var en bevisstgjøring rundt relasjonen mellom egen rolle og sikkerhet. Se hvordan sikkerhet henger sammen med det vi gjør.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Det var vanskelig å skille mellom hvor vi burde være og hvor vi er i gruppeintervensjonen.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Fornuftig tilnærming. Noe av det bedre jeg har vært med på. Så hvis det bør læres mer sikkerhet så ja.

Deltager L

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Jeg opplevde at det måtte forklares veldig mye i hver kategori for å definere nivåene.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Positivt med å kunne tilpasse seg rollen min. De ansatte trenger forskjellig opplæring.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Det var lærerikt og vi kom inn på noen nye aspekter under diskusjonen.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Stort sett, men jeg var nok ikke nok frempå. Ble en del vingling på skalaen.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Nivået blir mer målrettet. Metoden har ikke vært brukt tidligere.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Nei, ikke så lett å huske så lang tid tilbake.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Var høyt nivå. Burde kanskje hatt flere eksempler på de ulike nivåene.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Absolutt, dette bør kunne tas med videre.

Deltager M

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Var greit å sette seg inn i. Fint med knagger og henge sikkerhetsarbeidet på.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Ålreit for å øke bevissthet og fokus ytterligere.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Har ikke begynt å gjøre ting på andre måter. Tenker mer naturlig på det og på aspekter som dukker opp i hverdagen.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Ja. Gruppen var homogen som tenkte veldig likt.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja det tror jeg absolutt. Man jobber med ulike områder og bør derfor ha ulik opplæring.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Lærte mer rundt sammenhengen mellom sikkerhetsdokumentasjonen og det som gjøres som opplæring for de ansatte.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Ikke som jeg kan sette fingeren på. Metoden var metodisk og strukturert og man skaper en diskusjon som er positivt.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ja. Det generelle er en ting, men også viktig å kunne få med seg det spesielle i de ulike gruppene. Kan øke bevisstheten.

Deltager N

1) Hvordan opplevde du selve prosessen i gruppeintervensjonen?

Vi brukte litt tid innledningsvis men etter hvert gikk det bra.

2) Hva tenker du om å kunne være med på å forme din egen sikkerhetsopplæring?

Vil gjerne kunne ta del i det. Alle burde være med på det for man blir mer bevisst på sikkerhet.

3) Har du blitt mer engasjert i sikkerhet i etterkant av gruppeintervensjonen?

Var en bevisstgjøring på sesjonen som kan ha gjort meg mer engasjert i etterkant.

4) Føler du at dine synspunkter ble tatt i betraktning og påvirket resultatet i de forskjellige kategoriene?

Alle ble hørt og du forklarte ting bra.

5) Tror du at en metode med tilpasset brukeropplæring kan bidra til å øke bevisstheten og oppførselen til de ansatte vedrørende sikkerhet?

Ja jeg opplever det. Mer spesifikk opplæring er bra.

6) Lærte du noe nytt rundt sikkerhet og din rolle i Norsk Tipping i gruppeintervensjonen?

Husker ting som var blitt tatt lett på og sesjonen var veldig nyttig. Bevisstheten kom etter hvert.

7) Er det noe du mener burde blitt gjort annerledes i gruppeintervensjonen eller som burde bli tatt med i gruppeintervensjonen?

Få noe forklaring på forhånd. Burde kanskje gjennomføres med hele grupperinger, men det kan bli vanskelig å få til.

8) Synes du at en metode med tilpasset brukeropplæring bør innføres i Norsk Tipping?

Ja jeg tror at det funket veldig bra. Bevisstgjøring på et nivå som ikke har blitt gjort før.