ISBN 978-82-471-8026-6 (printed ver.)
ISBN 978-82-471-8043-3 (electronic ver.)
ISSN 1503-8181

NTNU
Norwegian University of
Science and Technology

Eirik Albrechtsen

Doctoral Thesis

Theses at NTNU, 2008:101

NTNU
Norwegian University of
Science and Technology
Thesis for the degree of
philosophiae doctor
Faculty of Social Sciences and Technology Management
Department of Industrial Economy and Technology
Management

NTNU

Theses at NTNU, 2008:101

Eirik Albrechtsen

Friend or foe? Information security management of employees

NTNU
Norwegian University of
Science and Technology

Eirik Albrechtsen

Friend or foe? Information security management of employees

Thesis for the degree of philosophiae doctor

Trondheim, March 2008

Norwegian University of
Science and Technology
Faculty of Social Sciences and Technology Management
Department of Industrial Economy and Technology
Management

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of philosophiae doctor

Faculty of Social Sciences and Technology Management
Department of Industrial Economy and Technology Management

ISBN 978-82-471-8026-6 (printed ver.)
ISBN 978-82-471-8043-3 (electronic ver.)
ISSN 1503-8181

Theses at NTNU, 2008:101

Printed by Tapir Uttrykk

Friend or foe?
Information security management of employees

Eirik Albrechtsen

PhD thesis
Trondheim, March 2008

Norwegian University of Science and Technology (NTNU)
Faculty of Social Sciences and Technology Management
Department of Industrial Economy and Technology Management

Preface

This thesis documents the work carried out during my PhD study at the Norwegian University of Science and Technology (NTNU), Department of Industrial Economics and Technology Management.

The PhD study has been financed by a scholarship from TrygVesta Insurance Company. I am grateful for their financial support.

I am proud to say that I have produced a PhD thesis. I have to admit that it has not always been straightforward and fun, but I persevered and finally completed it. I have learned a lot both professionally and about myself during these years, and feel I have become a more mature and reflected person during this period of study.

One man deserves special thanks for his support during this time. My supervisor, mentor and friend: Professor Jan Hovden. I appreciate and acknowledge the daily conversations, the valuable input, his sharing of experience and network, and his belief in me. Professor Stig Frode Mjølsnes and Professor Eric Monteiro, both at NTNU, have been appointed as co-supervisors.

Writing the thesis has mainly been a one man-show, but nevertheless some people deserve to be acknowledged here: former colleagues at NTNU for both scientific and non-scientific discussions: Snorre Sklet, Helene Cecilie Blakstad, Grethe Osborg Ose, Kjetil Hunnes, Ranveig Kviseth Tinmannsvik and Ivar Kufås; Tor Olav Grøtan and Stig Ole Johnsen at SINTEF for their interest in and the discussions on non-technological parts of information security; Janne Hagen, Gjøvik University College; and the organizing committee of Sikkerhetsdagene. I would also like to acknowledge the assistance from Stewart Clark, NTNU for editing the main part of this thesis.

I also want to thank all the people that made it possible to perform empirical studies: the interviewed users at the IT company and at the bank; the information security managers at the IT company and the bank; the employees at Brønnøysundregistrene for participating in the intervention study; the security managers at Brønnøysundregistrene, Olav Melteig and Marius Naalsund Gjerde, for the cooperation in the intervention project; the interviewed information security managers; and the respondents in the survey on organizational information security measures. Thank you all for sharing your experience and understanding of information security with me, it has been very informative and interesting.

My warmest thanks go to my beloved wife Lena for the encouragement, support and love, and to the best products made during my PhD study: our children Sebastian, Noah and Isabell.

Trondheim, 24 March 2008

Eirik Albrechtsen

Abstract

Although information security traditionally has been a technological discipline, the role and function of employees is an additional important part. Users can both be a threat and a resource in information security management. On the one hand, employees can produce or ignite threats and vulnerabilities. On the other hand, they are a precondition for safe and secure operation. As a consequence, information security management of employees is an important part of the total information security management in organizations.

The general aim of this study is to explore the information security management of employees. This is approached by studying: users' function in and view on information security; measures aiming at improving individual information security performance; and information security management practice in organizations. Findings from explorative interview studies of users and information security managers; an intervention study aiming at improved individual awareness and behaviour; and a survey on organizational security measures were used as the empirical basis in the study.

When it comes to operative work, employees' information security performance is weak. Users perform few proactive information security actions and are indifferent to information security in their daily work. Information security managers mainly view users as a threat and a problem to the information security level, while users view themselves as an untapped resource in the information security work. Individual security performance is created by technological frameworks and formal and informal organizational aspects of information security.

Besides technological solutions framing what it is possible for individual behaviour to perform, the most used measures directed at users are documented requirements for individual behaviour. These measures are evaluated to have limited effect on individual performance. However they are the basis for several other measures, thus they have an indirect effect. Instructions for behaviour are thus necessary, but not sufficient alone.

Education, training and information have the best effect on users when employees and communicators are interacting and are in dialogue. However, information and education

tends to be more based on written and electronic information, rather than rich information with possibilities for two-way communication.

Employee participation is evaluated to be the most effective process to improve individual information security performance, but is modestly used. An intervention study based on direct participation, dialogue and collective reflection in order to improve individual information security awareness and behaviour showed significant improvements among participants. Employee participation is likely to improve the quality of technological and administrative security solutions; improve the usability of security technology; improve security professionals' knowledge of sharp-end information security activities; close the gap in understanding and communication between security managers and users; improve individual ownership, acceptance and motivation for information security; and ensure democratic rights that influence personal working conditions.

If there is a social information security digital divide between users and information security managers, i.e. no interaction and dialogue; differences in risk judgement; and views and experience of information security practice, these will reflect the lack of participation. The information security professionals make the premises for the information security work in an organization without involving users to any extent. The differences result in management strategies based on the prejudiced view that users are more of a security threat than a resource. Consequently, the management approaches might be insufficient for dealing with users as a resource as the information security activities are based on non-realistic understanding of actual work at the sharp-end.

Combinations of adequate measures for all parts of the socio-technical information security systems must be available in order to perform efficient defence, including the handling of employees' function in information security. One needs to handle pragmatic, formal rule-based and technical principles. Managing the human element of information security is thus one of many activities in information security management. The thesis has identified some shortcomings in current approaches to employees. These shortcomings may not be inadequate for other information security efforts than human management, so the current approaches must not be discarded. This thesis has argued in favour of approaches that lead to greater user involvement which would be a complementary addition to traditional information security approaches.

List of publications

PAPER I: Albrechtsen, E. (2007). “A qualitative study of users’ view on information security”. *Computers & Security,* vol.26, iss.4, pp.276-289

PAPER II: Albrechtsen, E. and Hovden, J. “Information security digital divide in organisations: information security managers versus users”. Accepted with revision march 2008, *Computers & Security*. Unrevised document.

PAPER III: Albrechtsen, E. and Hovden, J. “Improving information security awareness and behaviour by a user participative approach: an intervention study”. Accepted for review in *Information & Management*

PAPER IV: Hagen, J., Albrechtsen, E. and Hovden, J. “Implementation and effectiveness of organisational information security measures”. Accepted paper, *Information Management & Computer Security*

PAPER V: Albrechtsen, E. and Hovden, J. (2007). “User participation in information security”. In Aven, T and Vinnem, J.E. (eds.) *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007 (Esrel 2007)*. London, UK: Taylor & Francis, 2551-58

PAPER VI: Albrechtsen, E. and Hovden, J. (2007). “Industrial safety management and information security management: risk characteristics and management approaches”. In Aven, T and Vinnem, J.E. (eds.) *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007 (Esrel 2007)*. London, UK: Taylor & Francis, 2333-40

Table of Contents

PART I: MAIN PART

PART II: PAPERS

PART I

MAIN REPORT

1 Introduction

"The train will stop for a couple of minutes.
We need to re-boot our computer before proceeding to the next station"
Message on the speaker system on a train heading for Oslo, September 2007

The message cited above illustrates that we live in a vulnerable IT society. Malfunctioning IT systems can stop trains as well as other functions in society. In general, failures in information technology systems can have wide-ranging consequences for society, institutions and individuals. On the one hand, information technology has certainly contributed to improvements and advantages for organizations and society by its ability to store information compactly and cheaply with easy access and search possibilities; its ability for externalization of processing; and new methods for communication (Groth, 1999). On the other hand, it has created negative impacts such as risks and vulnerabilities at all levels in society. Society may suffer from unwanted incidents such as power supply stoppage, lack of functionality of public services such as medical treatment and traffic control and lack of public communication paths due to information systems failures. At an organizational level, failures might lead to business interruptions; unavailability of necessary equipment for daily operations; and confidentiality issues. It might also jeopardize the health and lives of organizational members as safety and emergency systems have become dependent on ICT systems.

In a discussion on vulnerabilities regarding the millennium bug problem, Perrow (1999:392) argues that information systems have "…the potential for making a linear, loosely coupled system more complex and tightly coupled than anyone had any reason to anticipate". Although the Internet (servers and digital infrastructure) is robust and reliable (Perrow, 2007), the nature and linkage of computer devices, individuals and organizations connected to the Internet in addition to how organizations and society utilize ICT systems create vulnerabilities in any social system. The impacts of information technology on society are stressed by a number of dynamic external forces, e.g. globalization and fast pace of technological change (Hovden, 2003), making the risk picture dynamic, complex and uncertain. In that sense the information technology and the utilization of it is one of the produced uncertainties in the risk society (Beck, 1992).

As a consequence of the IT-based risk and vulnerabilities at all levels in society, preserving information security has emerged to be one of many essential parts in the creation of a safe and secure society. Basically, information security is about preserving confidentiality, integrity and availability of information systems and information (ISO/IEC 27002). However, as indicated in the paragraph above, the consequences of information security breaches are much more extensive than pure information system failures. As organizations and society become dependent on information technology, information security breaches influence processes at all levels in organizations and in society. For organizations, information security is thus business security (von Solms and von Solms, 2005). Due to the ripple effects of information security breaches, information security is understood in this thesis as not only being about securing the security of computers, i.e. techniques to maintain security within a computer system (Gollmann, 1999), but also about securing communication between systems and securing the use of IT systems by individuals and institutions. Preservation of information security is thus not only about means and methods to protect information technology, but also means and methods to prevent and be prepared for secondary and tertiary effects.

Information security has traditionally been technology-oriented (Dhillon and Backhouse, 2001; Siponen and Oinas-Kukkonen, 2007), with a large number of technological security solutions available. However, by the widespread use of computers at both work and home; the increased connectivity and access to information; the communication channels available by information technology; convergence of technology; and the utilization of technology in new organizational forms and ways of organizing work, non-technological aspects of information security now must be considered in addition to technological aspects. This development implies that the role and function of users of information technology is important to deal with, since users might be a considerable threat to the security level as well as being essential resources to prevent incidents from happening.

1.1 Aim, research questions and premises

The general aim of the study is to explore information security management of employees. This is approached by studying: the users' role and function in information security since it is important to know and understand what you are managing; measures aiming at improving individual information security performance; and actual information security practice in organizations.

The following research questions, which in sum elaborate different information security management strategies, are posed:

1) How is the role and function of regular users in operative information security efforts interpreted by users themselves and information security professionals? Do their interpretations correspond? What explains actual performance of users? (Papers I & II)

2) *How are different measures aiming at the individual level of information security work used?* There are several possible solutions and activities available for influencing user behaviour and awareness, ranging from technological security solutions, instructions for behaviour to awareness campaigns. *Why are some solutions expected to be more effective for this purpose than others?* (Papers I, II and IV)

3) *How do differences in information security expertise, authority and priorities in an organization affect individual information security performance?* Information security does not operate isolated from other organizational processes. Although security is the main goal of information security management, it is only one of many sub-goals for the organization as a whole. Information security professionals are the only members of an organization that have information security as their main agenda and that have expert knowledge on the subject (Paper II)

4) A presumption in the study is that participation is an essential part of all organizational processes. The study will explore *why is employee participation is an essential part of information security?* (Papers I-VI, particularly Papers III and V) *What are the effects on awareness and behaviour of an intervention based on participation and dialogue?*(Paper III)

The research questions are interrelated. The role and function of users found in question 1) can be explained by findings in questions 2), 3) and 4). The elaboration on measures in question 2) are closely linked to decision-makers of the measures in 3) and discussions on participative measures in 4). Question 3) and 4) are related as participation can be a link between different organizational roles.

The questions are responded to by both qualitative and quantitative data. Question 1) is responded to by qualitative interview data. This implies that answers to the question cannot be generalized as the elaboration is interpretations of the interviews of a small number of users and information security managers. Questions 2), 3) and 4) combine qualitative and quantitative data, thus preserving both an understanding of the studied phenomena as well as indicating generalized descriptions. Question 4) is also approached by an intervention study combining quantitative methods to study effects of the intervention and qualitative methods to understand the effects.

The study is based on the following premises, which are elaborated throughout the introduction and in Section 2:

- Information security is viewed in a framework of a socio-technical system. Technological, individual and organizational attributes and the interactions between these contribute in preserving information security in an organization.

- User performance is created by the organizational context. Organizational members' information security behaviour and awareness are created by a combination of technology, workplace conditions and formal and informal organizational factors.

- Employees are important resources in the information security activities of an organization. It would be naïve to neglect employees as a possible malicious threat, but in principle users are not the enemies within. To make use of the this resource, employee participation is regarded an important principle in all organizational processes.

1.2 Socio-technical information security system

”If you think technology can solve your security problems,
then you don’t understand the problems and you don’t understand the technology”
Schneier (2000:.xii)

This thesis is founded on a premise that the technical and the social sides of information security work are closely interrelated to each other, i.e. a socio-technical system. A socio-technical information security system is created by elements of all information security processes and the interplay between these elements: technological solutions; policies; guidelines and instructions for individual and organizational behaviour; methods and tools; the role and responsibilities of information security professionals; individuals’ behaviour, awareness, expectations and experiences; and collective norms and values; and interactions and relations between individuals and groups. These related factors produce a web of technological and non-technological elements that per definition should create a secure, reliable and available information system. A socio-technical approach to information security has been lacking, as information security research has been fragmented, i.e. several disciplines acting independent of each other, and has not addressed security problems holistically by interdisciplinary efforts (Siponen and Oinas-Kukkonen, 2007).

The socio-technical school has its roots back in the 1950s, e.g. the study of the outcomes of technological development in British coal mines by Trist and Bamforth (1951) that showed that technical and social systems are closely linked. They explain that incompatibility between demands created by technology and what is beneficial for workers’ situation do not create improved performance. This study was followed by several socio-technical studies (Trist, 1981), which have had a major influence on democratic traditions in Scandinavian organizations as well as participative approaches to organizational development and safety management in the Scandinavian countries (Greenwood and Levin, 1998; Levin and Klev, 2002; Hovden et al., in press)

Socio-technical theory emphasizes the development of humane working conditions and realizes ideas of participation and democracy. Socio-technical theory proposes a number of different principles for handling technical and social aspects of an organization as inseparable elements (Trist, 1981): joint optimization of technology and social organization; man as complementary to the machine; man as a resource to be developed;

optimum task grouping; self regulation subsystems; redundancy of functions; flat organization chart, participative style; collaboration; purposes of member, organizations and society; commitment; and innovation. These principles were efforts to break away from mechanical organizational views based on Taylor's scientific management (1911). Several of these socio-technical elements are discussed throughout the thesis.

This study is not a systematic socio-technical study. It is not mentioned explicitly in the papers that the studies are socio-technical, neither is the study based on an inter-disciplinary approach since it does not consider technological aspects. However, the socio-technical line of thinking is a basic foundation of this thesis, i.e. that technology, individuals and organizational factors and the interactions between them contribute in combination to the information security performance of an organization. One element in the socio-technical system or its interaction with another element can for example explain the success or failure of another element.

1.3 Individual behaviour created by organizational factors

> *"Today, neither investigators nor responsible organizations are likely to end their search for the causes of an organizational accident with the mere identification of sharp-end human failures. Such unsafe acts are now seen more as a consequence than as principal causes"*
> Reason (1997:10)

One can often see news articles giving examples of information security breaches caused by poor user behaviour or insufficient awareness (it must be assumed that these incidents only represent the tip of the iceberg), for example:

- *Incautious use of email:* before made public, a budget was accidentally sent to a newspaper rather than to the correct receiver, a public agency[1]
- *Lost mobile equipment:* At Oslo Airport, the lost property office receives about three computers every day[2]
- *Finger mistake:* A stock broker accidentally typed wrong numbers and unintentionally bought stocks for NOK 40 million, which were later sold with a loss of NOK6 million[3]

[1] http://www.vg.no/pub/vgart.hbs?artid=116162
[2] http://www.dagensit.no/min-it/article864669.ece
[3] http://e24.no/arkiv/article659858.ece

- *Sensitive information made public available*: The Norwegian National Security Authority found both trade secrets and security-graded information in Facebook profiles of members of public agencies in Norway[4]

These examples are mainly unintended acts. In addition, there are security incidents that are founded on employees being tricked. Mitnick and Simon (2002) give several examples of how social engineering can be used to attack information systems, i.e. hackers use social techniques to manipulate people into performing actions or give away confidential information. In a similar way phishing attempts and Nigerian fraud approaches are based on tricking people to perform actions they should not be doing. Furthermore, malicious acts of legal users of a system are a major threat to information security. Gordon et al. (2005) show that about half of reported computer crime incidents in the US are created by insiders, e.g. abuse of net access; unauthorized access to information; sabotage; theft of software or equipment and fraud.

These examples indicate that users can be a possible threat/vulnerability for the information security level either by deliberate or accidental incidents or by being tricked to create information security breaches. Blaming users for these incidents would be to go back to the mindset of the occupational and industrial safety discipline 20-30 years ago, when individual failures were emphasized as the main cause of many accidents (Reason, 1997). Blaming the operator rather than the technology or organizational aspects has a long history in the analysis of failures and accidents. Human failure is often the first and the most common attribution when accidents occur, such as the Chernobyl catastrophe, airplane disasters and major train accidents. Rather than giving the blame to the operator, one should ask what in the system made it easy for operators to make mistakes? (Reason, 1997; Perrow, 1999; 2007). This thesis follows the same basic idea: *individual information security acts (both normal operation and when creating security breaches) are generated by various factors in technology, at the local workplace and in the organization.* This statement needs some clarifications.

First, this does not imply that I neglect the fact that some employees have incentives to get some sort of gain by malicious acts. However, it is technological and organizational

[4] http://pub.tv2.no/nettavisen/innenriks/ioslo/article1315514.ece

vulnerabilities that create windows of opportunities to carry out malicious acts. For example lack of organizational information security measures (mainly lack of segregation of internal control) made it possible for Nick Leeson, a trusted General Manager at Barings Banks, to exploit the substandard information security systems to do unsupervised speculative trading thus making large personal profits, that finally caused the collapse of Barings Bank, the United Kingdom's oldest investment bank in the early 1990s (Reason, 1997; Dhillon, 2001b). Second, human behaviour is by nature unreliable (Rasmussen, 1982). Proper barriers must thus be in place to prevent information security incidents. Barriers are here understood as physical and/or non-physical means planned to prevent, control or mitigate undesired events (Sklet, 2006). The barriers can take many forms (Hollnagel, 2004) ranging from physical (prevent an action to be carried out); functional (impeding the action to be carried out, e.g. password authentication); symbolic (interpretations required in order to act, e.g. warning messages and interface layout); and incorporeal (the barriers are not physically present, but depend on the knowledge of the user in order to achieve its purpose, e.g. rules, guidelines and security norms and values). Poor quality or lack of one or more of these barriers creates possibilities for information security breaches were human acts can be the source of ignition. Having these barriers in place is managerial responsibility, not a user responsibility; consequently users cannot be blamed for making accidental incidents. Third, user's information security behaviour is normally preventive rather than dismal. Such normal behaviour is generated by a number of contextual factors which is further elaborated in Section 2.2.

1.4 Users as a resource in the information security work

> *"Users have to be treated as partners in the endeavour to secure an organization's system, not as the enemy within. System security is one of the last areas in IT in which user-centred design and user training are not regarded as essential – this has to change."*
>
> Adams and Sasse (2005:45)

As shown in Section 1.3??, many security incidents are caused by unsafe acts of employees in combination with basic causes in technology or the organization. On the other hand, employees function as important resources in preventing, detecting and reacting to unwanted incidents, given that they are appropriately informed and trained. Employees might be a resource for the systematic information security efforts of an organization by simple, no time-consuming actions such as:

- locking the computer when they are absent from it
- good password etiquette
- cautious use and transportation of mobile equipment
- cautious use of email and email addresses
- cautious use of the Internet
- cautiousness at home offices
- not using unlicensed software
- not distributing confidential, internal, sensitive or private information to people it is not relevant for
- reporting incidents and vulnerabilities or suspicion of these

In the safety research domain, resilience engineering (Hollnagel et al., 2006) has emerged as an innovative and new way to think about safety. This approach argues that safety is a core value, not a commodity that can be counted – safety is revealed by the events that do not happen. A key issue here is foresight – the ability to anticipate changing shapes of risk before failure and harm occurs. This is in contrast to the traditional reactive approach driven by events that have happened. This school of thought further argue that "success belongs to organisations, groups and individuals who are resilient in the sense that they recognise, adapt to and absorb variations, changes, disturbances and surprises". Consequently, the dynamics of normal operation becomes an important loss prevention process (Rasmussen, 1997). In addition, incidents are interpreted as unexpected combination of normal performance variability. *Viewing users* *as an important security resource is linked to this focus on normal operation* rather than hindsight on how and why incidents occur. The bulleted actions above are normal operation and even common sense/good manners, rather than complex, time-consuming security actions, and could easily be integrated into regular work tasks.

A good question here is whether it is necessary at all for users to consider the actions bulleted above. I would say no, in the sense that there are technological defences-in-depth that will prevent most security breaches to escalate if the actions above are not followed. On the other hand, the answer is yes for several reasons. First, poor quality of the actions can ignite external attacks (e.g. password in the wrong hands) or open vulnerabilities (e.g. download an unlicensed program containing malicious code). Second, many of the actions are protecting the public image of the organization (e.g. cautious handling of sensitive information). Third, reporting incidents and insecure conditions is an important principle in systematic information security management.

The belief in employees as a resource is closely linked to organizational democracy and employee participation. The belief in employees as a resource is also one of the major factors underpinning action research (e.g. Greenwood and Levin, 1998) and theories in organizational change and development, (e.g. Levin and Klev, 2002). These related research domains focus on involving members of organizations or local communities in collaboration with experts aiming at altering the initial salutation. Furthermore, this belief is influenced by the socio-technical school by it focus on change and innovation and the belief in involving employees in change processes. In such processes, employees get a chance to influence and shape their own working conditions, and thus realizing organizational democratically values. A participative democracy is based on a belief that only through participation can individuals develop the unexploited capacities inherent within them (Greenberg, 1975). As a result of the belief in users as a resource in the information security work, combined with a socio-technical framework, *participation is a presumption for managing users throughout the thesis*

1.5 Delimitations

Every organizational member using a computer is a user independent of knowledge, skills, authority and the situation they use the computer. As a result there are many different kinds of users. This study concentrates on users that are employees in an organization and their use of computers when working. The studied employees have no particular information security expertise. It is studied how users operate at a daily basis in interplay with other organizational members, technology and organizational structures and norms, i.e. *normal proactive operation rather than a reactive view on critical actions crating incident*s. I thus assume that employees in principle not are enemies within, but rather are important resources in the information security activities in an organization.

The thesis does not deal extensively with the technological aspects of information security. However, it is difficult to avoid mentioning the technology in a mainly technological field of research and practice. The technology is important to information security, and must not be forgotten although it has a minor part of this thesis.

There are a lot of information security means, methods and processes, which can be technological, formal or informal. This thesis concentrates on different types of measures directed at users, i.e. aiming at improving and maintaining the quality of users' awareness and behaviour

The notion information security culture is not used in the thesis. This does not imply that there is no such a thing as an information security culture or that I neglect the cultural factors. The reason that it is left out is that information security culture is a difficult and foggy concept, with many interpretations and approaches. Information security culture is a hot topic in information security work, but also one that creates confusion. "Although many researchers have identified the importance and the need for an information security culture in organisations, few have established a clear and definitive meaning to the term 'security culture'"(Koh et al., 2005:4). While culture is a new concept in the information security field (Ruighaver et al., 2007), it has been around for a time in the industrial safety domain. As for information security culture, it is unclear what safety culture is, and is often understood with several elements (Cox and

Flin, 1998; Hale, 2000; Guldenmund, 2000). It is also claimed that it is difficult to operationalise and measures safety culture. A solution to this problem has been to study safety climate, i.e. a descriptive measure reflecting a workforce's perception of the organisational atmosphere. Similar to safety culture, safety climate includes a wide range of features in current literature (Flin et al., 2000). Instead of using information security culture as an umbrella term for many different organizational and individual aspects, I call these aspects by name.

1.6 Some central concepts

Some central concepts used in the thesis need to be described, some of them are discussed more thoroughly later in the thesis. These are not definitions but my understanding of the concepts.

Information security is traditionally defined as preserving the confidentiality, integrity and availability of information (e.g. ISO/IEC 27002). This thesis understands information security as something more than securing technological solutions, and includes both individual and organizational aspects as important measures and processes that create security.

Information security management is understood as the total of activities conducted in a more or less coordinated way to control threats and vulnerabilities that in some way involves users. This includes both administrative routines and guides informal processes.

Users are in the thesis are understood to be employees with legitimate access to an organization's information systems.

Information security awareness. In the information security field one most often talk about individual awareness, rather than individual attitude and knowledge. ISF (2005) defines information security awareness to be the extent to which organizational members understand the importance of information security; the level of security required by the organization and their individual security responsibilities; and act accordingly. Siponen (2000:31) refers to information security awareness as "a state where users in an organisation are aware of – ideally committed to - their security mission (often expressed in end-user security guidelines)”. Individual information security awareness is thus a combination of attitude to and knowledge of information security. The definitions above also link awareness to obedience to the information security requirements. In this thesis information security awareness is understood as individuals’ information security attitudes and knowledge, independent of organizational requirements.

Behaviour – individual actions. This thesis considers individual behaviour to be influenced by many factors in the organizational context.

Individual performance, the result of individual action or inaction.

1.7 Structure of thesis

The thesis consists of two main parts: Part I: Main report and Part II: Papers, see Figure 1.

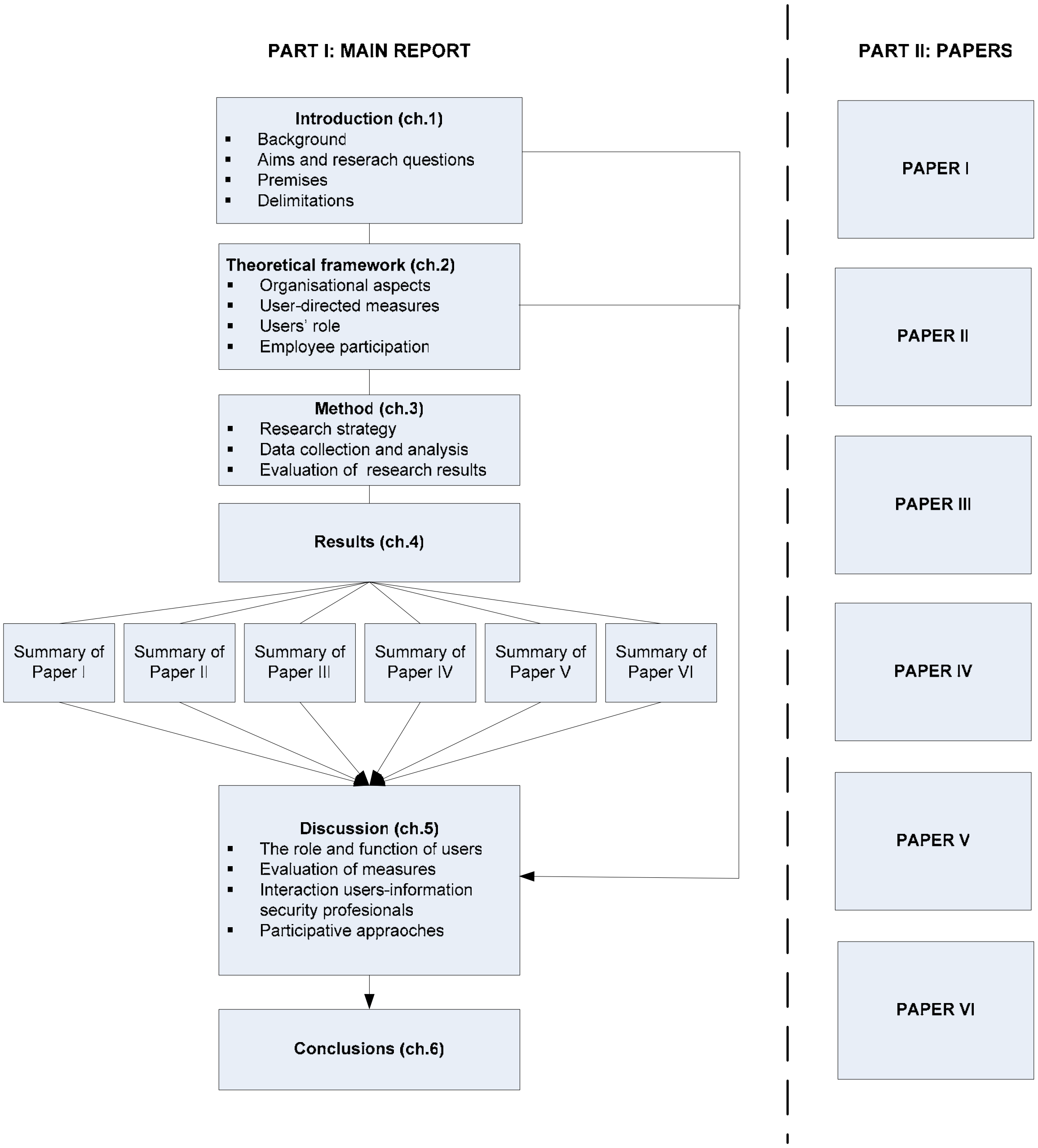

Figure 1. Structure of thesis: main part and papers

The main report puts the pieces together and is based on the findings of the papers. Part II consists of the following research papers published in or submitted to international journals or conference proceedings:

- PAPER I: A qualitative study of users' view on information security.
- PAPER II: Information security digital divide in organisations: information security managers versus users.
- PAPER III: Improving information security awareness and behaviour by a user participative approach: an intervention study.
- PAPER IV: Implementation and effectiveness of organisational information security measures.
- PAPER V: User participation in information security.
- PAPER VI: Industrial safety management and information security management: risk characteristics and management approaches.

The following papers and book chapters have also been published during the PhD study, but are not included in this thesis:

- Albrechtsen, E. (2002). "A review of the insider threat to organisations' information security level" In Kufås, I. and Mølmann, R.A. (eds.) *Informasjonssikkerhet og innsideproblematikk.* [Information security and insiders]. NTNU report ROSS(NTNU)200301
- Albrechtsen, E. (2004). "Handling of uncertainty, complexity and ambiguity related to IT risk." In proceedings of the *13th EICAR Annual Conference*, Luxembourg, May 2004.
- Albrechtsen, E. and Grøtan, T.O. (2004). "Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner", in Norwegian [Old-fashioned thinking in modern organizations? On information security in knowledge organizations]. In Lydersen, S. (ed.), *Fra flis til fingeren til ragnarokk,* Trondheim: Tapir Akademisk forlag, pp.335-355
- Albrechtsen, E. (2005). "Informasjonssikkerhet i et sluttbrukerperspektiv", in Norwegian [Information security in a user perspective]. In proceedings of *Norsk konferanse for organisasjoners bruk av IT (NOKOBIT)* [Norwegian conference on organizations' use of IT], Bergen, Norway, November 2005.
- Albrechtsen, E (2005). "Innledning: perspektiver på informasjonssikkerhetsarbeid", in Norwegian [Introduction: perspectives on information security work]. In Nordby, Y. and Waale Hanse, C., *Informasjonssikkerhet – atferd, holdninger og kultur* [Information security – behaviour, attitudes and culture] NTNU-report ROSS(NTNU)200504

- Albrechtsen, E., Grøtan, T.O. and Hovden, J. (2006). "Ethical issues in information security management". Extended abstract presented at *the European Conference on Computing and Philosophy (ECAP'06)*, Trondheim, Norway, June 2006.

- Line M.B., Albrechtsen E., Johnsen S.O., Longva O.H. and Hillen, S. (2006). "Monitoring Incident Response Management Performance". In proceedings of *the International Conference on IT Incident Management & IT Forensic*s, Stuttgart, Germany, October 2006.

Various parts of the findings of the PhD study have been presented in the following national popular scientific talks:

- "Hvordan kan organisasjonen påvirke informasjonssikkerheten?" [How can organizational aspects influence information security?]. Presented at the Norwegian Business and Industry Security Council's (NSR) annual conference in October 2003.

- "Hvordan kan organisasjonen påvirke informasjonssikkerheten? - i et sikkerhetsledelses perspektiv" [How can organizational and management aspects influence information security?]. Presented at ISACA Norway Chapter's Christmas Conference in December 2003.

- "Sluttbrukere om informasjonssikkerhet" [Users' on information security]. Presented at the Norwegian National Security Authority's (NSM) annual conference in November 2005.

- "Informasjonssikkerhet og ansatte"[Information security and employees]. Presented at the Norwegian Business and Industry Security Council's (NSR) annual conference in September 2006.

- "Om mus og menn." [Of Mice and Men]. Presented at the Safety Days at NTNU (Sikkerhetsdagene ved NTNU) in October 2006

- "Brukere som ressurs i arbeidet med informasjonssikkerhet" [Users as a resource in the information security work]. Presented at the workshop 'Workers as a resource in information security' at Gjøvik University College in October 2006

2 Theoretical framework and research literature on information security management of employees

The thesis is built on a theoretical framework of three research domains: 1) information security research, 2) industrial safety research; and 3) general organizational theories and research. Although there is some literature research on non-technological information security and the role of users, more research is asked for on the human part of information security (Schultz, 2004; 2005). In an extensive literature review on information security research contributions, Siponen and Oinas-Kukkonen (2007) show that information security research has been dominated by technical contexts and issues such as access and secure communication based mathematical approaches. They further argue that more information security research is needed that is based on other reference theories such as psychology, sociology and philosophy. To supplement a theoretical framework (to be used in Chapter 5 Discussion) on users' role in information security management, experience from industrial safety research and general organizational theory is used in this thesis. The field of information security and industrial safety has an important similarity which makes experience transfer possible: both concern loss prevention. Furthermore, the field of industrial safety is much more mature in socio-technical approaches, which extend the learning feasibility. When discussing participation another safety area is looked into: occupational accident prevention management, which has a long tradition in involving and collaborating approaches to loss prevention. The relationship between information security management and industrial safety management is discussed in Paper VI. General organizational theory is used to understand processes in organizations affecting information security and the function of users.

The non-technological side of information security, has been dominated by formal, technical-administrative approaches (Dhillon and Backhouse, 2001), e.g. policies and instructions for expected behaviour. However, during the last few years there has been an increased emphasis on informal aspects of information security as an addition to formal aspects. Both research and practice has turned their attention to individual awareness and behaviour (e.g. Besnard and Arief, 2004; Adams and Sasse, 2005;

Stanton et al., 2005) as well as the concept of information security culture (e.g. von Solms, 2000; OECD, 2002; Ruighaver et al., 2007)

This chapter starts with a short overview of external factors influencing the organizational work concerned with the human part of information security. Then organizational aspects that are relevant for individual information security performance are presented, followed by a brief look at information security management approaches directed at users. Subsequently, different views on the information security role of employees at the sharp-end are presented before ending the chapter with theoretical arguments for employee participation.

2.1 External factors

Figure 2 models risk management in a dynamic society (Rasmussen, 1997). It shows that many levels of politicians, managers and work planners are involved in the control of hazards and threats by means of laws, rules and instruction. At the bottom of the model one finds sharp-end practice, i.e. the information security performance of users without management responsibility and no information security expertise. At the top, society seeks control through the legal system, by laws and regulations. In Norway, there are several regulators concerned with information security (Bogen, 2005). Some of these authorities are cross-sectoral: the Norwegian National Security Authority, The Data Inspectorate and the Norwegian Post and Telecommunications Authority. Additionally, there are sector-based authorities regulating information security, e.g. the Financial Supervisory Authority of Norway, The Directorate for Health and Social Affairs, and The Petroleum Safety Authority Norway. These public authorities regulate information security by laws, inspections, advisory services and stimulation. At the same time they are dependent on input from the lower parts of the model to decide how they should regulate information security. The rules and regulations have to be interpreted in the context of a particular company and implemented by means such as policies, plans and measures, which directly influence work at the sharp end. This top-down approach shows that regulations of public authorities frames how companies organize their information security work, and thus indirectly influences user performance. At the same time, the model shows that bottom-up approaches are also essential. Higher levels need input on actual performance at the lower levels to adjust and implement security means and measures to the actual context.

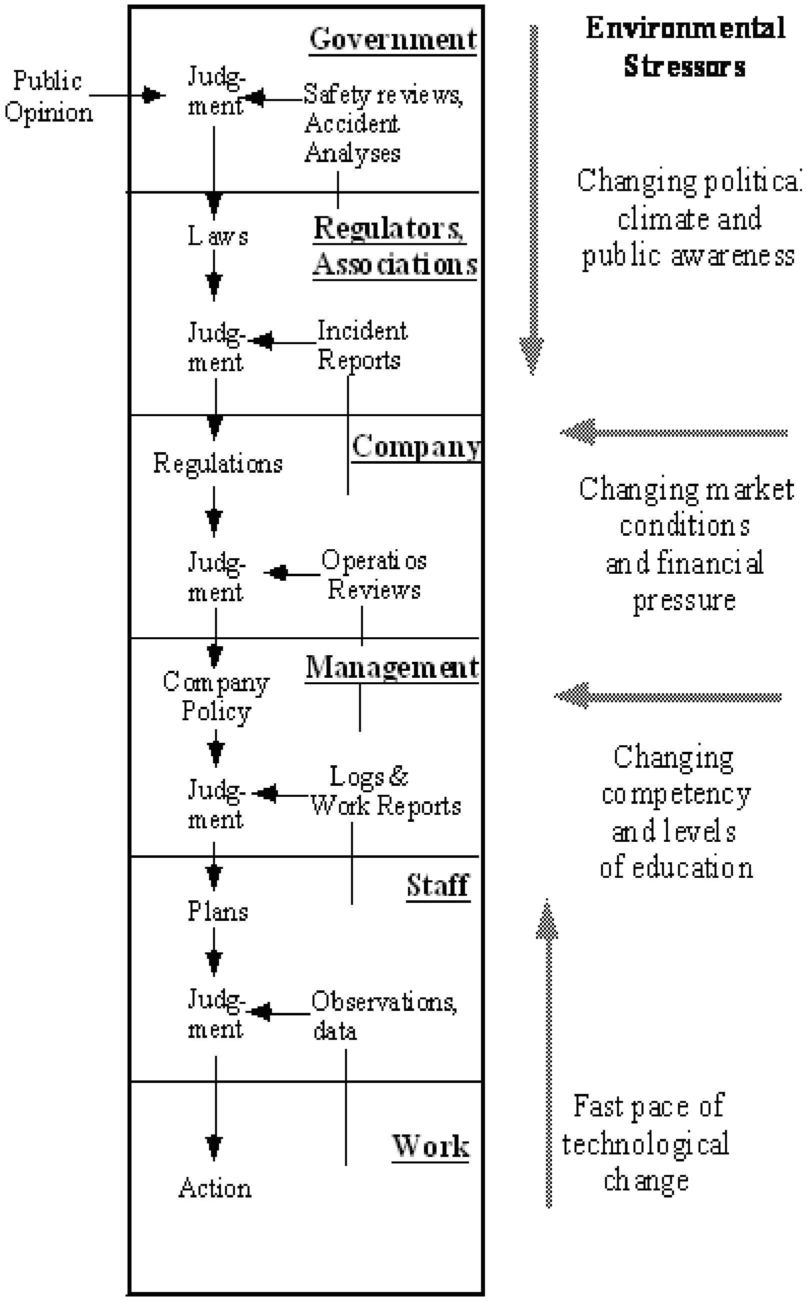

Figure 2. The socio-technical system involved in risk management in a dynamic society (Rasmussen, 1997)

The model also illustrates how environmental dynamics in society influence information security work at all levels in society. Technological change is of course an essential dynamic of information security: use of new software and hardware; new vulnerabilities in software; trends of use (e.g. Facebook); converging technologies; and coupling of systems. Differences in competency are also creating changes, in particular the difference in experience, knowledge and skills between old and young employees. Soon a new generation of workers, who have used the Internet and computers from pre-school age will enter the work market - what security challenges do this group of workers represent? Market conditions and financial pressures also generate environmental stressors: e.g. technology-driven organizational development and automation but also malicious acts such as industrial espionage. Public awareness and the political climate also influence risk management in society, e.g. by emphasis on terrorism but also on vulnerabilities in technology regarding for example air traffic control or the power supply.

This thesis focuses on the lower parts of the model. But as shown in Figure 2 these parts are not operating independently of other parts in a society.

2.2 Organizational aspects of information security

Organizational aspects of information security include formal technical-administrative measures as well as informal activities. The field of information security has traditionally mainly been directed towards technological problems and solutions, and has not paid attention to socio-organizational and human aspects (Dhillon and Backhouse, 2001). The administrative approach to information security has mainly been structured around legal regulations; public guidelines and standards such as ISO/IEC 27002 Code of practice for information security management; documented policies and procedures for individual and organizational behaviour; control and monitoring; and distribution of privileges, all controlled by powerful information security professionals (Albrechtsen and Grøtan, 2004). However organizations can be understood as more than a formal-technical system (Morgan,1998; Bolman and Deal, 2003), and include subjects such as politics and power, changes, human resources and culture. In a socio-technical perspective, formal and technological systems are influenced by the social life of an organization and vice versa.

As argued in Section 1.3, individual information security performance is influenced by technological and organizational factors. Leach (2003) describes two aspects in the organizational context that generates individual behaviour: 1) the individual's understanding of what behaviour is expected of staff (generated by the individual body of knowledge; behaviour demonstrated by senior management and colleagues; and the user's security common sense and decision-making skills) and 2) the user's willingness to constrain their behaviour to stay within accepted norms (generated by personal values and standards of conduct; psychological contract with their employer; and the effort for compliance, and temptations not to comply). In a survey regarding security-related behaviour of PC users, Frank et al. (1991) suggest a theoretical model of three factors influencing security behaviour: 1) motivation (perceived personal responsibility and impact of loss of files), 2) role clarity (informal norms and formal policies) and 3) ability (experience and knowledge). The factors described by Leach (2003) and Frank et al. (1991) are mainly centred on personal abilities. However, Dhillon (2001a) classifies three principles for managing information security that also influence individual information security behaviour: pragmatic aspects; formal rule-based aspect and technical aspects.

With the factors mentioned in the paragraph above as a basis, Figure 3 shows how individual information security behaviour can be explained by a number of organizational aspects. The model is adapted and adjusted from the analytical approach of an investigation of a gas blow out on an installation in the North Sea (Schiefloe and Vikland, 2006), which is a development of a general model of analysis of social phenomena by Schiefloe (2003). The model has many similarities to organizational diagnosis models (e.g. Weisbord, 1978; Irgens Karlsen and Veium, 1986), which are widely used in the organizational development field. However, in these models individual performance is substituted by organizational performance and processes. These models additionally include organizational aims as an element since the diagnosis process is based on comparison to this goal. The model in Figure 3 can be extended by the goal element and used as a diagnostic tool as well.

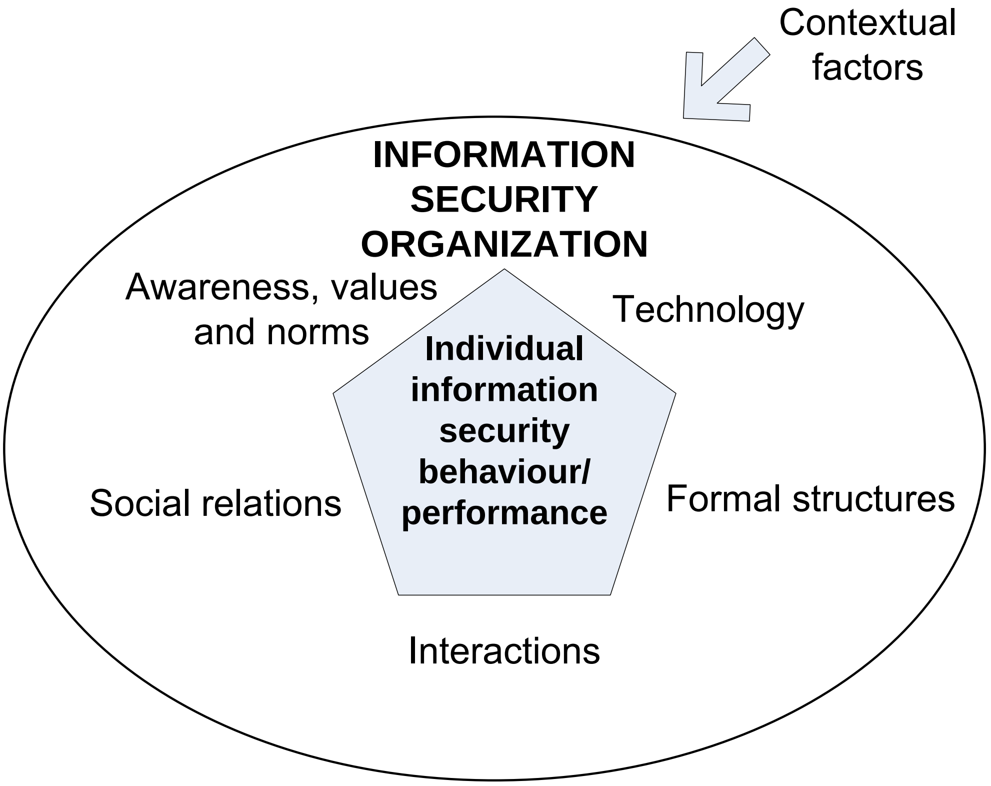
Contextual factors
INFORMATION SECURITY ORGANIZATION
Awareness, values and norms
Technology
Individual information security behaviour/ performance
Social relations
Formal structures
Interactions

Figure 3. Pentagon-model: individual information security performance created by different information security aspects in the organizational context. Adapted and adjusted from Schiefloe and Vikland (2006)

The model illustrate that information security behaviour and thus individual performance (performance is the result of the behaviour, i.e. action or inaction) is influenced by a set of organizational aspects: formal systems; technology; values and knowledge in the organization; interactions; and social relations.

- *Technology* is of course an important factor for information security behaviour, i.e. all kinds of technological security solutions, e.g. access control.
- *Formal structure* covers the formal distribution of responsibility and tasks and steering documents such as policies and instructions
- *Interactions* concerns how individuals and groups cooperate, communicate and coordinate their actions with each other. How management is performed is an important ingredient of this dimension
- *Social relations* are about social networks, collegial conditions and professional divides. Keywords are trust and access to knowledge and experiences.
- *Awareness, values and norms* (the origin of the model uses the notion culture for this element, which I find misleading since culture also concerns aspects such as

interactions, relations and even formal structures) both individual and shared with others play an important role and are closely related to behaviour. These are important factors concerning how people interpret situations and chose their actions, thus influencing work practices and norms. The attributes are influenced and maintained by formal structures, interactions and relations.

- *Contextual factors* influence the organizational and technological information security attributes such as: other organizational processes and requirements, technological development; legal requirements; and standards. See also Figure 2.

These organizational attributes create a space of guidance, possibilities and limitations for behaviour. The dimension are not independent of each other, they are closely connected and influence each other. For example interactions are creating relations, and the interactions reflect the relations of an organization. There is thus a continuous interplay of factors that generate social processes; in this case individual information security performance.

The model describes information security as a socio-technical system that considers and combines both theory-in-use (lower part of figure) and the espoused theory (upper part of figure) (Argyris and Schön, 1996) in addition to the essential security technology. This linkage of individual behaviour to organizational and technological factors makes the model a good starting point for the current treatise of understanding the role and function of employees in information security and how to manage accordingly, as it makes it possible to explain individual behaviour systematically by technological, formal and informal processes.

2.2.1 Organizational information security measures

Standards and public guidelines for information security management, e.g. ISO/IEC 27002 (former ISO/IEC 17799), provide a wide range of different organizational information security measures. These planned information security activities are recognized as the formal structures of the pentagon model in Figure 3. The measures can be categorized into four groups (see Paper IV):

- The *security policy* is the foundation of any security regime. It specifies the strategies behind an organization's information security approach by a written document, directly linked to the overall policies of the organization

- *Procedures and control* are directly derived form the security policy. This group of measures consists of documents guiding individual and organizational behaviour such as user instructions, security plans and non-disclosure agreements, as well as controls and follow-up activities of the documented systems e.g. by audits.
- *Administrative tools and methods* are both proactive and reactive means such as risk analysis, asset classification, reporting systems and incident handling systems.
- Creation and maintenance of *security awareness* that include both individual and collective activities

These non-technological information security measures are studied in Paper IV. Most of these categories of measures influence employees in some way, particularly the awareness group of measures. These measures are thus important tools for managing the human part of information security.

2.3 Information security management of employees

There are many understandings about what management is as well as many practical ways of performing management. Levin and Klev (2001) argue that management can be understood by two concepts; administrating routine tasks and leading/guiding organizational processes. Information security management of employees thus concern selection, implementation and follow-up of formal and technological information security solutions directed at users, but also about informal organizational processes, e.g. the engagement of managers in information security; employee participation; politics and power; trust; and decision-making processes. As a result *managing the human part of information security concerns the totality of activities conducted in a more or less coordinated way to control threats and vulnerabilities that in some way involves users*, i.e. processes related to all elements in Figure 3. Information security management of employees is thus based on principles for dealing with pragmatic, formal rule-based and technological aspects of an organization (Dhillon, 2001a).

Human barriers are more unreliable than technological measures (Rasmussen, 1982), which imply challenges for information security management of users: what measures should be used to successfully influence users' behaviour and awareness? Generally speaking, measures directed at individuals can be categorized into modifications of work conditions, modifications of skills and knowledge (education and training); modifications of attitudes (information campaigns); modifications of behaviour (rewards and sanctions); and selection of personnel (Rundmo, 1990). There is a sequence of ordering between these categories. First, change the preconditions in the working environment to be satisfactory for secure behaviour. If this is not sufficient, educate workers. If education is insufficient, inform employees in order to improve attitudes. If information is not satisfactory, modify behaviour by sanctions and rewards. Selection of employees is the final solution to deal with employees. Figure 4 illustrates different information security measures directed at individual (based on Rundmo (1990); Hovden et al. (1992); Aarø and Rise (1996); Voss (2001); Hubbard (2002); and Lund and Aarø (2004))

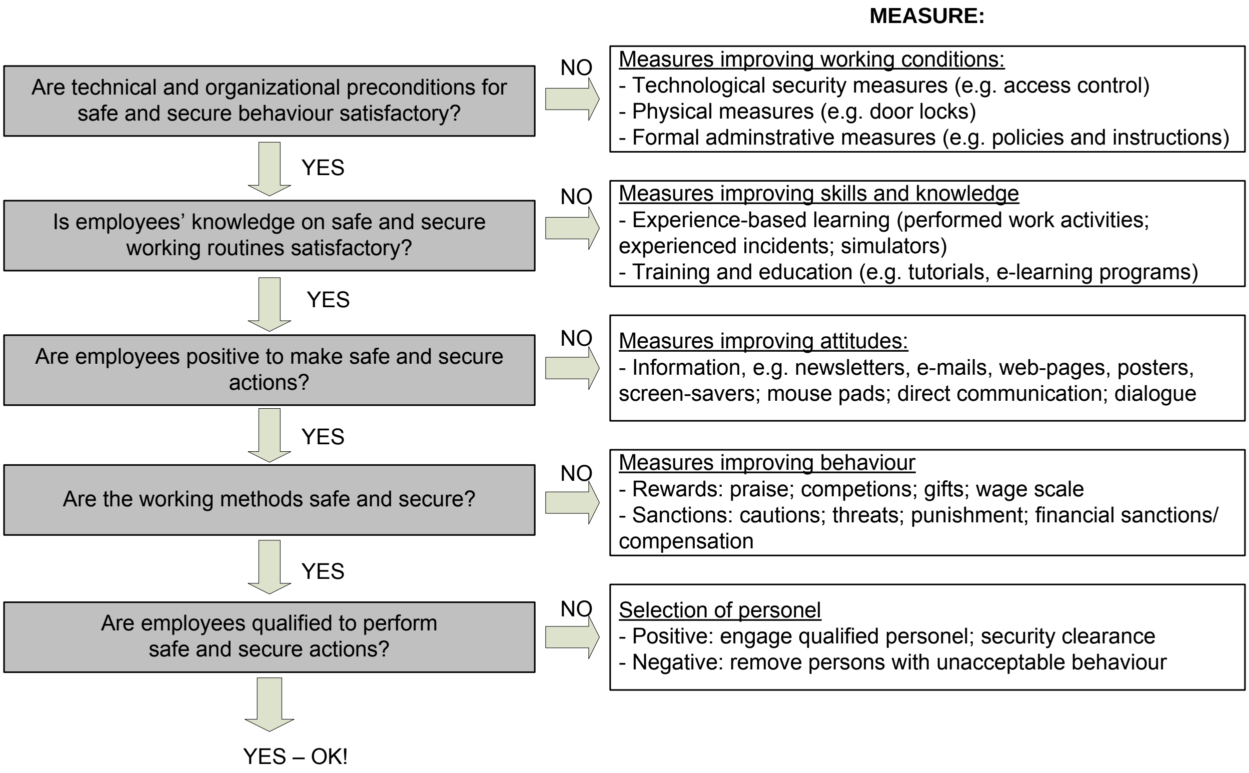
MEASURE:
Are technical and organizational preconditions for safe and secure behaviour satisfactory?
NO
Measures improving working conditions:
- Technological security measures (e.g. access control)
- Physical measures (e.g. door locks)
- Formal adminstrative measures (e.g. policies and instructions)
YES
Is employees' knowledge on safe and secure working routines satisfactory?
NO
Measures improving skills and knowledge
- Experience-based learning (performed work activities; experienced incidents; simulators)
- Training and education (e.g. tutorials, e-learning programs)
YES
Are employees positive to make safe and secure actions?
NO
Measures improving attitudes:
- Information, e.g. newsletters, e-mails, web-pages, posters, screen-savers; mouse pads; direct communication; dialogue
YES
Are the working methods safe and secure?
NO
Measures improving behaviour
- Rewards: praise; competions; gifts; wage scale
- Sanctions: cautions; threats; punishment; financial sanctions/ compensation
YES
Are employees qualified to perform safe and secure actions?
NO
Selection of personel
- Positive: engage qualified personel; security clearance
- Negative: remove persons with unacceptable behaviour
YES – OK!

Figure 4. Information security measures directed at users.

Lund and Aarø (2004) have argued that programmes combining different kinds of measures, i.e. information campaigns, education, rewards, technological/physical measures, legislation, and enforcement, have the most positive effect on risk behaviour. In that way the effect on security behaviour is larger than the sum of the effects of the single measures. As a consequence, there are many different measures that influence user behaviour and awareness.

2.4 Employees in information security management

Everyone involved in IT systems are users. Organizations are diverse and individuals are different, there are thus many kinds of user roles in information security. In this thesis, the focus is on employees with no management authority and no expertise in either information security or in information technology, i.e. the most common user role in most companies. Sharp-end users do not operate alone in the organization. Figure 5 shows different roles in information security management (based on Rosness, 2001). Here we find operators at the sharp-end and strategic planners and designers at the blunt end, removed from operation, threats and hazards at the sharp end. Line managers and top managers are found in middle between strategic planners and operators, but with higher level of authority. The interplay of blunt end and sharp end is discussed throughout the thesis, but it does not consider all roles in Figure 5 extensively.

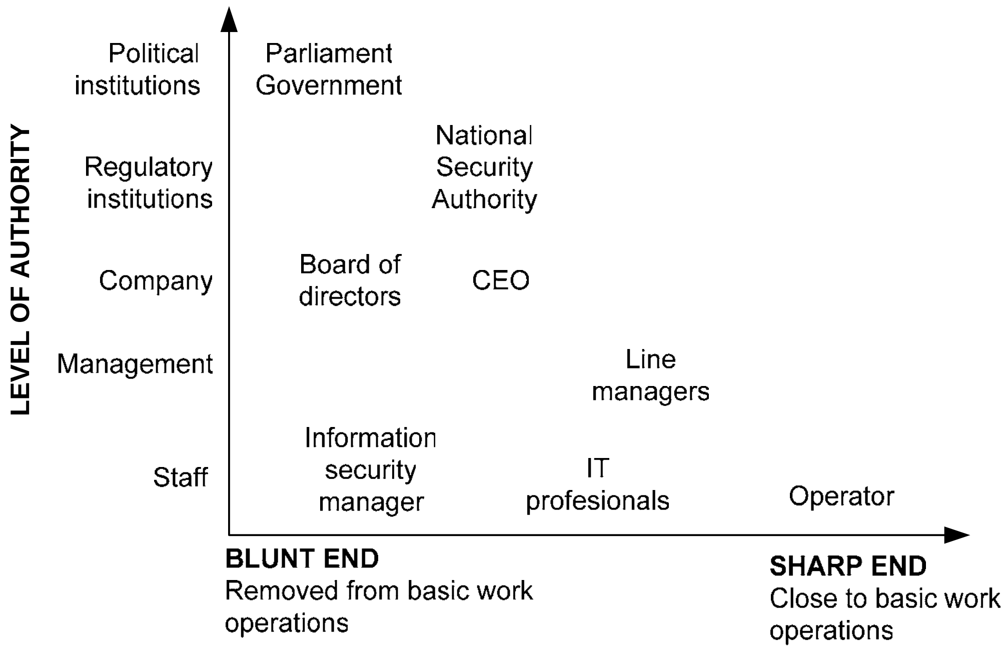

Figure 5. Two dimensions characterizing the setting for different information security roles (adapted and adjusted from Rosness, 2001).

There are three main groups of information security research on sharp-end activities (Stanton et al., 2005):

- Studies of human-computer interfaces concerning usability of security systems
- Studies of counterproductive computer usage

- Studies of human and organizational aspects related to individual behaviour

This thesis looks mainly at the last point. A brief overview of the other two is presented in this section.

2.4.1 Human-computer interaction studies

Computer security systems should not only preserve security, they should also be usable for users without expert knowledge in security. However, security systems often fail to consider both requirements (Furnell, 2005). For example, "many users will be familiar with seeing pop-up dialogs in their web browser asking them whether or not they wish to trust a particular certificate. However, given that only a substantially smaller proportion of such users are likely to know what a certificate actually is, many will be forced to make an arbitrary decision based upon their desire to access the site concerned" (Furnell, 2005:275).

To deal with the security vs usability problem of human-computer interfaces, human-factor approaches that aim at simplifying and rationalizing user interfaces of security-related systems has been carried out by researchers including Johnston et al. (2003) and Furnell et al. (2006). They identify the following key criteria to improve the usability of security systems: present options and descriptions in a manner that is meaningful for users; give an indication of whether security is being applied in the system; present features that users should be able to find when they need them; display only relevant information for the users; help users recognize, diagnose and recover from errors; ensure that the system should be easy to learn for the user; and remember that the system should help users.

2.4.2 Employees: the enemy within?

It is widely assumed that a remarkable portion of information security breaches in an organization are carried out by its own organizational members (e.g. Shaw et al.,1998; Neuman, 1999; Magklaras and Furnell, 2001; Schultz, 2002; Whitman. 2003; Gordon et al., 2005). This insider threat is understood as people who have been given access rights to an information system and misuse their privileges, thus violating the information security policy of the organization (Theoharidou et al., 2005). Most of the research on the insider threat has concerned the malicious dimension by analysing types of and causes for incidents (e.g. Shaw et al. 1998; Dhillon and Moores, 2001; Dhillon, 2001b).

This focus on users as an important cause to incidents has led to a mindset of humans as the weakest link in the security chain. Sasse et al. (2001) argue that when users are labelled as the weakest link this implies that they are to blame. This can be recognized as the human-error mindset of the industrial safety domain 20-30 years ago. In this field it is now recognized that unsafe acts of employees are the consequences of local workplace factors and organizational factors (Reason, 1997).

The accidental dimension of user-created incidents has not been addressed adequately in the information security domain (Wood and Banks, 1993; Magklaras and Furnell, 2001). Kraemer and Carayon (2007) describe a conceptual model of human errors and violations of users that is divided into unintentional and intentional errors, and have done an interview study to shed light on the model. Their study shows that network administrators and security specialists view errors created by users to be more intentional than unintentional, while errors created by network administrators as more unintentional than intentional. Their findings thus reflect the main emphasis on the user as a malicious agent.

2.4.3 Information security user performance

Stanton et al. (2005) provide a six-element taxonomy of information security user behaviour based on two dimensions: intentionality and technical expertise, see Figure 6. The paragraph about the insider threat above, mainly addresses the 'intentional destruction', i.e. malicious acts requiring high level of expertise. There are however also malicious incidents that require minimal expertise: 'detrimental misuse', i.e. do harm through annoyance, harassment and rule breaking. There is also some grey scale behaviour with no intention to harm the organization's IT and resources, e.g. configure wireless access wrong, choose bad passwords and phishing attempts. To the right in the figure is behaviour with beneficial intentions. 'Aware assurance' refers to positive security practice conducted by well-trained users, while 'basic hygiene' requires no technical expertise but includes an intention to preserve and protect the organization's IT and resources, i.e. normal operation.

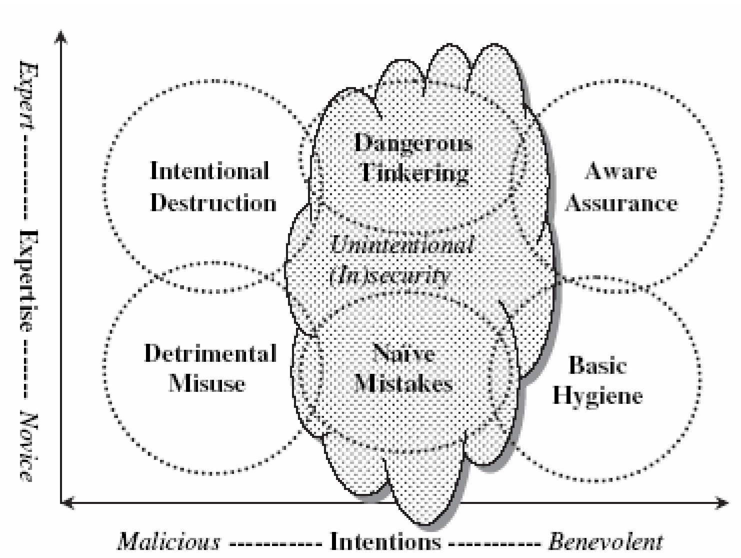
Expert ---------- Expertise ------- Novice
Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naive Mistakes
Basic Hygiene
Malicious ----------- Intentions ----------- Benevolent

Figure 6. Two-factor taxonomy of end user security behaviours (Stanton et al., 2005)

As argued in the introduction, the point of departure of this thesis is in the bottom right corner of Figure 6: 'basic hygiene'. *The users studied in this thesis are employees with no particular information security expertise who it is assumed wish to preserve the organization's security level. It is studied how users operate on a daily basis in interplay with other organizational members, technology and organizational structures* *and norms. I thus assume that employees in principle not are enemies within, but rather are important resources in the information security activities in an organization.* This does not mean that the malicious incidents are neglected. Other areas in the novice part of the expertise scale are covered indirectly, as poor basic hygiene is likely to create naïve mistakes and detrimental misuse.

Information security is one of many requirements in the working day of employees. Besnard and Arief (2004) and Post and Kagan (2007) show that users probably will overlook security if this allows them to ease their work when information security tasks are felt to inhibit the completion of their work tasks. Rosness (2001) shows that when there are goal conflicts between acceptable risk and functionality at the sharp end, individuals tend to put emphasis on efficient and least-effort work instead of loss prevention. When decision-makers are in a situation full of all kinds of different interests and demands, they are likely to choose a satisficing strategy (March and Simon (1958), i.e. they seek action that is good enough rather than choose the right alternative of action based on security considerations.

Rasmussen (1997) gives an explanation of possible consequences and causes of trade-offs by arguing that a systematic migration towards unacceptable risk performance is created by pressures towards efficiency provided by management and a gradient of least effort provided by operators. In addition, information security management functions as a counter gradient pushing the migration away from the boundary of unacceptable risk performance. This is illustrated in Figure 7, where pressures from economic efficiency, the human desire for least effort and security work creates migrating human behaviour within the space of boundaries of economic failures, unacceptable workload and unacceptable risk.

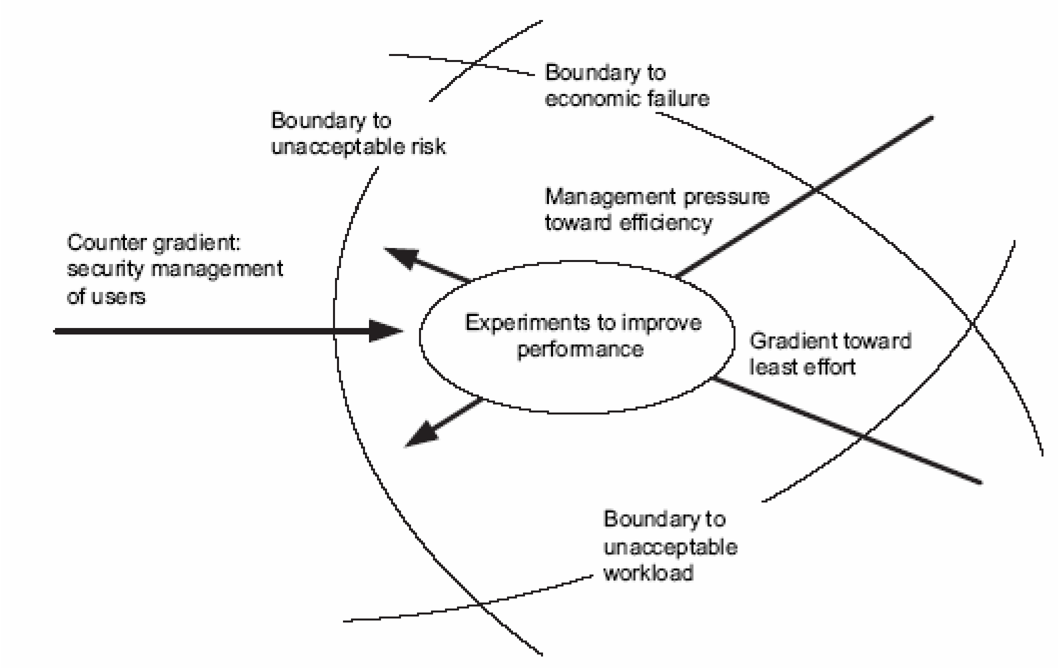
Boundary to economic failure
Boundary to unacceptable risk
Management pressure toward efficiency
Counter gradient: security management of users
Experiments to improve performance
Gradient toward least effort
Boundary to unacceptable workload

Figure 7. Under presence of strong gradients, behaviour is likely to migrate towards a boundary of unacceptable risk. Adapted from Rasmussen (1997)

2.5 Employee participation

Employee participation has not had a strong position in the field of information security. An electronic search in some public standards and guidelines for information security reveals a very modest focus on employee participation, see Table 1 and Paper V.

Table 1. Result of electronically search for keywords 'employee/worker/user participation/involvement' in public standards and guidelines.

Public standard/guideline	Result of search
ISO17799 Code of practice for information security management (Now named ISO/IEC 27002)	1 hit in the introduction, no further results: "Information security management needs, as a minimum, participation by all employees in the organization." (ISO 17799 2000:vii)
Information security forum's (ISF) Standard of Good Practice for Information	3 relevant hits, which all are minor parts of superior subjects. 1) Information risk analysis should involve "representatives from key areas, including business 'owners', IT specialists, key user representatives and experts in risk analysis and information security." (ISF 2005:82) 2) Regarding password changes, "there should be a process for issuing new or changed passwords that directly involves the person to whom the password uniquely applies" (ISF 2005:117). 3) Include users in testing whether security systems function as intended.
OECD (2002) Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security.	1 hit in the introduction, no further results: "Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants" (OECD 2002:9)
The Norwegian National Strategy for Information Security (2003)	No results found

There are however several other fields of research and practice that that emphasize the involvement of employees. Greenberg (1975) describes some general basic schools of thought that support worker participation in organizations, which all have different understandings of what participation look like, what the expected outcomes are and what the basic values of participation are to serve. *The management schoo*l argues for participation as one of several strategies to resolve differences between individuals and groups and thus found an environment of peace and stability. At the same time the main objective of the school is efficiency and productivity, participation can consequently be called symbolic. According to *humanistic psychologists,* participation is beneficial for economic efficiency and a more mentally healthy workforce, as it increases cooperativeness, reduces hostility and anxiety, and improves individuals' sense of responsibility. A third school of thought that argues for worker participation is *participatory democrats*. This democratic theory is not concerned with productivity and efficiency. They argue that only through participation in all aspects of social life, including the work place, can individuals develop the unexploited capacities inherent within them. In sum there are three main arguments for employee participation: utility-based, humanistic and political.

As shown in Section 1.2 participation is one of the main elements in socio-technical thinking. These ideas of worker participation in socio-technical systems have had a major influence on domains that are of relevance for experience-transfer to information security management: participative occupational health and safety management and user participation in technological and organizational development. Occupational health and safety (OHS) management aims - as information security management does – at loss prevention (see paper VI). Information security is mainly a technological discipline, user participation in the development and implementation of new solutions is thus of relevance to the field, which also is practically performed in many information security technological development projects.

Participative occupational health and safety (OHS) management is in many ways a Nordic construct, closely linked to socio-technical ideas (Hale and Hovden, 1998). The arguments for this participative approach to OHS-management were to a large extent based on socio-technical research and assumptions (see Section 1.2), and were characterized as “psychological job requirements” (in Hovden et al., in press): e.g. rights of self-determination; cooperation with and support from colleagues; and learning.

One of the strategies for democracy at the workplace has been to facilitate worker participation in the development and implementation of technology. Participative development of technology is strongly influenced by the socio-technical thought, which states that both technology and organization should be shaped by an understanding of both systems, and not be sub-optimized (Trist, 1981). A key challenge in designing new technologies is thus to take advantage of users’ skills in creating efficiency and productivity both regarding functionality and usability (Adler and Winograd, 1992). Two major arguments for a participatory approach in technological development are found. A utility argument stating that participation of skilled users in the design process can make an important contribution to successful design and implementation of high-quality products. Furthermore, Ehn (1992) links this to the political feature of democracy, power and control in the workplace.

Employee participation is one of the fundamental parts of organizational development (Levin and Klev, 2002). Participation gives organizational members a concrete chance to form their own working conditions by utilization of local knowledge on challenges and possibilities in the current state of the organization As a result securing local anchorage and understanding of the development process. Altogether, a participative democracy approach should ease the implementation of measures as organizational members have taken part in the development of the measures and have an ownership to the change process.

Risk analysis also represents possibilities for employee participation. Employees at the sharp end have important knowledge of what undesired incidents that may occur and how likely it is that these incidents occur and what the consequences of them will be. The voice of employees working close to vulnerabilities and threats thus ensures that all conditions of significance to risk are brought up in discussions and assessed. By including employees in the process, ownership of both the results and the processes behind the results is created. The ownership might ease the implementation of countermeasures as well as improve the quality of the countermeasures. Often, experts and lay people perceive and assess risk differently (Slovic, 2000). Consequently, the interpretation of risk, decision-making and development and implementation of measures can be poor regarding increased safety. This gap is to be closed by including public concerns about risk evaluation (Shrader-Frechette, 1991).

3 Methods

3.1 Research approach and design

The main aim of this PhD work is to study information security management of employees. Consequently, I have selected a combined approach of complementary qualitative and quantitative research methods to elaborate the role and function of employees and some management approaches to users, see Figure 8.

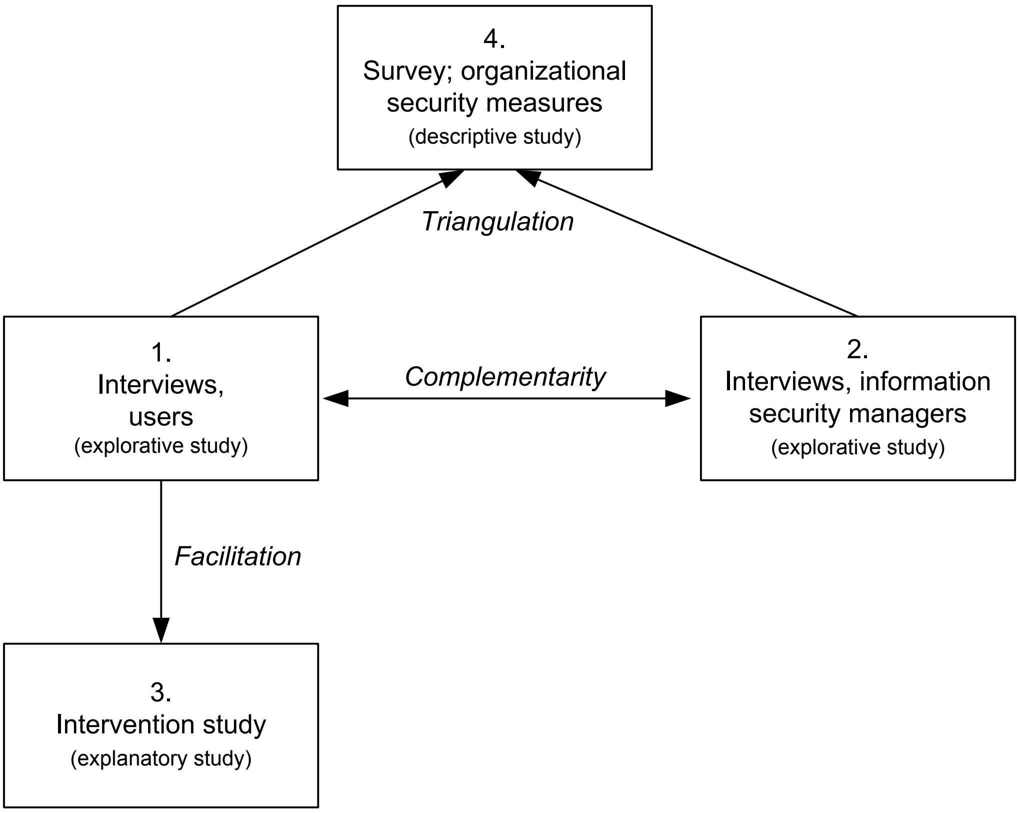

Figure 8. Relations between different sources of empirical data. The numbering shows the sequence of the research approaches.

Figure 8 illustrates the four sources of empirical data and the relations between them: a qualitative interview study of users; a qualitative interview study of information security managers; an intervention study of an awareness training programme; and a survey among a sample of companies. The numbers in the boxes indicate the order in which they were carried out. The quantitative and qualitative methods were combined in three ways as described by Hammersley (1996): complementarity (each method produces different, complementary data about the same phenomenon); facilitation (one method produces hypotheses to be tested by another method); and triangulation (using data produced by different methods to validate each other).

The starting point of the study was an interview study of eighteen users at a department in a bank and in an IT company. This proved to be a good starting point for the other empirical studies as it provided an in-depth understanding of how the interviewed users interpret information security in their working day. In general, qualitative research provides understanding of social phenomena by proximate studies of the local contexts of the phenomena (Thagaard, 2003). Interviews support this purpose neatly as they generate knowledge in interaction with informants by collecting and interpreting the interviewees' perception of the world (Kvale, 1997). The results of this qualitative study of users and information security should not be seen as generalized facts. Rather, the results are interpretations of some users' experiences of information security in their working context.

Some of the findings in the interview study of users pointed at the role and function of information security managers. As a consequence I decided to carry out a new qualitative interview study. This time information security managers at different companies were interviewed about their experience with and expectations of; the function of users; the management of users; and their own role as information security managers. In that way the findings in the first interview study of the users' understanding of information security management in their company were combined with information security managers' interpretation of the same phenomena. Some of the findings in the two studies corresponded while others were different.

Some months after the interview studies of users, I presented the main findings at a national information security conference. One of the findings I presented was that the users studied felt that a participative approach to awareness training emphasizing involvement, dialogue and reflection was the most efficient way to improve their awareness and behaviour. By serendipity, the information security manager at Brønnøysundregistrene, asked me if I was willing to help him develop such a training programme. A few months later I was on the plane heading for Brønnøysund. The research design included both developing the intervention and studying its effects on individual awareness and behaviour. The evaluation of effects was based on experience from intervention studies in the safety domain, e.g. Robson et al. (2001) and Kristensen (2005). The effects were studied by surveys once before and twice after the intervention in an intervention group and a control group. By using an experimental design it was possible to study effects over time in the intervention group. The control group, which was uninfluenced by the intervention, made it possible to study if the intervention caused effects among the intervention participants. The survey was combined by qualitative data, which explained the dynamics of the intervention process and the outcomes of the intervention.

The fourth source of data is a survey studying the use and perceived effect of different information security measures directed at users. This is a descriptive study of the use and effects of organizational information security measures. Organizational measures are thus studied by data produced by three complementary methods: interviews with users, managers, and the survey.

Table 2 shows how the different sources of data are used in the papers. Papers V and VI do not include any empirical research. Papers II and III combine data from different research approaches.

Table 2. Empirical sources for papers

	Interview study of users	Interview study of information security managers	Survey among Norwegian companies	Intervention study, survey	Intervention study, observation	Intervention study, interviews	Intervention study, group conversations
Paper I "A qualitative study of users' view on information security"	●						
Paper II "Information security digital divide in organisations: information security managers versus users"	●	●	●	●			
Paper III "Improving information security awareness and behaviour by a user participative approach: an intervention study"				●	●	●	●
Paper IV "Implementation and effectiveness of organisational information security measures"			●				

The data sources of the thesis are thus based on complementary qualitative and quantitative methods. Table 3 shows some main differences between quantitative and qualitative research designs. Such distinctions are in practice too simplistic, as there is both qualitative research that is theory-driven and tests hypothesis as well as quantitative studies that are exploring concepts.

Table 3. Main differences in quantitative and qualitative research designs Ringdal (2001)

Quantiative research design	**Qualitative research design**
Objective social reality	Social constructed reality
Stable social phenomena in time and space	Social phenomena constructed in local context
Large samples	Small samples
Distance to what is studied	Proximity to what is studied
Explaining/testing causes	Explaining contextual processes
Theory-driven, defined concepts	Exploring, defining concepts
Analysis of numerical data	Analysis of textual data
Statistical analytical methods	Informal analytical techniques

For the present study, qualitative research was a good starting point in the relatively unexplored field of user performance and management field of user performance, as such approaches by nature are explorative and flexible to the context. This approach provided an understanding of how some users function in the information security activities and what views users had on information security and how management should be performed. The qualitative interviews also made it possible to interpret the basic processes explaining the users' views. By combining the users' interpretation with security managers' views, information security management of employees was highlighted in two different perspectives. However, the findings from the qualitative studies are not generalized facts. Rather than talk about generalization as an important principle, one can talk about transferability in qualitative research (Thagaard, 2003). To test possibilities for generalizing the findings, two surveys were conducted. These surveys made it possible to test hypotheses generated by the qualitative findings.

The research design is thus first based on an inductive strategy, which is followed up by a deductive strategy. The explorative interviews were data driven, while the quantitative-based designs were driven by theoretical concepts to be tested.

3.2 Data collection and analysis

This section describes how data were collected and analysed for the four sources of data illustrated in Figure 8.

3.2.1 Interview study with employees

The interview study with employees, which is described and discussed in Paper I, was performed at a department at a Norwegian bank and an IT company. 18 interviews with duration of about 1 hour each were conducted, nine at each of the studied companies. Prior to the interviews talks with the security professionals at the companies were made in addition to studying information security documents at the companies.

The interviews were semi-structured, and addressed employees' experiences and expectations of information security in their working day by discussing subjects such as: individual information security behaviour and awareness; the role and function of users; and information security measures, activities and managers involved in the users' daily operations. The guide was pre-tested and expert opinions on the guide were collected before conducting the interview study.

The analysis of the data was based on an iterative approach, where the data reduction, data display, conclusion drawing and verification is interwoven before, during and after data collection (Miles and Huberman, 1994). For example, during data collection and transcription, possible ideas and questions were recorded. These ideas and questions were later tested on the data material. The interviews were recorded and transcribed. The transcribed interviews were coded in HyperRESEARCH and categorized in relation to the research questions. The categorized data was analysed by switching between the whole picture and details by (Leiulfsrud and Hvinden, 1996): 1) testing the registered ideas during data collection, transcription and coding; and 2) using detailed data material as pieces in a jigsaw puzzle. The aim of this approach was to map and inquire into patterns of the data material; reasons for this pattern; and contrasts of the patterns. Consequently, the analysis is based on Straus and Corbin's (1998) principles of grounded theory by coding and categorizing data looking for patterns. However the current analysis does not consider theoretical saturation as systematically as suggested by Strauss and Corbin. On the other hand they state that their proposed techniques and procedures should not be used rigidly in a step-by-step fashion, rather they emphasize a flexible and creative use of their framework.

3.2.2 Interview study with information security managers

The interviews with information security managers were performed to study the findings in Paper I in a management perspective. 11 interviews with information security managers in 11 different large Norwegian organizations were conducted. The interviews lasted from 1-1.5 hours. The objective of the interviews was to talk about the managers' interpretations of the human part of information security by discussing these topics: the role and function of users; the role and function of information security managers; information security measures aiming at individuals; and functionality and quality of day-to-day information security

The qualitative analysis was mainly performed in the same way as the data from the interviews with employees. However, since the study was based on interviews with 11 different managers in 11 different contexts, the approach was not as constructivist as the interview study of users. The contexts were not considered extensively, and the data were handled in a quantitative way by looking for the causes of patterns of data in the transcribed text. To look for patterns and causes, matrices were used as presented by Miles and Huberman (1996).

3.2.3 Intervention study

An intervention study aiming at improving employees' information security awareness and behaviour by involving employees directly was performed at a Norwegian Public Agency, the Brønnøysund Register Centre. The intervention was small-sized workshops where the participants reflected on information security on their own premises. The intervention and its effects were evaluated by a quantitative survey and a qualitative approach combining interviews, group conversations and observation of the intervention. The effectiveness of the intervention, i.e. the degree to which it causes an effect under realistic workplace conditions (Shannon et al., 1999) was evaluated by quantitative analysis of data material from one survey before and two surveys after the intervention, see Figure 9. The research design was drawing on experience from methodological issues in occupational health and safety intervention studies, e.g. Goldenhar and Schulte (1994); Shannon et al. (1999); Robson et al. (2001); and Kristensen (2005).

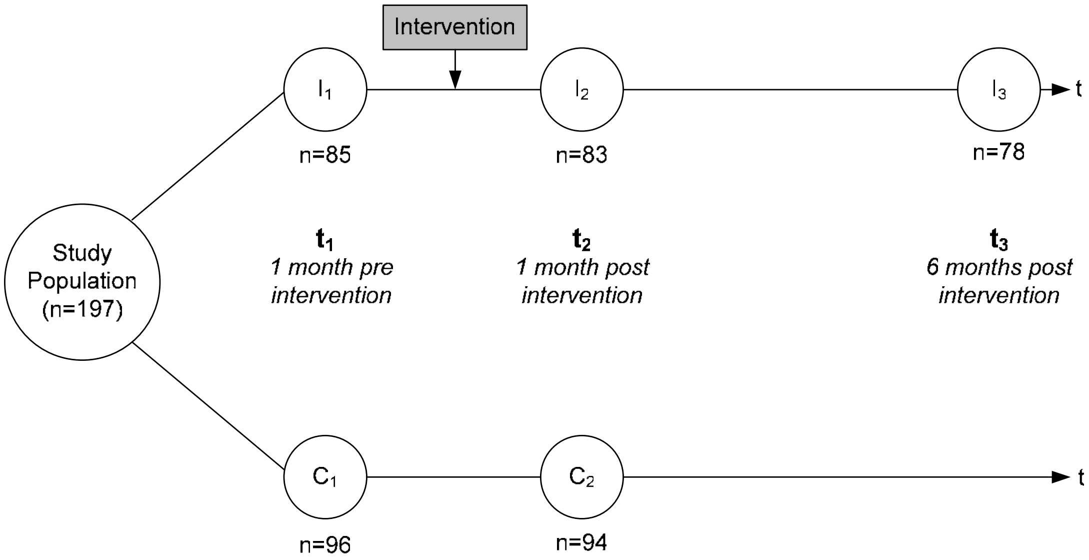

Figure 9. Design of multiple time-series research design with an intervention and a control group.

An experimental design was used for measuring individual awareness and behaviour before and after the intervention. The study population was randomized into an intervention group and a control group. An initial survey was performed 1 month before (t_1) the intervention took place. Invitation to a web-based questionnaire containing questions regarding information security awareness and behaviour was sent by email to the study population. The second survey took place a month (t_2) after the workshops were arranged. To evaluate the stability of the awareness and behaviour after the intervention, a third survey was performed half a year (t_3) after the intervention. The same questions as the one used in the first survey were used in the second and third studies as well. For each survey, both groups received the same questionnaires. Areas covered by the questionnaires on each occasion included personal responsibility for information security; importance of information security; individual information security behaviour; importance of different loss prevention measures; information security versus functionality; and information security as a technological challenge. The items were reduced to indexes which were used for analysing whether there were significant changes in awareness and behaviour from t_1 to t_2 and t_2 to t_3. The respondents were given an anonymous respondent-number, which was automatically generated by the web-based questionnaire. The web-based solution thus made it possible to give the respondents the same respondent-number for each of the three surveys. Respondent data was consequently matched for each survey. The experimental design of the intervention study thus makes it possible to do a participant-by-participant analysis, which requires analysis with the paired-samples t-tests, i.e. to test hypothesis of no difference between the means of two variables based on paired measurements (Ringdal, 2001).

Additionally, qualitative data were used to provide an understanding of how the intervention had the effect uncovered by the quantitative data. Observation studies of the workshops were carried out to understand the processes in the actual execution of the intervention. At the end of each of the studied workshops, the intervention was evaluated by the participants. Additionally, interviews with the security managers were conducted after all the workshops had been arranged. No participants were interviewed. In hindsight, I see that some participants should have been interviewed as well, which should have strengthened the understandings of the processes in the intervention.

The third survey also included questions regarding judgement of the risk of different threats and vulnerabilities, which was used to compare risk judgement of users and security professionals in Paper II.

3.2.4 Survey on organizational security measures

A survey among a sample of Norwegian organizations was performed to study the implementation of organizational information security measures and the effectiveness of such measures. A web-based questionnaire addressed questions on whether different organizational measures were implemented or not. Some of these measures were accompanied by more detailed questions regarding how they were used. Furthermore, the respondents were asked to subjectively assess the effectiveness of different measures and also to specify their understanding of effectiveness of information security measures. Additionally, the questionnaire contained questions regarding perceived information security performance of the organization.

The survey produced three main groups of data: use and implementation of different organizational measures; subjective evaluation of the security performance of the organization; and subjective assessment of the effectiveness of information security measures. To reduce the complexity of the data material, factor analyses were performed, and different indexes for implementation and effectiveness were created. These indexes were used in a descriptive analysis of groups of measures implemented and how the effectiveness of the groups of measures was evaluated. In order to study the relative contribution from different security measures, a linear regression analysis was performed with the assessed security performance of the organization as the dependent variable and single measures as the independent variable.

The questionnaire also included questions regarding judgement of the risk of different threats and vulnerabilities, which was used to compare the risk judgement of users and security professionals in Paper II.

3.3 Evaluation of research results

This section evaluates the results of the research strategies above. Qualitative and quantitative results are evaluated differently, and by use of different notions. Quantitative findings are assessed by reliability, validity and generalization (Ringdal, 2001). These standards to evaluate quantitative studies are not suitable for qualitative studies (Miles and Huberman, 1994; Strauss and Corbin, 1998), which rather can consider the notions credibility, confirmability and transferability (Thagaard, 2003).

3.3.1 Reliability/credibility

The use of different data sources with different objectives and research design is in itself a way improving the reliability and credibility of the research results.

Intervention study and survey on organizational measures

Reliability concerns the quality of measurement. In its everyday sense, reliability is the "consistency" or "repeatability" of your measures (Trochim, 2006). Reliability of the measurement tool is whether the used method gives the same result if used on the same phenomena several times (Ilstad et al., 1977). One possibility to test this is the test-retest technique (Ringdal, 2001), i.e. use the same method for data collection on the same sample at different points of time. In the intervention study the same tool for data collection was used three times. The problem of such measurement of reliability is that the respondents might change their opinion in transit. The control group, uninfluenced by the intervention, mainly remained unchanged between the first and second surveys (see Section 4.3). This indicates good reliability of the measurement tool as the index scores was mainly the same at two different times of measurement for those uninfluenced by the intervention. At the same time, filling out the questionnaire itself three times might have created biased answers. There was a question in the second and third survey if filling out the questionnaire was a reason for a perceived improvement in awareness and behaviour; about 30% of those participating in the intervention answered yes to this question (about 90% felt the intervention had changed their information security performance). However, the control group, which responded to the same questionnaire, remained stable during the same period.

Another relevant type of reliability for the quantitative part of the study is internal consistency, where the most common way to measure reliability is using Cronbach's alpha on an index (Ringdal, 2001). In the intervention study, all indexes for the intervention group were satisfactory, i.e. Cronbach's α >.70. This was measured by data from all three surveys, so the reliability between the three surveys was good for the intervention group. Similarly, the Cronbach's alpha was satisfactory for all indexes in the survey on organizational measures.

Qualitative studies

Reliability in qualitative research deals with replicability, the question of whether or not some future researchers could repeat the research project and come up with the same results and interpretations (Silverman, 2006), However, some researchers argue that this is problematic for qualitative findings, since data are gathered in a given context which might be problematic to reproduce (Strauss and Corbin, 1998). Rather than talk about reliability, one can consider the credibility of qualitative results that concerns techniques to process data, i.e. the quality of the data the research is based and how this data is used and developed (Thagaard, 2003). A key here is to make the research process and findings transparent by describing the research strategy and analysis methods.

To create credibility of the qualitative research methods, the research processes are described to get an impression of how the data was collected and analysed. Furthermore, credibility is generated by drawing conclusions from the data material during the whole process, in an iterative process as described by Miles and Huberman (1994). In that way the results are anchored in the informants' reflections. Furthermore, the papers based on the qualitative data make a clear distinction between what is direct information from the studies (results) and what is the researcher's interpretation of this information (discussion). This is done by having separated sections of results and discussion, but also by tables and citations of the interviewees' understandings of information security.

That only one researcher has analysed the qualitative data is a threat to the credibility of the study. The results and the discussion are as one would expect coloured by the researcher's thoughts, as he cannot leave his body and soul during collection and analysis of data. Analysis is the interplay between research and data, it is both science and art (Strauss and Corbin, 1998:13). Nevertheless, during the interviews the researcher tried to avoid influencing the informants, by being a discussion partner who listened to the informants and make them reasoning on the subjects of the interview. Kvale (1997) argues that interviews are neither objective nor subjective; rather they are based on inter-subjective interactions. The interaction between the researcher and the data both during collection and analysis of data makes the researcher influenced by the data and the data influenced by the researcher (Straus and Corbin, 1998). However, to verify that the researcher had interpreted the results correctly in the given context, the findings were communicated to the interview participants as well as compared to previous research literature on the topics.

3.3.2 Validity/confirmability

The quantitative studies are evaluated by external validity, internal validity and content validity. External validity is related to generalizing conclusions of a study to other persons in other places and other times (discussed in Section 3.3.3). Internal validity considers the approximate truth about causal effects, which is relevant for the intervention study. Content validity is the extent to which individual items provide adequate coverage of the problem, which is relevant for both survey studies. For qualitative studies one rather looks at the confirmability of the findings.

Intervention study

Internal validity is the approximate truth about inferences regarding cause-effect or causal relationships (Ringdal, 2001; Trochim, 2006). The key question in internal validity is whether observed changes can be attributed to causes related to the intervention and not to other possible causes. For experimental designs, the best way to ensure internal validity is randomizing groups (Ringdal, 2001). Randomization gives the design greater strength as one can be more certain that differences between the intervention group and the control group can be attributed to the effect of participation in the intervention and not to group differences (Robson et al., 2001). The internal validity of the intervention study was good, as there were significant differences between the intervention group and the control group, and the only thing that differed between the two groups was participation in the intervention.

Validity of quantitative measurement can be assessed by content validity; construct validity and criterion-related validity (Undheim, 1996; Ringdal, 2001). The latter two are more complex to examine than content validity (Ringdal, 2001). Criterion validity checks the performance of the operationalization against some criterion, which is not relevant for the studies in the thesis since there is no criterion which functions as a correct solution to compare with. Construct validity concerns the theoretical relationship of a variable to other variables. To consider this type of validity empirical assessments are needed which had not been performed in this study. The content validity of the intervention survey, i.e. whether the sample of items covers the population of hypothetical items, should be quite good. Assessing attitudes and behaviour by questionnaires is difficult. To ensure some degree of content validity the questionnaire was developed in cooperation with security managers at Brønnøysundregistrene, tested among a selection of security experts and compared to attitude questionnaire used in the traffic safety domain (Iversen et al., 2005).

The validity of the quantitative findings in the intervention survey is improved by combining the results with the findings in the qualitative studies of the intervention, i.e. observation of the intervention, group conversations and interviews with the security managers. The qualitative data did not contradict the quantitative findings. Additionally they provide more insight into the processes explaining the quantitative findings.

Survey on organizational measures

Content validity is relevant for the measurement of the use of organizational information security measures. The items used in this survey cover a broad range of different measures and are developed based on acknowledged standards and literature in the field of information security.

Qualitative studies

Confirmability of qualitative research results considers how results are used and interpreted. Two main approaches were utilized to strengthen the confirmability of the qualitative findings: respondent validation and combining other methods and research results to the findings.

Respondent validation improves the confirmability of the results. The transcribed interviews were submitted by email to the interviewees to verify the findings. Furthermore, the IT company and the bank were given a report of the findings. At the IT company the researcher was invited to present his findings at a meeting at the department studied. The interviewed security managers received a report of the main findings of the interview study. The response to this communication was mixed, but those who commented did not suggest any significant changes.

Comparing the qualitative results with other research results and its context also strengthen the confirmability (Thagaard, 2003), this is done when discussing the qualitative findings in Papers I and II. The combination of multiple methods produced more accurate and comprehensive results, thus strengthening the confirmability (Silverman, 2006) of the qualitative results in Papers I and II.

3.3.3 Generalization/transferability

Intervention study

The generalization of quantitative findings is related to the external validity (Trochim, 2006), i.e. the degree to which the conclusions in the study hold for other persons in other places and at other times. The intervention proved to cause changes in awareness and behaviour among participants of the intervention. These participants can be characterized as average IT users without any expert knowledge on IT or any management responsibility. Most companies mainly have this kind of IT users. As a consequence the intervention approach is transferable to other companies and sectors as well. The descriptions of the intervention are not normative; it is thus possible to adjust the approach to other contexts and even other kinds of threats and hazards in risk management, as it was the processes behind the workshop and not its contents and subject that were the important causes for the intended modifications.

Survey on organizational measures

Generalization of quantitative results depends on the respondents being representative of a large population (Undheim, 1996). There were only 87 respondents to the survey, which is a small sample with limited potential for generalizing. Kotulic and Clark (2004) experienced the same problems regarding response rate in a US study of information security management effectiveness. They received only 67 questionnaires of 1474 possible respondents. The small response rate was followed up by a study that showed that the main reasons for the non-responses were: related to volume of survey requests the companies get; a policy of not sharing information regarding their information security performance; and a desire not to spend valuable manager time on the particular research project. Our sample was also skewed regarding assessed security performance; about all the respondents assess their performance to be high or average. Hence, the respondents believe that they are “the best of the class”, which often is the case for voluntary self-assessments. It can thus be claimed that only those who have knowledge and interest in information security responded to the survey. Independent of the skewness and sample size, it was possible to study the relations between implementation and effectiveness which was the aim of the paper. Nevertheless, the possibility to generalize is poor. However, the study provides good understanding of information security management, since it can be assumed that the respondents were well-informed and had a good management performance.

Qualitative studies

The results of the interview studies of users are not generalized facts, but understandings of processes in the particular context of the two studied companies. Rather than generalizing the results, one should consider whether the results are transferable to other conditions, processes and people. In Paper I the two companies studied are described in order to give an understanding of the contexts the results originate from, thus strengthening the possibility to transfer the results to other contexts.

Similarity, the interview study of information security managers is not generalized facts, but understandings of the interviewed managers' interpretations of users and information security in the context of the managers at his company. However, it is difficult to treat many different contexts when considering one phenomenon (Silverman, 2006). As a consequence, the qualitative data from the interview study of managers were treated more quantitatively than qualitatively, as the data were disconnected from their context to some degree and analysed by use of cross-case matrixes as shown by Miles and Huberman (1994). One of the main objectives of this interview study was to test findings in the user study in the information security managers' perspectives. In that sense, the disconnection of context did not influence the credibility of the findings.

3.3.4 Strength and weaknesses of research approach

Users' role in information security and the management of employees is an unexplored area of research (see Section 2). The research design described in Section 3.1 suited this state of research well, beginning with an inductive strategy and moving to a deductive strategy. As a result, the study gives both a deep understanding of a selection of organizational information security processes as well as descriptions of information security management in several businesses. The intervention study in Paper III examines the effects of information security measures in an experimental manner, rather than a descriptive, subjectively way. Other measures evaluated in the thesis are evaluated based on descriptive statistics; subjective interpretations; and literate. The power of such intervention studies could have been employed with other measures as well, which is suggested as further research in Section 6.1.

Since qualitative findings are the core of the results of the study, the discussions and conclusions in section 5 and 6 might be a weak construction. However, this is strengthened by complementary quantitative studies and comparison with research literature. Would different findings in the qualitative studies have generated a different conclusion of the thesis? Probably yes, since the hypothesis and questions in the quantitative studies originate from the qualitative findings. At the same, there are indications that the qualitative findings are likely to give a ‘correct’ picture of the information security processes involving users. Research literature supports the qualitative findings; reactions to popular-scientific talks about the subject support the findings; and experts who have looked at the results assume the findings to be realistic.

4 Summary of papers

4.1 Paper I: A qualitative study of users' view on information security

The first paper *'A qualitative study of users' view on information security*' aims at providing insight into users' experiences and views on information security by qualitative research interviews. The study revealed some main patterns regarding users' views and experience of their own information security function in daily work:

- The interviewed users state that they were motivated for information security work, but do not perform many security actions in daily work nor are they aware of what actions they can make. This gap between talk and action among the informants can be explained by a combination of users not being as motivated as they declare; lack of knowledge about how to perform well due to poor information and training provided by the information security management; and a latent conflict of interest between functionality and information security.
- An increase in the current very low information security workload of users will create a conflict of interest between information security and work functionality.
- Documented requirements of expected information security behaviour have a limited effect on user behaviour and awareness. Similarly, general awareness campaigns (i.e. expert-based one-way communication directed towards many receivers) have limited effect on users.
- A user-involving approach is considered more effective for influencing user awareness and behaviour than documents and one-to-many awareness campaigns as this make it possible for users to reflect on their own situation, and meet information security professionals face to face.

4.2 Paper II: Information security digital divide in organisations: information security managers versus users

The second paper *'Information security digital divide in organisations: information security managers versus users'* is a continuation of Paper I. This paper looks at similarities and differences in information security managers' and users' views and experience of information security practice in organizations. This aim was approached by considering the differences between the groups regarding risk judgement; the role of managers; the role of users; and administrative security measures, by combining different sources of empirical data.

The study revealed a social digital divide between information security managers and users regarding risk judgement, and the views and experience of information security practice:

- Information security managers mainly view users as an information security threat, while users believe they are an untapped resource for security work
- Users trade-off security for other work tasks, while information security managers of course have information security as their main working task
- There are limited interactions between users and managers. As a result of the limited interactions users view managers as remote, invisible and secretive, but nevertheless leave the responsibility for information security to the managers.
- The interviewed managers have no explicit detailed knowledge on users' security performance in their organization. As a consequence, there is a gap between managers' professional knowledge and their knowledge of real-world practice at the sharp end.
- Users trust managers and technological solutions to take care of security, while managers do not trust users to be a reliable security resource.

Users and managers agree that the effectiveness of formal documentation on expected behaviour and formal one-way information measures is limited on user behaviour and awareness. Both studied groups felt that a participative approach is most likely to influence user behaviour and awareness.

4.3 Paper III: Improving information security awareness and behaviour by a user participative approach: an intervention study

The third paper *'Improving information security awareness and behaviour by a user participative approach: an intervention study'* describes and evaluates the effect of a training programme, aiming at improving users' information security awareness and behaviour. The project, carried out in a Norwegian public agency was based on the principles of active employee participation; collective dialogues; reflection in groups.

The evaluated effects by an experimental research design showed that the intervention was powerful enough to significantly change awareness and behaviour among the participants in the intervention group. The third survey half-a-year after the workshops showed that the awareness modifications among the participants have remained stable over time, while some behavioural attributes have significantly improved even more from the second survey. The control group mainly remained unchanged in the pre-post test. Participation in the workshops is the only thing that separates the intervention and control group, it can thus be claimed that the effect of the workshop has created intended improvement of awareness and behaviour.

Qualitative data from the intervention study indicated the participative approach at a group level was the main reason for this change. By involving the participants in dialogues with each other and the avoidance of one-way-communication from the security officers, the employees discussed information security on their own premises in a lively and relaxed atmosphere.

4.4 Paper IV: Implementation and effectiveness of organisational information security measure

The fourth paper *'Implementation and effectiveness of organisational information security measures'* evaluates organizational information security measures by looking at implementation and subjective assessment of such measures. This was approached by a survey among a sample of Norwegian organizations.

The survey showed that formal technical-administrative measures such as security policies, procedures and methods are the most common implemented organizational information security measures. Measures aiming at improving awareness are used to a less extent.

Subjective assessment of security measures showed that awareness creating measures along with technological measures are believed to be the most effective measures. The respondents understood effectiveness of measures as 1) reducing the risk of unwanted incidents; and 2) creating good informal processes and improving awareness. Policy and other documents were not considered to be as effective as awareness creation and technology.

A linear regression analysis, with perceived security performance of the organization as the dependent variable and implementation of single measures as independent variables, was performed to study the relative contribution from implemented measures. This analysis showed that the single organizational activities "involving employees in the security work", "perform risk analysis frequently" and "security policy" are independent significant contributors to how the respondents assess the security performance of their organizations. Consequently, implementation of these three measures is believed to be most effective for producing a high level of security.

As a result the study showed an inverse relationship between implementation of organizational security measures and assessed effectiveness of the same measures. The most used measures are assessed to be the least effective, and the least used measures are assessed to be most effective.

4.5 Paper V: User participation in information security

The fifth paper *'User participation in information security*' discusses employee participation in information security in a theoretical perspective. The paper shows that some of the current public standards and guidelines for information security management have a modest emphasis on worker participation. However, several other fields of research and practice of relevance to information security management, have a long tradition for involving employees in many organizational processes, e.g. technological development, occupational health management, risk research, and organizational development. The paper presents arguments from these relevant research areas and considers possible positive outcomes of a participative approach to information security: improved usability and functionality of security technology; improved security awareness, ownership, acceptance and motivation among employees; reduced gap between security professionals and employees; and improved decisions due to better understanding of risk and the function and quality of information security in an organization.

The paper provides three practical examples of user participation in information security: awareness training (the intervention in Paper III); informal pizza meeting; and participation in a risk analysis.

4.6 Paper VI: Industrial safety management and information security management: risk characteristics and management approaches

The sixth paper *'Industrial safety management and information security management: risk characteristics and management approaches'* examines basic theoretical differences and similarities between industrial safety management and information security management.

The basic idea of industrial safety and information security is the same: loss prevention. There are however some different views on risk and risk mitigation within the two fields. The uncertainty, complexity, ambiguity and ripple effects of IT-related risks are higher than for industrial safety-related risks. Furthermore, there are different loss prevention management approaches within the fields of information security and industrial safety. This is partly explained by different characteristics of the risks and by the historical development of the two fields. Information security management has traditionally utilized technological and passive administrative measures for risk mitigation, and lacks the mature socio-technological perspectives and approaches of industrial safety.

Due to integration of IT in industrial systems, information security becomes important for IT-based safety systems. This calls for a merged approach to industrial safety management and information security management in industrial organizations. The two approaches have both their strengths and weaknesses, which implies the possibilities for experience transfer. Information security management can learn from the more mature socio-technical perspectives and democratic ideas of industrial safety and adapt related approaches. The possibilities for experience transfer from information security to industrial safety are good when it comes to preservation of IT-based safety systems.

5 Discussion

This chapter discusses information security management of users by considering the findings of the study (Chapter 4) in combination with relevant research literature (Chapter 2). First, the quality of user behaviour and awareness is discussed based on qualitative results in Papers I and II and is supported by some research literature. Then individual security decisions and actions are explained by organizational and technological structures and processes. The first part of the discussion relates to the problems and explanations for these problems regarding user performance. However, in the final parts of this chapter, users are looked at as a resource in the information security work by considering employee participation in information security management.

5.1 The role and function of employees in information security

The qualitative studies in Papers I and II show a *poor quality of users' information security behaviour and awareness as the users contributed with few security actions and were quite indifferent to information security when it came to actual daily work.* The interview study of users (Paper I) reveals that users neither perform many security actions in their daily work nor are they aware of what actions they can make. The interviewed users were not familiar with possible threats; were not aware of possible consequences of security breaches; and some of the informants did not see the value of their information security role in the holistic security work of their company. The interviewed information security managers (Paper II) mainly looked at users as a problem in systematic information security work, as the managers felt most users were unaware of risks; risk mitigation; and the importance of information security as the users lacked the necessary incentives, knowledge and skills for safe and secure behaviour.

These qualitative findings are supported by some empirical research literature that shows poor quality of employee security performance, particularly related to password etiquette. Stanton et al. (2005) performed a survey to shed light on their taxonomy presented in Figure 6. Their study focused on password-related behaviour and showed that users had a rather dismal record of enacting basic hygiene behaviour e.g. frequent changes of passwords. Quantitative and qualitative findings by Adams and Sasse (2005) support that password-related behaviour of users is poor, and explains this behaviour by the nature of passwords (multiple passwords, content, frequency of change); perceived compatibility with work practice; and users' perceptions of organizational security approaches. Unsatisfactory password-behaviour is thus created by basic causes in the organizational context. In a similar way, Frank et al. (1991) and Leach (2003) presents theoretical arguments showing how poor user security performance is created by formal and informal organizational factors.

5.1.1 Information security trade-offs

Theoretically, actions and decisions made by users should function as one of many interacting elements in a socio-technical information security system. The findings of the thesis indicate that users lack the necessary knowledge and incentives to consider information security and behave accordingly in their daily work. This is visible by information security trade-offs, i.e. other work tasks are prioritized ahead of information security. Although the interviewed users in Paper I did not perform many security actions, they nevertheless did not see how they could perform more actions as this was expected to create problems for work functionality and efficiency as indicated by the following citations from the interviews in Paper I:

> *"Information security is not my job. I have to concentrate on my own working tasks, and trust that the security system is in place. Information security is not something I should think about…How much should a user actually think about information security? It is not possible to be too cautious - it must be possible for us to carry out our work smoothly"* Bjørn (43), ♂, bank

> *"We are measured by sale. Our salary depends on it, bonuses and stuff like that. Information security is definitively a second or third priority. If we have to use half an hour extra on information security per day – that simply doesn't function! …. One of the greatest problems of information security is to find the balance between security and functionality. You can have a very strict IT-system that makes you unproductive in the sense that it is not possible to do your actual work tasks. I believe that's why so many have a poor information security behaviour. It is a combination of not knowing and a conflict between security and functionality.... A lot of those working in the bank have no background knowledge of IT. They know how the systems they use on a daily basis should be used. Beyond that, they hardly know where the on/off switch of their computer is."* Halvard (29), ♂, bank.

These citations reflect the explanation of the trade-offs uncovered in the interviews: requirements of efficiency, lack of knowledge and functionality issues. Additionally, Post and Kagan (2007) and Besnard and Arief (2004) argue that users experience interferences or delays in daily operations due poor usability of security systems. As shown in Section 2.4.3, in the set of demands for information security, functionality and efficiency, users tend to prioritize the latter two ahead of information security. When it comes down to business; functionality, usability and efficiency are likely to be prioritized ahead of information security (Besnard and Arief, 2004). The information security rationality of the interviewed users in Paper I is consequently based on a tendency to prioritize other activities ahead of information security.

Rasmussen (1997) explains that systematic migration towards unacceptable risk performance is created by pressures in the direction of efficiency by line management and a gradient of least effort provided by operators. Furthermore he argues that loss prevention approaches are supposed to function as a counter-gradient to these pressures, in this particular case different approaches to information security management. According to Rasmussen's (1997) migration model, information security trade-offs are explained by demands of efficiency, functionality issues and how information security management approaches handle the trade-off problems.

Consequently, *information security trade-offs are generated by a combination for interwoven motives: 1) individual motivation for information security; 2) prioritizing work tasks; and 3) quality of information security management approaches*. One of the premises of this thesis is that employees are not to blame for incidents. Bearing this in mind, motives for information security trade-offs are created by the information security system and processes in the organizational context, which will be discussed in subsequent parts of the discussion.

The users' information security trade-offs raise two questions. One question regarding the extent to which one can expect users to contribute in information security efforts and another question about how to deal with the trade-off problem.

► *How much should one expect employees to contribute with considering that they have other primary work tasks?*

The main goal of most organizations is making money, in that sense it is important for the organization that employees perform regular work tasks to reach the organization's goals and thus generate value. However, preserving information security is also one goal for organizations, as most organizations today are dependent on reliable, credible and available information systems. So although information security is resource demanding, information security breaches may cost even more. As a result, preserving information security is one of many equally important subgoals of an organization that influence the financial performance such as quality management. Similarly, at the individual level, information security is one of many secondary tasks such as HSE, quality, ethical values, which are "additions" to primary working responsibilities.

One cannot require that employees should be security experts; but *one can expect users to be aware of information security and perform simple, not time-consuming action*s. Most information security actions performed by users are simple and not very time-consuming and should not in principle interfere with regular work tasks. In fact many security actions are just common sense, e.g. not talking about sensitive information to strangers and avoiding dubious web pages. This was also pointed out by a female user that was interviewed at the IT company, who was clearly the most security aware user among those interviewed at the IT company and thus represented a contrast to the other patterns revealed by the interviews:

> *"It doesn't take much effort from us to do something about information security. It's simple to delete spam mail; to lock the computer when absent from it; and to avoid downloading stuff from the internet. These are some of the things we can contribute with in our daily work – and they are simple actions."* Frida (36), ♀, IT company

It is thus a paradox that most security actions and thoughts to be performed by users are simple and can in principle be easily integrated in regular work tasks, but are nevertheless not performed in practice.

►*How to handle the trade-off challenges?*

It would be naïve to require users to be aware of security and act accordingly without considering the fact that most employees have other primary work tasks than information security. A key challenge for information security management is thus to make employees sufficiently aware of security issues without disturbing employees' regular work and other organizational goals. According to human-computer security studies (see Section 2.4.1), one solution to handle trade-offs is improved usability of technological solutions. This study showed that another solution is to convince members of the organization to consider information security as an integrated part of their working day.

Tightening security even more will obstruct employees and make them less productive, as users are likely to struggle to find ways around the security condition to enable them to do their jobs. In a similar way, loosening up security can result in a more vulnerable situation. Both technological and administrative security systems must be in place. However these measures should be designed and implemented to fit the context of the organization. This implies that the usability of the technological security systems must be improved (e.g. Johnston et al., 2003; Furnell et al., 2006). For example by fewer passwords or other login systems to overcome the challenges of poor password-related behaviour. The key challenge in designing user-friendly technology is to take advantages of users' skills in creating the most effective and productive working environment (Adler and Winograd, 1992), which can best utilized by involving employees in the design of new solutions (Ehn, 1992).

As discussed above and in Section 1.4, considering information security in their daily work should not raise the work load of the individual worker significantly. It should even be possible to integrate information security with other work tasks - however the interview studies indicate that this is not easily done in practice. This is explained by lack of knowledge of how to think and act; lack of incentives to consider information security; and lack of knowledge on the importance of preserving information security. These causes can further be explained by basic causes of inadequate information security approaches directed at users. As will be discussed later (Sections 5.3.3 and 5.5), the key to handle the lack of knowledge and motivation is participation in information security activities and dialogue on how they can contribute, why their contribution is important and that their contributions are simple, not time-consuming and are not likely to interfere with other work tasks.

5.2 User performance explained by an organizational context

Errors and violations committed by individuals at the sharp-end are created by causes throughout the organization to individual workplaces (Reason, 1997). Following this argument, being one of the premises of the study (Section 1.2), individual information security behaviour is created by the socio-technical context of operation. By using the pentagon model (Figure 3) as a framework, Figure 10 summarizes how basic causes identified in empirical findings in the present study are mechanisms that generate the behaviour in the work context. *The rest of this section discusses the elements in the model.* For simplicity, the elements of the figure are kept separated in the discussion. However, the elements in the model are closely interrelated; consequently some overlapping discussions are unavoidable. The limited effect of formal systems is for example explained by lack of interaction and dialogue between information security managers and users that result in unrealistic premises for the development of e.g. documented instructions.

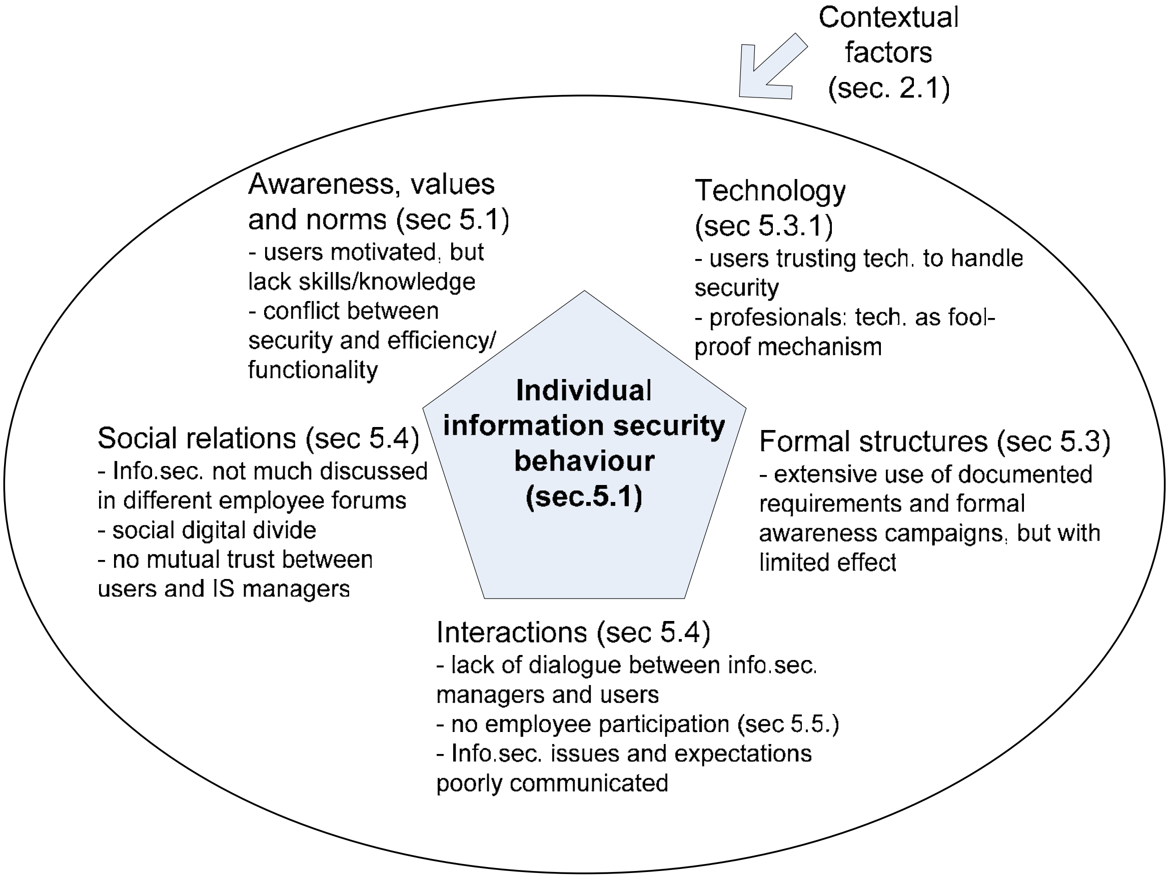
Contextual factors (sec. 2.1)
Awareness, values and norms (sec 5.1)
- users motivated, but lack skills/knowledge
- conflict between security and efficiency/ functionality
Technology (sec 5.3.1)
- users trusting tech. to handle security
- profesionals: tech. as fool-proof mechanism
Individual information security behaviour (sec.5.1)
Social relations (sec 5.4)
- Info.sec. not much discussed in different employee forums
- social digital divide
- no mutual trust between users and IS managers
Formal structures (sec 5.3)
- extensive use of documented requirements and formal awareness campaigns, but with limited effect
Interactions (sec 5.4)
- lack of dialogue between info.sec. managers and users
- no employee participation (sec 5.5.)
- Info.sec. issues and expectations poorly communicated

Figure 10. Socio-technical information security aspects explaining poor individual information security behaviour. Identified in empirical studies.

5.3 Formal structures and technology: evaluation of user-directed measures

Several administrative, technological and informal processes can be used to improve or maintain the information security performance of organizational members, see Section 2.3. The interview study of users (Paper I), the interview study of information security managers (Paper II) and the survey in Paper IV give respectively qualitative understandings and quantitative descriptions of the extent of different user-directed measures, and how the effectiveness of these measures are evaluated. These studies show that documented requirements describing expected behaviour is the most widely used measure to influence user behaviour, which is in accordance with overview articles by Dhillon and Backhouse (2001); Clarke and Drake (2002); and Siponen and Oinas-Kukkonen (2007). This is followed by passive information and education campaigns, e.g. emails, interactive learning programmes, intranet notices, posters and gifts. These sources of information are called passive, because they are artefacts that receivers have to actively seek and read information about in order to gain knowledge. Other educational information campaigns based on face-to-face communication such as meetings, classroom education and lunch talks are not used to the same extent. These sources differ from passive information as the receiver can listen to information rather than read information. Although education and information campaigns are separated as different measures in Section 2.3, they are handled together here since they influence awareness. Finally, participative approaches, such as participation in risk analysis and formal and informal dialogue on information security, are not used to any large extent, which is supported by Paper V that shows that employee participation has a very modest position in public information security standards and guidelines.

Both the qualitative and the quantitative studies show that the least used measures also are the measures that are evaluated to be most effective for influencing users, and vice versa. As a result the relations between use and effectiveness of measures directed at users can be summarized as a metaphorical staircase, see Figure 11. This section discusses the strength and weaknesses of each of the groups of measures. Effectiveness is understood here as the ability to accomplish objectives of reducing risk for unwanted incidents by influencing user behaviour and awareness, see Paper IV. Below the staircase is an axis of information richness (Hodge et al., 1996: 301), i.e. the carrying capacity of a method conveying information. The staircase is proportional to information richness; as a consequence it can be argued that the effectiveness of influencing awareness is dependent on rich information. Spoken information with possibilities of dialogue is considered more effective for the purpose of influencing users than lengthy documents.

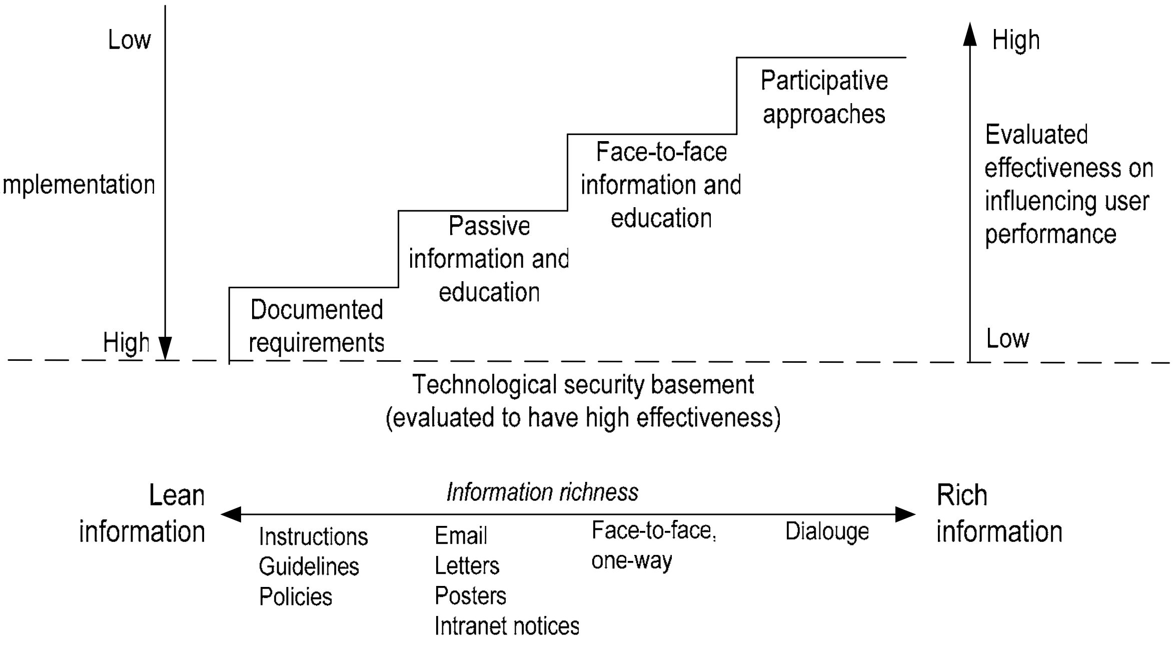

Figure 11. Staircase of information measures aiming at influencing individual user behaviour and awareness

► *Why is there a transverse relationship between implementation and evaluated effectiveness?*

Paper IV shows the same transverse relationship between implementation and effectiveness of all kinds of organizational information security measures. What distinguish the staircase in Figure 11 from a similar metaphor in Paper IV is that Figure 11 is more fine-meshed on awareness creating activities than the one in Paper IV and that the one in Paper IV considers administrative tools and methods such as risk analysis, audits and incident handling in addition to the documents and awareness approaches in Figure 11. This transverse relationship is explained by 1) logical relations between the stairs (e.g. documented requirements must be in place before one can plan processes such as incident handling); 2) demand of resources (developing documents is less costly than performing awareness campaigns); and 3) status of current implemented measures. The first two should be quite self-explanatory; however the latter one needs some further explanation. When you have already implemented a set of measures, a possibility to improve is to implement a new measure that has not been used before, thus bringing the security performance an innovative step forward. As a consequence measures not implemented to a large extent might be expected to be more effective than the measures already in place

5.3.1 Technology

Technological security solutions are the foundation of information security. Technology is essential for preserving security. It would have been of no use to look into users' role if there is no technology as a foundation. However, user-computer interaction was an important part of a socio-technical information security system. Literally, the first contact users have with information security is when a user logs in to a computer and is asked to enter user name and password, i.e. identification and authentication, which also is important part of access control and logging of security events (Gollmann, 1999). Users meet security technologies both explicitly and implicitly in their daily IT use. Most of the information security activities it is possible for users to perform are user-computer interactions, e.g. cautious use of e-mail and avoid publishing sensitive information on social networking sites such as Facebook. Explicit means solutions that attempt to control and regulate user behaviour, e.g. passwords for login to different systems; access control to files and map of files; and pop-up warnings. Implicit means the techniques used in maintaining security in application, services, operation systems, kernels and hardware (Gollmann, 1999), i.e. solutions that preserve a secure environment for employees' use of ICT systems. Empirical findings in the study show that users have trust in these technological solutions, and to some extent attribute the responsibility for information security to technology.

Empirical findings in the study show that information security professionals evaluate technology as the most effective information security measures along with awareness training. The interviewed information security managers interpret technology as a foolproof system for preventing many of the intentional and unintentional actions of users. Technological security solutions are also believed to be more sound and reliable than users:

> *"The advantage of technological solutions is that there are no human parts that can fail. Of course they sometimes fail, but not in the same way as humans do. You don't have to inform the technology, which is a clear advantage. Technology definitively reduces risk more than you can train a user to do."* Information security manager, Public agency I

It can thus be claimed that the design of information security systems is based on an idiot-proofing assumption (i.e. the machines are so perfect that it is immune from the limitations of users) and a deskilling assumption (i.e. to automate work so that one needs fewer users and workers who are less skilled), which is a traditional approach to tje design of systems (Adler and Winograd, 1992). Such approaches have treated users from a mechanical point of view and looked at humans as a system component with a particular repertoire of actions. Adler and Winograd further argue that a countermeasure to these myths is to design new technologies by taking advantage of users' skills and experience in creating user-friendly technologies that create an effective and productive working environment. This is supported by human-computer interaction studies on information security by Besnard and Arief (2004) and Furnell (2005).

The planned and actual use of passwords provides an example of user-friendly issues and idiot-proof and deskilling assumptions in design. The interviews show that users often experience problems with passwords – they have a lot of them, and have to change them at different intervals. In the following paragraphs, the design of password-based systems is discussed by a simple version of a Actor-Network Theory study of the mechanisms that glue the socio-technical information security system together, i.e. "how do actors and organisations mobilize, juxtapose, and hold together the bits and pieces of which they are composed" (Law, 1992:386).

The information security designers work out a scenario for how the system will be used and misused. Protection in this scenario is then inscribed by the use of technology and administrative efforts: user behaviour is inscribed by access control based on passwords, i.e. they presuppose that users will get permissible access to applications and information by logging on with their personal passwords, which according to instructions and regulations are supposed to be kept secret. The inscriptions programme the action of the users, and define roles to be played by both users and the technological system (Latour, 1991). As argued above, the design of password-based systems looks at the users as a system component with a particular repertoire of actions, and delegate roles and competencies to human as well as non-human actors in the socio-technical network.

In theory, the designed system will be adopted by the users, who will relate the system into their context. The design presupposes that humans should act according to measures, i.e. use secret passwords kept away from others to log into systems. Practical life, on the other hand, show that users keep their passwords on Post-it notes, and thoughtlessly gives away their passwords to strangers. Adams and Sasse (2005) show that poor password-behaviour is explained by the nature of passwords (multiple passwords, content, frequency of change); perceived compatibility with work practice; and users' perceptions of organizational security approaches. It is thus technological and organizational aspects that generate poor password-behaviour, as informal organizational action is often incompatible with the planned, formal processes (Brunsson, 1989), and "the fate of facts and machines is in later users' hands" (Latour, 1987:259).

Inscribed password routines might easily, deliberately or accidentally, be worked around, e.g. a writing passwords on a Post-it note. The strengths of the inscriptions are thus too weak in the non-design context. In the design of password-based security systems, someone apparently forgot to ask the employees about how they experience the use of passwords. This calls for more user-participative approaches in design, as suggested for system design in general by Ehn (1992).

Technology is essential of any aspects of information security. Technological security measures must be implemented to prevent external threats but also handle vulnerabilities within the organization. However it is not the only solution to information security. Regarding users the challenge is to 1) inform and train users in using ICT systems in a secure manner and 2) balance security and usability of security solutions. Training and education of employees is discussed in subsequent parts of the discussion. Regarding usability and security issues, tightening too much will be a further obstacle for users, while loosening security might improve usability but at the same time it will create less security produced by technology. As a result, technological solutions must be adjusted to working conditions.

5.3.2 Documents: policy, procedures and instructions

According to Papers II and IV, documented requirements are widely used in the studied organizations. However, the qualitative interviews in Papers I and II and the survey in Paper IV show that neither users nor information security managers believe that documented requirements of expected behaviour have any influence on user performance, because of availability issues, difficult to understand the contents and no time and no incentives to study the documents, here exemplified by one users' view on rules and guidelines:

> *"Of course, there are rules and guidelines for information security behaviour. Nevertheless, I haven't heard about them or seen them. I believe they're available at the bank's intranet. I don't believe that everyone has read them… Our working day is too busy. There's a lot of information on all kinds of things all the time, but there is simply not time to read everything. There are instructions for everything in the bank, even on how to order a ball pen. To put it this way: I don't think everyone has read all these instructions… I believe my behaviour is approximately the same as the documented expected behaviour, although I don't know what is written. My behaviour is based on the experience I've acquired during my years here."* Erik (43), ♂, bank

A survey by Frank et al. (1991) also shows that formal policies regarding behaviour did not appear to be associated with security-related behaviour. However the study showed significant relations between security behaviour and informal norms and users' knowledge and experience. Dhillon (2001a:4) argues that in attempts to shift focus from technology to business and social processes, "over-formalized, acontextual and ahistorical solutions designed in a reactive manner" dominate. The empirical findings of the thesis show in a similar way that the formal system is unavailable, difficult to understand and employees lack time and incentives to study the documents. Consequently, the system is over-formalized and not contextualized to the employees' world. The formal rule-based system must be contextualized (Dhillon, 2001a) by understanding the issues the policy must address and understanding the security challenges in the organization; and be integrated with other business goals of the organization (Whitman et al., 2001). The lack of contextualization in the studies can be understood by the lack of interaction and dialogue between uses and those involved in the decision related to the formal systems as the formal systems are developed and implemented top-down without involving employees or employee representatives. In the early 1990s a mandatory public reform, the internal control, with regard to enterprises health, environment and safety (HES) systems was introduced in Norway. Among other things, the internal control required a documented HES system. Studies revealed that employee participation and the engagement of top managers in local development of documents led to better formal systems than professionally developed ready-made systems (Hovden, 1998a).

The basic idea of documented descriptions of expected behaviour is "programming" behaviour. Organization are hard to run, people do not always do what they are supposed to do. Argyris and Schön (1996) distinguish between the concepts of theory-in-use (what actually is done) and espoused theory (what is expected and told to be done). When it comes to formal information security systems directed at individuals, these theories of action are not in line. Brunsson (1989) argues that in a busy working day of conflicting demands, organizational ideas and individual actions become loosely coupled or de-coupled. Two organizational forms thus occur: a formal and an informal organizational form. Braverman (1974) has explained such patterns by arguing that separated planning and work can lead to unmotivated and uncommitted operators, hence resulting in lack of emphasis on obedience to the documented requirements for behaviour.

► *Why are documented requirements so extensively used when the effects on user behaviour and awareness are considered to be low?*

First, the extensive use of documented requirements for user behaviour is influenced by legal requirements and recommendations in standards and guidelines. Information security has been a rule-based domain (Clarke and Drake, 2002), and both ISO/IEC 27002 and regulations (see Section 2.1), request user instructions organizations should comply with.

Second, documented systems are an essential part of systematic information security work in general. There are documented plans and requirements for all parts of the information security work, not just for expected individual behaviour. The interviews with the information security managers shows that documented plans are necessary to be able to organize systematic security work in the complex, dynamic nature of organizations. For example in large, distributed organizations one must have some common rules about how to behave, in order to have a unified management system in different parts of the organization. Following the metaphorical staircase in Figure 11, documented requirements are an important basis for developing and implementing other measures. The content of a user training programme should, for example, be in line with requirements in the documented information security system.

Third, documented systems are valuable for modes of knowledge conversations that make either tacit or explicit knowledge explicit, which are among the important processes for creating organizational knowledge (Nonaka and Takeuchi, 1995)

Fourth, interviews with the information security managers show that documented requirements serve a purpose of blaming. The requirements are a reference point when sanctions have to be imposed.

Documented requirements are thus necessary, but not sufficient. They are a necessary platform for other measures, as a result they have an indirect effect on user performance. However, there are indications that there is too much emphasis on the direct effectiveness of them.

5.3.3 Training, education and information campaigns

The user education and awareness training approaches mapped out in the study can be categorized into two groups:

- Formal, one-way communicated information (employees must actively seek information and gain knowledge by themselves, e.g. emails and interactive educational programmes)
- Face-to-face activities, where employees and information security professional interact in some way, e.g. information meetings and participative approaches to awareness training.

The empirical studies revealed that passive informing was used more than face-to-face activities, although interacting approaches were believed to be much more efficient both by users and by security managers (see Figure 11).

At the studied IT company in Paper I, there had been a passive information campaign half a year before the interview study. The campaign was a small box of chocolate that included a pamphlet on cautious use of email, which was distributed to all members of the organization. Only one interviewee remembered the campaign, the rest remembered it when the chocolate was mentioned, but only remembered that the chocolate tasted good:

> *"I don't think any of my colleagues remember what information they got together with the chocolate box…I believe most of them ate the chocolate, and left the pamphlet in the box….The campaigns are just a stunt. After the campaign, you never hear anything. I don't think any campaign has had an effect my security behaviour. The message of the campaign is quickly forgotten. Other tools than chocolate and pamphlets should be used. I think a course describing how one should behave should be arranged. I think it's easier to become aware if one meets information security professionals face to face."* Camilla (30), ♀, IT company

Passive information campaigns have, according to the interviewed users, no significant long-term effects on users' behaviour and awareness. The informants state that such campaigns do not create individual and collective reflections on the subject of the campaigns. This view is explained by impersonal one-way communicated messages and that the wrapping becomes more important than the content. There is a lot of information from different parts of the organizations, due to lack of motivation, information security messages are forgotten or deleted in the information overload. At the same time, the interviewed users at the IT company indicated that interaction with information security professionals and more participative approaches were assumed to be more effective. Aarø and Rise (1996) argue that pure information seldom has any effect on individual behaviour as behaviour is created by more factors than knowledge and attitudes. A literature review by Lund and Aarø (2004) show that information measures alone such as leaflets, booklets, films, postern or direct mail do not give any proven effect on behaviour or reduced risk potential.

The qualitative study of information security professionals in Paper II, shows that although few had actually made use of it, user participation was evaluated as the most effective approach to improve user behaviour by several of the interviewed managers, but also as an important tool in other information security processes, e.g. participation in risk analysis. Several interviewed users (Paper I) also believe in involvement as the most effective method to influence user behaviour and awareness, here exemplified by a citation of a female employee:

> *"The security management department should give us some information about information security and themselves… Involving us is the best way to communicate. They have to make themselves visible to us. Then we will become more interested in information security as well.. It is much better with information meetings than documents and mails."* Bente (53), ♀, IT company

Employee participation in information security is further elaborated upon in Section 5.5.

Awareness campaigns can be grouped as society-based or community-based campaigns. The society-based campaigns are characterized by use of experts, individual interventions, large population groups and communicated from authorities to single individuals. The community-based campaigns on the other hand use resources in the local community (empowerment), focus on individuals and groups and use cross-disciplinary cooperation. The study indicates that most mapped awareness creating attempts are society-based. However, community-based approaches are regarded to be more effective on individual awareness and behaviour. This is supported by safety psychology studies that show that community-based attitude campaigns often show better results than society-based campaigns (Aarø and Rise, 1996; Iversen, 2005). Participative awareness training approaches such as the intervention in Paper II is an example of community-based campaigns.

The key to successful awareness training is thus participation and convincing; telling how and why by reflection in interaction and dialogue by reflections, rather than passive information and documented requirements. The use of Facebook by organizational members provides an example of this issue. This year, the number of Norwegian members of the social networking site Facebook has exploded. There are however some risks associated with social networks. The Norwegian National Security Authority has discovered classified information in profiles of members of public administrations. The Data Inspectorate has also warned people about privacy issues, i.e. that once you publish private information in social networks you lose control of this information. Publishing sensitive information, either personal or company-related, in your profile can thus harm individual, organizational and national interests. How can a company handle this? Several possibilities are available. First, forbidding or restricting the use of Facebook in working hours by formal and technological solutions may of limited effect. Employees will have access in their spare-time, and next year there might be new Internet services that create harm. It can also be claimed that Facebook profiles are beneficial for the company as colleagues can communicate with each other as well as customers and other stakeholders, so avoidance might be opposite to functionality. Second, the privacy policy of Facebook is not reliable. According to a blog-entry by security expert Bruce Schneier[5], the policy is about 3000 words long and ends with a notice that it can change at any time – how many members ever read that policy and check back for changes? (I have to admit I did not do so when creating my profile). Third, it is possible to edit privacy preferences. My experience is that these preferences are not user-friendly, and that few members have edited these preferences to any extent. Fourth, formal and technological solutions seem to be ineffective so one should rather inform and educate employees on how to use Facebook in a sensible way. This can be done by emails,

[5] http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html

Intranet messages and telling employees face to face to consider the privacy policy, edit preferences, do not give away your work email addresses or your passwords, avoid publishing sensitive information, etc. However, the lesson learned from the paragraphs above is that *telling employees how to use Facebook is not sufficient; one has to tell why as well.* Consequently, communication should put emphasis on convincing rather than top-down persuasion, hence being based on a discursive ethical perspective (Hovden, 1998b) rather than duty ethics, which mainstream information security management is based on (Albrechtsen et al., 2006).

5.4 Interactions and social relations: social digital divide between users and information security managers

Paper II reveals a social digital divide between users and information security managers as the two groups have different views on the expectations of and experiences with information security. In addition there is a modest dialogue and interaction between them. An important difference revealed by both quantitative descriptions and qualitative understandings is that users regard themselves as a resource in information security work, while information security managers tend to mainly focus on users as a security threat or a problem than a resource.

This perspective is also reflected by the amount of literature focusing on users as the enemy within (see Section 2.4.2). Formal structures and technological solutions (see Section 5.3) are based on this underlying premise of users as a security threat. If one assumes that employees are incompetent, unreliable and lazy, is a custom choice to organize things in a way that employees do not need to think, and add control and surveillance (Schiefloe, 2003:118).

Users and information security managers have different responsibilities and spheres of authority, and employ a different rationality. Maintaining information security in an organization is the information security manager’s main work task. Users, on the other hand, have other, equally important, work tasks, mainly achieving the organization’s goals of profit and productivity. However, users have the responsibility to maintain information security since this is also one of the organization’s goals.

Figure 12 shows the levels of information security professionals and users in relation to information security tasks, interpreted from data in Paper II. The differences explain the information security digital divide in an organization. Users, on the other hand, operate at the sharp end. The figure also introduces the role of line managers and IT managers, which has not been elaborated on in the present study. They have nevertheless an important role in the information security work of an organization. According to the interviewed information security professionals, many of the strategic and operative information security decision are made by line and IT managers, often on the basis of expert evaluations made by the professionals. The decision-making situations of line and IT managers are often characterized by lack of time, information overload and the frequent necessity to make rapid decisions (Rosness, 2001). Under such conditions decision-makers are likely to base decisions on a satisfying strategy (March and Simon, 1958), i.e. they make decisions that are good enough but not necessarily the best option.

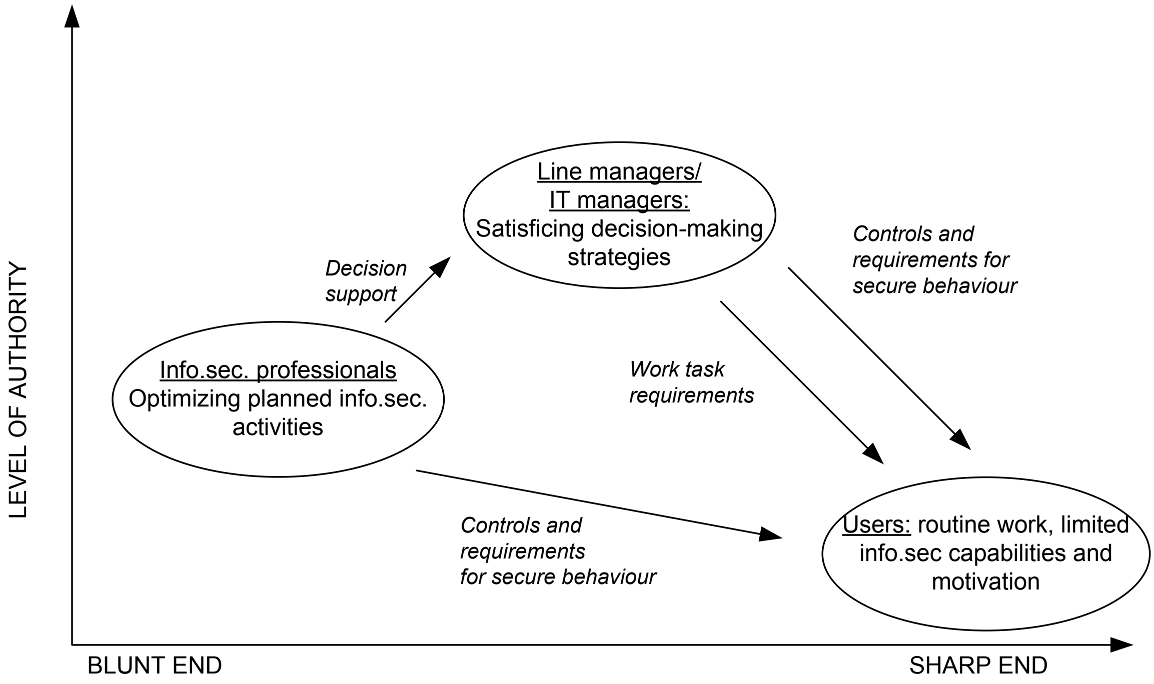
LEVEL OF AUTHORITY
Line managers/
IT managers:
Satisficing decision-making strategies
Decision support
Controls and requirements for secure behaviour
Info.sec. professionals
Optimizing planned info.sec. activities
Work task requirements
Controls and requirements for secure behaviour
Users: routine work, limited info.sec capabilities and motivation
BLUNT END
SHARP END

Figure 12. Work situations in operative information security work. Based on Rosness (2001).

Information security professionals have a degree of specialization, access to expert knowledge, time and resources for collecting and processing information, and sophisticated tools and methods for information processing. Consequently, they have time and space to optimize planned information security activities. On the other hand, since they are at the blunt end they often lack hands-on experience of the systems they influence or develop since they are not close to actual working situations and accompanying threats and vulnerabilities (Rosness, 2001; Rosness et al., 2004). The interviewed managers confirmed this by their statements that they knew little about the users' situation and that they had little interaction with users. They also said that they were seldom decision-makers; their task was to provide input to decisions made by managers in other parts of the organization. Besides decision input, the information security professionals influence users by developing strategic documents, e.g. instructions for safe and secure behaviour and formal one-way communication, such as emails.

The information security digital divide within organizations is not in itself a threat to the functionality of information security management. However, the differences in approach, experience and priorities between managers and users in this field result in management strategies based on the prejudiced view that users are more of a security threat than a resource. The information security professionals thus give the premises for the information security work in an organization without involving users to any extent. Consequently, the management approaches might be insufficient for dealing with users as a resource as the information security activities are based on non-realistic understandings of actual work at the sharp-end.

The trade-offs described in Section 5.1.1 can be explained by the interactions and relations of the actors in Figure 12. The low priority users give to information security is the result of a range of different management decisions influencing the users' total work situation. Users at the sharp end are recipients of outputs from decisions concerning information security and other work tasks made by both professionals and other management. One output of management decisions takes the form of information security measures that directly influence the working day of users at the sharp end, e.g. new technological security solutions and mandatory training programmes. However, this tends to conflict with management decisions to impose work tasks other than information security, such as requirements with respect to sales and efficiency.

5.5 Employee participation in information security

Modest attention is paid to employee participation in some public standards and guidelines in information security (see Section 2.5 and Paper V). The empirical studies in the papers reflect this scarcity. However, all papers present arguments for a participative approach to information security management:

- The qualitative interview study of users in Paper I shows that employees believe that small-sized meetings that involve users in informal discussions is the most effective tool for influencing user behaviour and awareness as this allows them to reflect on their own situation; and meet security professionals face-to-face, thus making information security management more visible.
- Paper II argues that the information security digital divide between users and managers can be closed by dialogue and interaction. This will imply that information security mangers will get an improved understanding of actual information security performance at the sharp-end, thus improving information security decision-making. In addition, users are likely to improve their understanding, motivation and acceptance of information security.
- The qualitative interviews with information security managers presented in Paper II show that employee participation is evaluated to be the most effective approach to influencing user behaviour and awareness.
- The intervention study in Paper III shows that a participatory approach to awareness training significantly improves the awareness and behaviour of participants. See 5.5.1 for further discussion
- The survey study in Paper IV shows that participation is one of three single measures that are independent significant contributors to how the respondents assess the security performance of their organizations. Consequently, involving employees is effective for producing a high level of security.
- The survey study in Paper IV also shows that employee participation is subjectively evaluated to be one of the most effective organizational information security measures.
- Paper V presents theoretical arguments for employee participation in information security based on other relevant fields of practice and research.
- Paper VI shows a potential experience transfer between the domains of industrial safety and information security. The field of industrial safety has a long tradition and

legal requirements for employee participation in systematic safety management both for identifying and solving safety problems.

5.5.1 A practical example of employee participation

The intervention study in Paper III gives a practical example of how user education can be performed by a participative approach based on dialogue and reflections, i.e. a community-based awareness campaign. The intervention study shows how direct participation can successfully improve an organization's information security performance. The intervention consisted of small-sized workshops aiming at improving information security awareness and behaviour. An experimental research design revealed significant improvements in awareness and behaviour among participants. Additionally, the information security managers in the organization improved their insight of information security processes at the sharp-end. Why did the participative intervention modify the awareness and behaviour of its participants?

- Active involvement in discussion on information security. The officers were not in command, but still present, thus leaving the word open to the participants
- The participants reflected on information security subjects and why information security is important on their own premises rather than being told what they are supposed to do, hence a convincing strategy
- Groups made it possible to take care of individual considerations and initiatives at the same time the overall picture was taken care of. In addition, groups are a meeting place for experience and knowledge transfer between managers and employees (Levin and Rolfsen, 2004).
- Organizational knowledge (Nonaka and Takeuchi, 1995) was created and shared among organizational members as the participants shared their tacit knowledge with each other combined with the expertise of the security officers. Organizational learning (Argyris and Schön, 1996) was an important result of the intervention, as the improved information security abilities among and between employees should be more long-lasting and easier maintained if shared among more people. An organization is a collective institution of interplay and coordination. Consequently, common insight into information security structures and procedures is fundamental important for coordinated information security interplay in an organization.

Paper V provides two more examples of how users can be directly involved in the information security work: an informal meeting where information security was talked about among the participants; and employees being involved in risk analysis processes.

5.5.2 How and why user participation?

►*How can employee participation occur as a part of information security?*

Participation can take many forms. One can distinguish between direct and representative/indirect participation (Walters and Frick, 2000). This thesis looks at direct participation.

Direct participation can happen in arenas for dialogue, reflection and problem solving that aim at building awareness and confidence, improving knowledge. These are important activities to utilize the potential of users as a resource and make them aware of security. By direct participation users get involved in decision-making either by giving input to decisions or by being involved in the decision-making process in some way. Examples of direct approaches to employee participation are informal meetings, focus groups and seek conferences. The workshop-based information security awareness training program in Paper III is also an example of such an approach.

Another participative activity is when employees' knowledge is utilized to improve organizational processes. For example user panels and test groups for new technology; participation in risk analysis; and organizational development methods.

Worker involvement should also happen in operative activities (Walters and Frick, 2000), e.g. delegation of authority to workers or representatives and self-management based on worker's ownership. In modern ways of organizing work, where the use of IT is decentralized and risk is distributed, such involvement of users is necessary to preserve information security, as each user's responsibility and integrity becomes important principles in systematic information security work (Dhillon and Backhouse, 2000).

Another type of participation, not discussed here is representative participation, which is a widely used approach in occupational safety (Hovden et al., in press), where it is even a legal requirement in Norway. Representative participation, typically represented by labour unions or employee spokesperson, is here looked at as an important opposition to management decisions. As a result representative participation is balancing the interests of management and the employees. Direct participation is the opposite of representative participation as direct participation implies that employees are embodied in the decision making-processes. This means that representative participation loses its right to raise objections to the decisions made.

►*Why is employee participation an essential part of information security?*
The empirical findings of this study and research literature in other fields of practice than information security (see Section 2.5) provide three groups of arguments for making employee participation an essential part of information security: 1) utility-driven, 2) humanistic and 3) political.

Utility-driven ideas are based on premises that the workforce must be collaborated with for improving all parts of information security. There are several benefits of a participative approach that is the sum should influence all the elements in the pentagon model in Figure 3. First, participation is likely to improve technological and administrative security solutions by utilizing employees' local knowledge and experiences for development of technology (Section 2.4.1) and organizations (Section 2.5 and Paper V). As a result, technology and formal and informal processes are developed in accordance with the actual context of work. The usability of security technology will improve and thus reduce the possibilities of information security trade-offs. Second, participative approaches will mean that security professionals improve their knowledge on actual security performance at the sharp-end, which will improve information security decisions and support for decisions. Third, by interactions and dialogue between users and information security professionals, the gap in understandings and communication between the two groups is likely to close, thus improving the trust between the two groups.

Humanistic arguments for workplace participation state that user participation is likely to create individual ownership, acceptance and motivation for information security. These arguments reason that job enrichment and decisional participation will be beneficial for economic efficiency and a more mentally healthy workforce, as it increases cooperativeness, reduced hostility and anxiety, and improves individuals' sense of responsibility (Greenberg, 1975). Measures taken within a humanistic school of thought improve information security in two ways. First, it is assumed that implementation of technological and administrative security measures should be easier as the members have a concrete possibility to shape their own working conditions. Second, as argued within the safety domain (Sections 2.5 and 5.3.3), it is argued that direct involvement in training and education is the approach which is most likely to improve individual attitudes, knowledge and understandings. A qualitative study by Adams and Blanford (2005) shows that employee participation in the development of security technology and formal systems improves the awareness of users. The same study shows that measures not "owned" by users create a poor view on information security among users.

Political arguments aim at ensuring workplace democracy by employees' rights to gain influence over personal conditions. Such democratic theories can take on the form of representative and full participation (Greenberg, 1975) and argue that only through participation in all aspect of social life, including the work place, can individuals develop the unexploited capacities inherent within them.

5.5.3 Arguments against employee participation

Regarding the design of secure information systems, Siponen (2002:58) argues that "user participation may be rejected by security personnel. They may see that user participation is a security threat. On the other hand, the worst possible "de facto" standard of handling users, namely to forget their views and to force security policy/procedures upon the users with punishment may be far more serious threat in the long run". This section has described the advantages of involving employees in the information security work, not only for design but also in daily operation. However, one can also argue for negative consequences of a participative approach to information security, which also partly explains the lack of participation. First, participation on a large scale is resource demanding for the organization. Second, the need-to-know principle has been an important strategy for assuring confidentiality of information systems (Gollmann, 1999). Involving employees might jeopardize this principle. Third, by looking at users as the enemy within, one can also argue that participation is an unwanted approach as it implies that malicious employees will acquire knowledge of vulnerabilities.

However, a participative approach to information security does not necessarily imply contact with sensitive information. Rather it is the processes behind the participation that are important for creating improved support for decision-making and comprehension of the information security practice among the security managers as well as improving awareness among users.

Some studies indicate that employee participation actually is only symbolic (Greenberg, 1975) or bounded (Hatling and Sørensen, 1998). Greenberg (1975) argues that a management school of thought argues for participation as one of several strategies to resolve differences between individuals and groups and thus favours an environment of peace and stability. At the same time the main objective of the school is efficiency and productivity, participation can consequently be called symbolic. Regarding designing security systems, another challenge is that user participation actually is in the hands of the designers; consequently it is argued that only bounded rather than full participation takes place (Hatling and Sørensen, 1998).

5.6 Information security management: bureaucracy, technocracy, and democracy

The discussion in this section, which is based on empirical findings of the study in combination with research literature, show that the information security management approaches directed at employees can be characterized by:

- use of technology to control and monitor user behaviour in addition to function as a fool-proof system
- use of documented descriptions of expected individual and organizational behaviour
- use of formal, one-way communicated, expert-based training and education of employees
- modest involvement of employees in the information security work
- lack of dialogue and interaction between information security professionals and users
- centralized management, with expert knowledge on information security and modest knowledge on actual work context at the sharp-end.

Powerful IS professionals are in charge of IS management, resulting in technocracy. Information security is mainly controlled with the centralized experts' knowledge, power and ability to solve problems. As information systems are distributed in the organizations, IT related risk becomes distributed as well. However, the responsibility for information security remains centralized.

Dhillon and Backhouse (2001) and Siponen and Oinas-Kukkonen (2007) have argued that information security approaches in general tends to be technology-oriented and based on formal administrative activities. The present study show that this tendency in general information security approaches is reflected in management of employees. Revisiting the pentagon model in Figure 3, one can see that most emphasis in information security management has been on the upper part of the figure: technology and formal structures.

These structures have many similarities with Weber's (1971) descriptions of bureaucracies, i.e. organizations that reach their goals of being regular, reliable and efficient by use of unambiguous distributions of tasks, monitoring and detailed rules and regulations. Such mechanical approaches might function well for some organizational contexts, but has some major limitations since such organizations has difficulties in adjusting to contextual changes; creates unexpected consequences as organizational members put their individual interest ahead of the organizations' interests and can be perceived as degrading among employees (Morgan, 1998). Like Weber (1971), Morgan (1998) presents scepticism toward bureaucratic approaches directed at humans. Mechanical definitions of job responsibility encourage thoughtlessness, like "this is not my table". When the responsibility for one task is clearly defined, the workers get an impression of what is expected by them. At the same time it give employees an understanding of what is not expected from them. There are thus two main causes why bureaucratic approaches are insufficient for information security management in modern organizations. First, bureaucratic structures will have problems to adjust to the dynamic nature of IT, organizations and the threat picture. Second, bureaucratic approaches are improper for handling the human part of information security. Morgan (1998) further argues that mechanical definitions of job responsibility encourage thoughtlessness, like "this is not my table". When the responsibility for one task is clearly defined, the workers get an impression of what is expected by them. At the same time it give employees an understanding of what is not expected from them. Employees are forced to adapt the mechanistic requirements, rather than build the security organization by their strengths. The organization, the security management and the employees are likely to suffer from such an approach.

Underlying the traditional management strategies is a thought that users can be managed by use of technological and bureaucratic inscriptions. The security of modern and dynamic information technology and the use of it is thus paradoxically managed by traditionally structured organizational approaches and perspectives. Nevertheless, there is more to modern organizations and their members than this management strategy covers (Albrechtsen and Grøtan, 2004). New approaches are thus required. Organizations today can be understood as much more than mechanical bureaucracies (Morgan, 1998; Bolman and Deal, 2003). The recent years there has been an increased emphasis on informal aspects of information security (see Chapter 2). Dhillon and Backhouse (2000) have suggested to handle the dynamics in new organizational forms by the principles responsibility and knowledge of roles; integrity as a member of an organization; trust and self control instead of external control and supervision; and ethicality as opposed to rules as equally important to the much used principles confidentiality, integrity and availability. The findings in this study reveal more participative approaches as one possible development in the field of information security to manage users' role and function in information security and contextual adjustments of information security strategies. More democratically organizational ideas are thus called for.

The traditional organizational views must however not be thrown away. First, information security is and still will be mainly a technological field of practice and research. Technological security solutions can never be substituted by other solutions and must be in place. Second, such organizational structures might function well for some organizational context, e.g. military organizations. Third, a structural framework consisting of documents, responsibilities and roles must be in place in order to perform operative information security work. Other organizational approaches than those mentioned in the list above must also be based on this structural framework. Fourth, combinations of different measures and activities are likely to be the most efficient loss prevention efforts (Lund and Aarø, 2004).

6 Conclusions

"The real danger is not that computers will begin to think like men,
but that men will begin to think like computers."
Sydney J. Harris

The empirical point of departure in the thesis is qualitative results, which per se are not generalized findings. These qualitative results are supported by quantitative studies and relevant research literature. Nevertheless, the findings in the study should not be looked at as generalized facts. Rather the thesis has explored information security management of employees by providing some understandings and interpretation of this topic.

The thesis aimed at exploring the information security management of employees. This purpose was divided into four research questions which are recapitulated in the following.

How is the role and function of regular users in operative information security efforts interpreted by users themselves and information security professionals? Users view themselves as an untapped resource in the information security work, while information security managers mainly view users as a threat and a problem to the information security level. But when it comes to operative work, users' information security performance is poor. Users perform few proactive information security actions and are indifferent to information security in their daily work

How are different measures aiming at the individual level of information security work used? Why are some solutions expected to be more efficient for this purpose than others by information security professionals? The most used non-technological information security measures directed at users are formal techno-administrative measures: technological frames; documented requirements; control and monitoring; and formal, expert-based one-way information. Face-to-face communication and employee participation is modestly used in the information security community. The more users are involved actively in the measure, the more effective is the measure evaluated to be for improving awareness and behaviour. The effect on individual behaviour and awareness from the most commonly used measures, is evaluated to be low. There is consequently a transverse relationship between use and subjectively evaluated effect.

How do differences in information security expertise, authority and priorities in an organization affect individual information security performance? Differences in approach, experience and priorities between information security managers and users result in management strategies based on the prejudiced view that users are more of a security threat than a resource. The information security professionals give the premises for the information security work in an organization without involving users to any extent. Consequently, the management approaches might be insufficient for dealing with users as a resource as the information security activities are based on non-realistic understandings of the actual work at the sharp-end.

Why is employee participation an essential part of information security? What are the effects on awareness and behaviour of an intervention based on participation and dialogue? Employee participation is likely to improve the quality of technological and administrative security solutions; improve the usability of security technology; improve security professionals' knowledge on sharp-end information security activities; close the gap in understanding and communication between security managers and users; improve individual ownership, acceptance and motivation for information security; and ensure democratic rights to influence over personal working conditions. Paper III shows that participation in a workshop where participants reflected on information security significantly improved the awareness and behaviour among the participants compared to a group of non-participants.

Paradoxically, users are both a friend and a foe in information security management. Employees are a precondition for safe and secure operation as well as incubating threats and vulnerabilities. The awareness and behaviour of employees are important contributions to preserving security along with other information security processes. On the other hand, employees are also a threat and vulnerability to the security level. Traditionally, most emphasis has been placed on the problem side of this dual face of users, which also is reflected in management approaches. The main challenge of the function of employees in information security work is that information security is not the main work task of most employees it is rather one of many sub-goals. Convincing employees that their contribution is essential is thus important. The key here is not only to tell how they should contribute, but have a dialogue on what and why they should contribute and why most of their security actions are simple and not time-consuming.

By collaborating with and involving employees, information security professionals should improve their understanding of sharp-end security and as a consequence develop more user-friendly technological and administrative information security solutions. According to Ashby's law of requisite variety, to gain control over a system one must be able to generate measures at a rate corresponding to the rate of variety that the observed system can exhibit (Kjellén, 2000). Consequently, combinations of adequate measures for all parts of the socio-technical information security systems must be available in order to perform efficient defence, including the handling of the employees' function in information security. One needs to handle pragmatic, formal rule-based and technical principles (Dhillon, 2001a). Managing the human element of information security is thus one of many activities in information security management. The thesis has identified some shortcomings in the current approaches to employees. These shortcomings may not be inadequate for other information security efforts than man management, so the current approaches must not be thrown away. This thesis has argued for more user participative approaches as a complementary addition to traditional information security approaches.

6.1 Further work

The findings in the thesis indicate possibilities for further research:

Only the roles and interplay of users and information security managers in staff functions have been addressed in the present study. Other important information security actors in the organization are line managers; IT managers and professionals; and top managers. To draw a total picture of information security processes in organizations, studies of these functions should be done regarding decision-making by IT managers and line managers and top managements' engagement in information security.

The explorative nature of parts of the empirical studies of the thesis invite more quantitative studies. Hypotheses based on the qualitative findings can be tested for generalization

Intervention studies, in a similar approach as in Paper III, should be performed on other information security measures, to evaluate whether measures have an intended effect or not, e.g. to test if interactive learning actually leads to changes in knowledge. .

More studies on could be done how and why different participative approaches to information security function. These could be user panels aiming at improving technological solutions and participation in risk analysis.

Studies on the users' role in the future are another area. There are clearly differences in computer skills and knowledge between different age groups. What happens when those who have grown up with computers and the Internet from birth are the main group of workers? This might create new challenges, since it can be assumed that many of these have expertise making it possible to do more harm than current employees with average computer skills. At the same time it might be assumed that this new working group possesses improved information security awareness compared to the average worker today. What can be expected, and how can future challenges and advantages be handled?

References

Adams, A. and Blandford, A. (2005). “Bridging the gap between organizational and user perspectives of security in the clinical domain”. *International Journal of Human-Computer Studie*s. **63**(1-2): 175-202

Adams, A. and Sasse, M.A. (2005). ”Users are not the enemy”. *Communications of the ACM,* **42**(19): 41-46.

Adler, P.S. and Winograd, T.A. (1992). “The Usability Challenge”. In Adler, P. S. and Winograd, T. A. (eds.) *Usability - turning technologies into tools*. New York: Oxford University Press**:** 3-14.

Albrechtsen, E. and Grøtan, T. O. (2004). “Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner”. In Norwegian [Old-fashioned thinking in modern organizations? On ICT security in knowledge organizations] In Lydersen (ed.), *Fra flis i fingeren til ragnarok : tjue historier om sikkerhet.* Trondheim: Tapir Akademisk: 335-355

Albrechtsen, E., Hovden, J. and Grøtan, T. O. (2006). “Ethical issues in information security management”. Extended abstract presented at *the European Computing and Philosophy Conference*, June 2006, Trondheim, Norway.

Argyris, C. and Schön, D. A. (1996). *Organizational learning II: theory, method, and practice*. Reading, Mass.: Addison-Wesley.

Beck, U. (1992). *Risk society: towards a new modernity*. London: Sage.

Besnard, D. and Arief, B. (2004). "Computer security impaired by legitimate users." *Computers & Security* **23**(3): 253-264.

Bogen, L. (2005). ”Organisering av IT-sikkerhet i statlig sektor”. In Norwegian [Organizing IT security in the public sector]. Master thesis at, *the Department of Industrial Economics and Technology Management. Norwegian University of Science and Technology,* Trondheim, Norway

Bolman, L. G. and Deal, T. E. (2003). *Reframing organizations: artistry, choice, and leadership*. San Francisco, Ca: Jossey-Bass.

Braverman, H. (1974). *Labor and monopoly capital: the degradation of work in the twentieth century*. New York: Monthly Review Press.

Brunsson, N. (1989). *The organization of hypocrisy: talk, decisions and actions in organizations*. Chichester: Wiley.

Clarke, S. and Drake, P. (2002). “A Social Perspective on Information Security: Theoretically Grounding the Domain”. In Clarke, S., Coakes, E., Hunter, G.M., Wenn, A (eds.), *Socio-technical and Human Cognition Elements of Information Systems*. Hershey, PA, USA: IGI Publishing.**:** 249-265.

Cox, S. and Flin, R. (1998). "Safety Culture: philosopher's stone or man of straw?" *Work and Stress* **12**(3): 189-201.

Dhillon, G. (2001a). *Information Security Management. Global Challanges in the New Millennium*. London, Idea Group Publishing.

Dhillon, G. (2001b). "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." *Computers & Security* **20**(2): 165-172.

Dhillon, G. and Backhouse, J. (2000). "Information System Security Management in the New Millenium." *Communications of the ACM* **43**(7): 125-128.

Dhillon, G. and Backhouse, J. (2001). "Current directions in IS security research: towards socio-organizational perspectives." *Information Systems Journal* **11**(2): 127-153.

Dhillon, G. and Moores, S. (2001). "Computer crimes: theorizing about the enemy within." *Computers & Security* **20**(8): 715-723.

Ehn, P. (1992). “Scandinavian Design: On participation and Skill.” In Adler, P. S. and Winograd, T.A. (eds). *Usability - turning technologies into tools*. New York, Oxford University Press**:** 96-131.

Frank, J., Shamir, B. and Briggs, W. (1991). "Security-related behavior of PC users in organizations." *Information & Management* **21**(3): 127-135.

Flin, R, Mearns, K., O’Connor, P. and Bryden, R. (2000). “Measuring safety climate: identifying the common features” Safety Science **34**(1-3): 177-192

Furnell, S. (2005). "Why users cannot use security." *Computers & Security* **24**(4): 274-279.

Furnell, S. M., Jusoh, A. and Katsabas, D. (2006). "The challenges of understanding and using security: A survey of end-users." *Computers & Security* **25**(1): 27-35.

Goldenhar, L. M. and Schulte, P. A. (1994). " Intervention research in occupational health and safety,." *J Occup Med* **36**(7): 763-775.

Gollmann, D. (1999). *Computer security*. Chichester, Wiley.

Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Service*. Computer Security Institute.

Greenberg, E. S. (1975). "The Consequences of worker participation: A clarification of the theoretical literature." *Social Science Quarterly* **56**(2): 191-209.

Greenwood, D. J. and Levin, M. (1998). *Introduction to action research : social research for social change*. Thousand Oaks, Calif., Sage Publications.

Groth, L. (1999). *Future organizational design: the scope for the IT-based enterprise*. Chichester, Wiley.

Guldenmund, F. W. (2000). "The nature of safety culture: a review of theory and research." *Safety Science* **34**(1-3): 215-257.

Hale, A. R. (2000). "Culture's confusions." *Safety Science* **34**(1-3): 1-14.

Hale, A.R. and Hovden, J. (1998). ”Management and Culture: the third age of safety.” In A.M. Feyer & Wlliamson, A. (eds.) *Occupational Injury. Risk Prevention and Intervention.* London: Taylor & Francis.

Hammersley, M. (1996). “The Relationship between qualitative and quantitative research: Paradigm loyalty versus methodological eclecticism.” In Richardson, J.T.E. (ed.), *Handbook of qualitative research methods for psychology and the social sciences*. Leicester, UK, The British Psychological Society.

Hatling, M. and Sørensen, K. H. (1998). “The construction of user participation.” In Sørensen, K.H. (ed.), *The Spectre of participation: technology and work in a welfare state*. Oslo, Norway, Scandinavian Univ. Press.**:** 171-188.

Hodge, B.J., Anthony, W.P., Gales, L.M. (1996). *Organization Theory. A strategic Approach*. Upper Saddle River, NJ: Prentice-Hall

Hollnagel, E. (2004). *Barriers and accident prevention*. Aldershot, Ashgate.

Hollnagel, E., Woods, D. D. and Leveson, N. (2006). *Resilience engineering: concepts and precepts*. Aldershot, Ashgate.

Hovden, J, Ingstad, O, Mostue, B.A., Rosness, R, Rundmo, T, Tinnmansvik, R.K. (1992). *Ulykkesforebyggende arbeid,* In Norwegian [Accident prevention] Oslo, Yrkeslitteratur

Hovden, J. (1998a). "The ambiguity of contents and results in the Norwegian internal control of safety, health and environment reform." *Reliability Engineering & System Safety* **60**(2): 133-141.

Hovden, J. (1998b). “Ethics and Safety: "mortal" questions for safety management”. Paper presented at *Safety in Action,* Melbourne 1998.

Hovden, J. (2003). “Theory Formations related to the "Risk Society".” Paper presented at *NoFS XV 2003*, Karlstad, Sweden.

Hovden, J., Lie, T., Karlsen, J. E. and Alteren, B. (in press). "The safety representative under pressure. A study of occupational health and safety management in the Norwegian oil and gas industry." *Safety Science*

Hubbard, W. (2002). *Methods and Techniques of Implementing a Security Awareness Program*. SANS Institute white paper

Ilstad, S., Paasche, T. and Hovden, J.(1977).. *Survey-metoden.* In Norwegian [Survey methods] Trondheim, Tapir.

ISF Information security forum. (2005). *The Standard of Good Practice for Information Security,* Version 4.1

ISO17799 (2000). Information Technology - Code of practise for information security management.

Iversen, H., Rundmo, T. and Klempe, H. (2005). "Risk Attitudes and Behavior Among Norwegian Adolescents: The Effects of a Behavior Modification Program and a Traffic Safety Campaign." *European Psychologist* **10**(1): 25-38.

Irgens Karlsen, J. and Veium, K. (1986). *Fra analyse til handling: praktisk organisasjonsutvikling*. In Norwegian [From analysis to action: practical organizational development] Oslo, Bedriftsøkonomens forlag.

Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003). "Security and human computer interfaces." *Computers & Security* **22**(8): 675-684.

Kjellén, U. (2000). *Prevention of accidents through experience feedback*. London, Taylor & Francis.

Kraemer, S. and Carayon, P. (2007). "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists." *Applied Ergonomics* **38**(2): 143-154.

Kristensen, T. S. (2005). "Intervention studies in occupational epidemiology." *Occup Environ Med* **62**(3): 205-210.

Koh, K. Ruighaver, A.B. Maynard, S. and Ahmad, A.(2005) “Security Governance: Its impact on Security Culture.” Proceedings of the 3 rd *Australian Information Security Management Conference*, Perth, Australia , September 2005.

Kotulic, A.G. and Clark, J.G (2004) “Why there aren’t more information security research studies”. Information & Management, **41**(5): 597-607

Kvale, S. (1997). *Det kvalitative forskningsintervju*. In Norwegian [Interviews: an introduction to qualitative research interviewing] Oslo, Ad notam Gyldendal

Latour, B. (1987). *Science in action : how to follow scientists and engineers through society*. Milton Keynes, Open University Press.

Latour, B. (1991). “Technology is society made durable.” In Law, J (ed.), *A sociology of monsters. Essays of power, technology and domination* .London, Routledge

Law, J. (1992). “Notes on the theory of actor-network: ordering, strategy and heterogeneity.” *Systems practise*, **5**(4) : 379-393

Leach, J. (2003). "Improving user security behaviour." *Computers & Security* **22**(8): 685-692.

Leiulfsrud, H. and Hvinden, B (1996). ”Analyse av kvalitative data: Fikserbilde eller puslespill?” In Norwegian [Qualitative data analysis: puzzle picture or jigsaw puzzle?] In Holter, H. and Kalleberg, R. (eds.), *Kvalitative metoder i samfunnsvitenskapene*. Oslo, Norway, Universitetsforlaget.

Levin, M. and Klev, R. (2002). *Forandring som praksis : læring og utvikling i organisasjoner*. In Norwegian [Changes in practice: learning and development in organizations] Bergen, Fagbokforlaget.

Levin, M. and Rolfsen, M. (2004). *Arbeid i team: læring og utvikling i team*. In Norwegian [Work in team: learning and development in teams] Bergen, Fagbokforlaget

Lund, J. and Aarø, L. E. (2004). "Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors." *Safety Science* **42**(4): 271-324.

Magklaras, G. B. and Furnell, S. M. (2001). "Insider Threat Prediction Tool: Evaluating the probability of IT misuse." *Computers & Security* **21**(1): 62-73.

March, J. G. and Simon, H. A. (1958). *Organizations*. New York, Wiley.

Miles, M. B. and Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. Thousand Oaks, Calif., Sage.

Mitnick, K. D. and Simon, W. L. (2002). *The art of deception : controlling the human element of security*. Indianapolis, Ind., Wiley.

Morgan, G. (1998). *Images of organization*. San Francisco, Berrett-Koehler Publishers.

Neuman, P. G. (1999). "Inside risks: risks of insiders." *Communications of the ACM* **42**(12): 160-160.

Nonaka, I. and Takeuchi, H. (1995). *The knowledge-creating company: how Japanese companies create the dynamics of innovation*. New York, Oxford University Press.

Norwegian Ministry of Trade and Industry (2003), *National Strategy for Information Security*

OECD (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*

Perrow, C. (1999). *Normal accidents: living with high-risk technologies*. Princeton, N.J., Princeton University Press.

Perrow, C. (2007). *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton, N.J., Princeton University Press.

Post, G. V. and Kagan, A. (2007). "Evaluating information security tradeoffs: Restricting access can interfere with user tasks." *Computers & Security* **26**(3): 229-237.

Rasmussen, J. (1982). "Human errors: a taxonomy for describing human malfunction in industrial installations." *Journal of Occupational Accidents* **4**: 311-33.

Rasmussen, J. (1997). "Risk management in a dynamic society: a modelling problem." *Safety Science* **27**(2-3): 183-213.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot, Ashgate.

Ringdal, K. (2001). *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode*. In Norwegian [Unity and diversity: social science and quantitative methods] Bergen, Fagbokforlaget

Robson, L. S., Shannon, H. S., Goldenhar, L. M. and Hale, A. R. (2001). *Guide to evaluating the effectiveness of strategies for preventing work injuries: how to show whether a safety intervention really works.* NIOSH Publication No. 2001-119

Rosness, R. (2001). *Om jeg hamrer eller hamres, like fullt så skal der jamres. Målkonflikter og sikkerhet.* In Norwegian [Goal conflicts and safety]. SINTEF report no.STF38 A01408M

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K. and Herrera, I. A. (2004). *Organisational accidents and resilient organisations: five perspectves*. Trondheim, SINTEF, Industrial Management, Safety and Reliability. SINTEF report no. STF38 A04403

Ruighaver, A. B., Maynard, S. B. and Chang, S. (2007). "Organisational security culture: Extending the end-user perspective." *Computers & Security* **26**(1): 56-62.

Rundmo, T. (1990). *Atferdsvitenskaplig sikkerhetsforskning*. In Norwegian [Safety reserach on behaviour]. SINTEF report STF75A9007

Sasse, M. A., Brostoff, S. and Weirich, D. (2001). "Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* **19**(3): 122.

Schiefloe, P. M. (2003). *Mennesker og samfunn: innføring i sosiologisk forståelse*. In Norwegian. [Humans and society: introduction to sociology] Bergen, Fagbokforl.

Schiefloe, P. M. and Vikland, K. M. (2006). “Formal and informal safety barriers: The Snorre A incident.” Presented at *ESREL 2006*, Estoril, Portugal, Taylor & Francis.

Schneier, B. (2000). *Secrets and lies : digital security in a networked world.* New York, Wiley.

Schultz, E. (2002). "A framework for understanding and predicting insider attacks." *Computers & Security* **21**(6): 526-531.

Schultz, E. (2004). "Security training and awareness--fitting a square peg in a round hole." *Computers & Security* **23**(1): 1-2.

Schultz, E. (2005). "The human factor in security." *Computers & Security* **24**(6): 425-426.

Shannon, H. S., Robson, L. S. and Guastello, S. J. (1999). "Methodological criteria for evaluating occupational safety intervention research." *Safety Science* **31**(2): 161-179.

Shaw, E., Ruby, K. G. and Post, J. M. (1998). "The insider threat to information systems. The psychology of the dangerous insider." *Security Awareness Bulletin*(2): 1-10.

Shrader-Frechette, K. S. (1991). *Risk and rationality : philosophical foundations for populist reforms*. Berkeley, Calif., University of California Press.

Silverman, D. (2006). *Interpreting qualitative data: methods for analyzing talk, text and interaction*. London, Sage.

Siponen, M.T. (2000). “A conceptual foundation for organizational information security awareness” Information Management & Computer Security. **8**(1): 31-43

Siponen, M. T. (2002). Designing Secure Information Systems and Software. PhD thesis at the *Department of Information Processing Science and Infotech. University of Oulu, Finland,*

Siponen, M. T. and Oinas-Kukkonen, H. (2007). "A Review of Information Security Issues and Respective Research Contributions." *Database for Advances in Information Systems* **38**(1): 60.

Sklet, S. (2006). "Safety barriers: Definition, classification, and performance." *Journal of Loss Prevention in the Process Industries* **19**(5): 494-506.

Slovic, P. (2000). *The perception of risk*. London, Earthscan.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005). "Analysis of end user security behaviors." *Computers & Security* **24**(2): 124-133.

Strauss, A. L. and Corbin, J. M. (1998). *Basics of qualitative research: techniques and procedures for developing grounded theory*. Thousand Oaks, Calif., Sage Publications.

Taylor, F. W. (1911). *The Principles of scientific management*. New York, Harper & Brothers.

Thagaard, T. (2003). *Systematikk og innlevelse: en innføring i kvalitativ metode*. In Norwegian [Systematic and insight: introduction to qualitative methods] Bergen, Fagbokforl.

Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005). "The insider threat to information systems and the effectiveness of ISO17799." *Computers & Security* **24**(6): 472-484.

Trist, E. (1981). *The evolution of socio-technical systems: a conceptual framework and an action research program*. Toronto, Ontario Quality of Working Life Centre.

Trist, E. and Bamforth, K. W. (1951). "Some social and psychological consequences of the longwall method of coal getting." *Human Relations* **4**(1): 3-38.

Trochim, W.M. (2006) The Research Methods Knowledge Base, Accessed 05/10/2007 at www.socialresearchmethods.net/kb/ (version current as of 20/10/2006).

Undheim, J.O. (1996). Innføring i statistikk og metode for samfunnsvitenskaplige fag. In Norwegian [Introduction to statistics and methods in social science] Oslo, Universitetsforlaget

von Solms, B. (2000). "Information Security -- The Third Wave?" *Computers & Security* **19**(7): 615-620.

von Solms, B. and von Solms, R. (2005). "From information security to...business security?" *Computers & Security* **24**(4): 271-273.

Voss, B. D. (2001). *The Ultimate Defense of Depth: Security Awareness in Your Company.* SANS Institute white paper

Walters, D. and Frick, K. (2000). Worker Participation and the Management of Occupational Health and Safety: Reinforcing or Conflicting Strategies. *Systematic occupational health and safety management: perspectives on an international development*. Frick, K., Langaa Jensen, P., Quinlan, M. and Wilthagen, T. Amsterdam, Pergamon**:** 43-66.

Weber, M. (1971). *Makt og byråkrati: essays om politikk og klasse, samfunnsforskning og verdier*. In Norwegian [Power and bureaucracy] Oslo, Gyldendal.

Weisbord, M. R. (1978). *Organizational diagnosis: a workbook of theory and practice*. Reading, Mass., Addison-Wesley.

Whitman, M. E. (2003). "Enemy at the gate: threats to information security." *Communications of the ACM* **46**(8): 91-95.

Whitman, M. E., Townsend, A. M. and Aalberts, R. J. (2001). "Information Systems Security and the Need for Policy".In Dhillon, G. (ed.), *Information Security Management: Global Challenges in the New Millennium*. London, Idea Group Publisher**:** 19-35.

Wood, C. C. and Banks, Jr. (1993). "Human error: an overlooked but significant information security problem." *Computers & Security* **12**(1): 51-60.

Aarø, L. E. and Rise, J. (1996). Den menneskelige faktor. Kan ulykker forebygges gjennom holdningspåvirkning? In Norwegian [The Human Factor. Can accidents be prevented by attitude modification?] Skadeforebyggende forum report 5-96.

PART II

PAPERS

PAPER I:

Albrechtsen, E. (2007).

“A qualitative study of users’ view
on information security”.

Computers & Security, vol.26, iss.4, pp.276-289

available at www.sciencedirect.com

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A qualitative study of users' view on information security

Eirik Albrechtsen

Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, N-7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 10 January 2006
Revised 30 October 2006
Accepted 6 November 2006

Keywords:
Information security
Information security management
Users
Awareness
Behaviour
Participation
Qualitative research

ABSTRACT

Users play an important role in the information security performance of organisations by their security awareness and cautious behaviour. Interviews of users at an IT-company and a bank were qualitatively analyzed in order to explore users' experience of information security and their personal role in the information security work. The main patterns of the study were: (1) users state to be motivated for information security work, but do not perform many individual security actions; (2) high information security workload creates a conflict of interest between functionality and information security; and (3) documented requirements of expected information security behaviour and general awareness campaigns have little effect alone on user behaviour and awareness. The users consider a user-involving approach to be much more effective for influencing user awareness and behaviour.

1. Introduction

The information security role of users is an important part of a holistic approach to information security management. Dhillon and Backhouse (2000) have argued that the role, responsibility and integrity of users are important principles of information security management in new forms of organisations, which can be characterized by blurred organisational and geographical borders; use of mobile equipment; and information and knowledge being the organisation's most important resources. Users should play an active part in the information security work by preventing unwanted incidents; protecting an organisation's material and immaterial assets; and reacting to incidents. Users can contribute with several security actions in their daily work, e.g. locking the computer when absent from it; password etiquette; cautious use of e-mail and Internet; avoid using unlicensed software; cautious use of organisational assets when working outside the organisation; and reporting information security breaches. A user can be characterized as a person with legitimate access to the organisation's information systems. This study concentrates itself on users with no management responsibility and low degree of information security awareness and knowledge about information systems.

This paper aims at providing knowledge of users' experience of information security and their individual security role in daily work. This purpose is approached by qualitative interviews of users at a Norwegian bank and a Norwegian

E-mail address: eirik.albrechtsen@iot.ntnu.no
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.11.004

IT-company. The following research questions are discussed in the paper:

- How do users experience their own information security role and the administrative information security measures in their work processes?
- Why do users experience the information security work the way they state?
- Are there arguments in the users' views on information security that imply alternative approaches to information security management at the studied companies?

Editorials of this journal have called for more papers on the human factor in information security (Schultz, 2004, 2005). Current human related information security research has been categorized into four main directions by Stanton et al. (2005): (1) user interfaces of security-related systems; (2) information security management concerns for risk, business processes and finance; (3) organisational issues related to information security behaviour; and (4) counterproductive computer usage. This paper positions itself into the third line by studying users' understandings of organisational issues related to individual information security behaviour, as the study mainly is about administrative aspects, and does not discuss users' views on technological security measures.

A user's view on information security is created by several interlocking organisational, technological and individual factors. The context of a user's work may, e.g. create information security trade-offs. Furthermore, social norms and interactions at the work place influence individual understanding of information security. The quality of information security management also affects users' awareness, motivation and behaviour in some way. Technological information security solutions influence users by framing what it is possible for users to do in information systems as well as function as a foolproof security mechanism for whatever actions users may do. Individual factors such as motivation, knowledge, attitudes, values and behaviour also influence individual views on information security. How people perceive risk is also a part of the explanation for users' view on information security. The paper mainly explains users' experiences of information security by organisational factors. It is, however, impossible to neglect individual and technological factors in this exploration due to the interwoven relations between organisation, technology and individuals.

2. Users' role in information security

The information security function of each user is an important part of information security. Users are often the weakest link in the information security chain (Schneier, 2000), as users might be a single or the least reliable barrier to prevent unwanted incidents. Hence, users should contribute with information security actions such as cautious use of e-mail and password etiquette. Loss prevention behaviour is created by a combination of several factors (Aarø and Rise, 1996): personal characteristics; administrative structures; technological and physical inscriptions; and social norms. As a result, possible information security weaknesses related to user behaviour should not only be explained by individual failures and violations but rather by mechanisms in the individual's context that generates the behaviour (Rasmussen, 1997).

Consequently, an important part of information security management is to deal with and to understand users' function within their work context.

Human barriers are more unreliable than technological measures (Rasmussen, 1982), which imply challenges for information security management of users: what measures should be used to successfully influence users' behaviour and awareness? Lund and Aarø (2004) have argued that programs combining different kinds of measures, i.e. information campaigns, education, rewards, technological/physical measures, legislation, and enforcement, have the most positive effect on risk behaviour. In that way, the effect on security behaviour is larger than the sum of the effects of the single measures. The field of information security has traditionally mainly been directed towards technological problems and solutions, and has lacked attention to socio-organisational and human aspects (Dhillon and Backhouse, 2001). The administrative approach to information security has mainly been structured around legal regulations; standards such as ISO17799; documented policies and procedures for individual and organisational behaviour; control and monitoring; and distribution of privileges, all controlled by powerful information security professionals (Albrechtsen and Grøtan, 2004). Recent years, there has been a trend of making information security ''softer'' by focusing on cultural aspects, e.g. by OECD (2002). This trend is also revealed in an increased emphasis on awareness campaigns in several companies, e.g. information on certain risks and how to minimize them such as leaflets, films, posters and direct mail.

Information security is one of many requirements in the working day of employees and employers. Besnard and Arief (2004) have argued that users probably will overlook security if this allows them to ease their work when information security tasks are felt to inhibit the completion of their work tasks. Wilde's (1982) risk homeostasis theory explains such individual safety trade-offs by the person's risk perception and her risk acceptance criteria, i.e. people adjust their behaviour in order to balance individual perceived and acceptable risk. Perceived and acceptable risk is influenced by a wide range of psychological and contextual factors. Slovic (2000) shows that risk is subjectively decided by individuals who may be influenced by a wide range of psychological, social, institutional and cultural factors. Cultural and organisational factors (e.g. Douglas and Wildavsky, 1982) are important for understanding risk behaviour. Risk related to information systems is one of today's produced uncertainties contributing to Beck's (1992) characteristic of a risk society. Consequently, macro-sociological factors are also important for understanding risk perception and behaviour.

In goal conflicts between acceptable risk and functionality at the sharp end, individuals tend to put emphasis on efficient and least-effort work instead of loss prevention (Rosness, 2001). In a work day full of all kinds of different interests and demands, decision makers are likely to choose a satisficing strategy (March and Simon, 1958), i.e. they seek action that is good enough rather than choose the right alternative of action based on security considerations.

Rasmussen (1997) gives an explanation of possible consequences and causes of trade-offs by arguing that a systematic migration towards unacceptable risk performance is created. The migration originates in a pressure toward efficiency provided by management and a gradient of least effort provided by operators. In addition, information security management functions as a counter gradient pushing the migration away from the boundary of unacceptable risk performance. This is illustrated in Fig. 1, where pressures from economic efficiency, the human desire for least effort and security work creates migrating human behaviour within the space of boundaries of economic failures, unacceptable workload and unacceptable risk.

3. The study

The research questions were approached by analysing qualitative data from two interview studies of users in a service centre at a Norwegian IT-company and in a department of customer counselling at a Norwegian bank. The two cases were chosen because the researcher had cooperated with security professionals at the companies on past occasions, thus the security professional functioned as gatekeepers for the interviews. Both cases were interesting to study as they are organisations where information security is essential for business. The IT-company was particular interesting to study since they recently had carried out several mass-media based awareness campaigns.

Prior to the interviews, talks with information security professionals at the studied companies were made. The professionals were asked to describe the administrative security processes and their expectations and impressions of users in the information security work. Additionally, information security documents at the companies, e.g. guidelines for cautious use of e-mail, were studied.

3.1. *Interview method and analysis*

The research questions were transformed to qualitative interviews. Eighteen interviews were conducted with duration of about 1 h each. There were nine interviews in each of the studied companies. Interviews will generate knowledge in interaction with informants by collecting and interpreting the interviewees' perception of the world (Kvale, 1996). Consequently, the interviews in the study create a deep understanding of users' experiences of information security.

The number of respondents was decided due to three reasons: (1) the exploring nature of qualitative research; (2) practical conditions; and (3) theoretical saturation. The aim of the study was not to generalize, but to interpret some users' experiences of information security. Consequently, a too high number of informants will make thorough interpretations of the interviews impossible (Kvale, 1996). The common question of 'how many interview objects are needed' can according to Kvale (1996) be answered simply: 'interview the number of persons that is needed to find out what you need to know'. This approach is given support by Strauss and Corbin (1998, p. 292) who has argued that data collection should continue ‘‘until theoretical saturation takes place. This simply means (within the limits of available time and money) that the researcher finds that no new data are being unearthed. Any new data would only add, in a minor way, to the many variations of major patterns''. This was the case for the current study as well. Due to practical reasons at the studied companies, it was not possible to get access to more informants. More importantly, theoretical saturation took place. The interviewed users' views on information security produced some general patterns with very few contrasting opinions to those patterns. The study showed that the last conducted interviews at both companies did not produce any new insight into the users' view on information security.

In qualitative data analysis the data reduction, data display, conclusion drawing and verification are interwoven before, during and after data collection (Miles and Huberman, 1994). This iterative approach was utilized in the current study. For example, during data collection and transcription, possible ideas and questions were recorded. These ideas and questions were later tested on the data material. The transcribed interviews were coded in HyperRESEARCH (a software

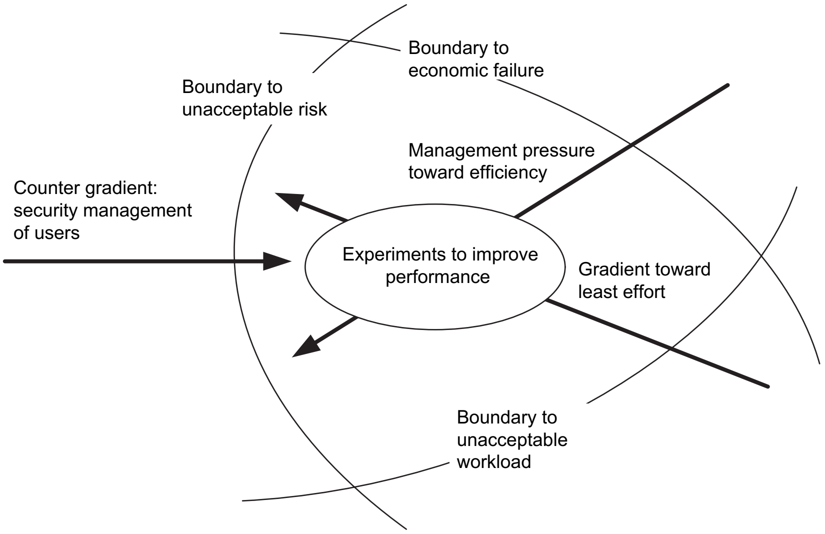
Boundary to economic failure
Boundary to unacceptable risk
Management pressure toward efficiency
Counter gradient: security management of users
Experiments to improve performance
Gradient toward least effort
Boundary to unacceptable workload

Fig. 1 – Under presence of strong gradients, behaviour is likely to migrate toward a boundary of unacceptable risk. Adapted from Rasmussen (1997).

tool for analysis of qualitative data). These codes were categorized in relation to the research questions. The categorized data was analyzed by switching between the whole picture and details by (Leiulfsrud and Hvinden, 1996): (1) testing the registered ideas during data collection, transcription and coding; and (2) using detailed data material as pieces in a jigsaw puzzle. The aim of this approach was to map and inquire into patterns of the data material; reasons for this pattern; and contrasts of the patterns.

Qualitative research can be evaluated by assessing credibility, confirmability and transferability (Thagaard, 2002). The description of the research process support the credibility of the results, as it is possible to get an impression of how the data was collected and analyzed. Furthermore, credibility is generated by drawing conclusions from the data material during the whole process. In that way the results are anchored in the informants' reflections. The results and the discussion are as one would expect coloured by the researcher's thoughts, as he cannot leave his body and soul during collection and analysis of data. Nevertheless, during the interviews the researcher tried to avoid influencing the informants, by being a discussion partner who listened to the informants and make them reasoning on the subjects of the interview.

Confirmability is created by developing research questions from theory; by continuous control during interviews; and exact transcription. Furthermore, a summary based on the transcribed interview was sent by e-mail to the informants for control and acceptance. Half of the informants responded to this the e-mail, none of them had comments or corrections. Furthermore, the results and conclusions were presented and discussed at a group meeting at the IT-company and in a meeting with the bank's security manager. None of them had any contradictory comments to the results and conclusions. In addition, the interpretations of the results were compared to results in scientific publications relevant for the study.

The results of the study are not generalized facts, but understandings of processes in the particular context of the two studied companies. Rather than generalizing the results, one should consider whether the results are transferable to other conditions, processes and people. Below the two studied companies are described in order to give an understanding of the contexts the results originate from, thus strengthening the possibility to transfer the results to other contexts.

3.2. *Description of the studied companies*

In this section, the contexts of the two companies are described by presenting the work tasks of the interviewed users; the organisation's information security work; and characteristics of the informants.

3.2.1. *Service centre at an IT-company*

The main work task of the service centre is support of systems and other business areas in the company. A typical task is to receive an error regarding a customer's address, find the reason for this error, and fix the problem in a database. The operators at the service centre only have access to data, not to the database designs. There are 15 employees in the department, of which only two are men. Nine female users were interviewed ranging from 30 to 60 years old. All of them had been employed for a long period at the company, and few of them had higher education. None of them had any management responsibility.

Besides technological security measures that inscribe patterns of use, the individual security work at the IT-company is centred on documented rules and guidelines; and awareness campaigns. According to one of the information security managers at the company is it expected that users follow the information security rules and guidelines. The recent years several mass-media based awareness campaigns have been arranged, e.g. posters and pamphlets often with a humoristic twist or a small gift with a security message attached. The last campaign before the interviews was arranged about half year before the interviews were conducted. That campaign contained a small box of chocolate containing a pamphlet carrying a message of cautious use of e-mail that was distributed to all employees in the company.

3.2.2. *Bank*

The interviewed users at the bank work as consultants for private and corporate costumers. This service includes all kinds of bank consultations by phone or e-mail, and face-to-face meetings regarding, e.g. insurance and loans. The bank's security management system is centred on a security handbook. The book is short and user-friendly, and is available at the bank's intranet. The handbook gives a nice description of what might be expected of users in the information security work, e.g. password etiquette; careful use of moveable units; saving and handling of sensitive information; and cautious use of the Internet and e-mail. The security handbook was revised half a year before the interviews were conducted. At the time of the interviews the modified handbook was not presented to the users, but was available at the intranet. Consequently, the security manager did not assume that the informants were familiar with the handbook. Furthermore, there have been some sporadic department meetings on information security topics. Some of the informants had participated in these meetings.

There were eight men and one woman among the informants ranging from 30 to 60 years. Most of the informants had worked within banks for decades and had higher education. The IT-systems are an essential working tool at the bank as it is impossible to carry out the work without the systems available.

4. Results

This section presents the major patterns in the data material. Three main findings are presented: users' view on their information security role and responsibility; users' perception of functionality issues related to information security; and users' evaluation of behavioural effects of information security measures. First, an interpretation of the informants' information security awareness is presented. This presentation of awareness among the informants is valuable in order to understand the context which the results of the study originate from.

4.1. *Information security awareness*

There was evidence of both a high and a low degree of information security awareness, i.e. the extent to which organisational members understand the importance of information security; the level of security required by the organisation and their individual security responsibilities; and act accordingly (ISF, 2005), among the informants. Altogether there were more negative indications than indications pointing to a high degree of information security awareness. On the positive side, the informants at the two companies generally viewed information security as important to themselves and the company. They also stated that they were motivated for contributing to the information security work.

On the other hand, there was indications that the information security awareness was inadequate: each individual performed very few information security actions; the informants were not familiar with possible threats; the interviewed users were not aware of possible consequences of security breaches; the informants did not see many problems or potentials of improvement in their own working conditions; and some of the informants could not see the value of their information security role in the holistic security work of the company.

4.2. *Users are motivated for individual information security work, but do not know how to perform*

The informants state that they have an important role to play in the information security work and are familiar with the information security responsibilities they have. This is neatly expressed by a female operator at the IT-company:

> *If my behaviour isn't safe and secure, then the security level of the company won't be adequate either*. Dina (30), ♀, IT-company.

The informants experienced their information security role as important because: (1) information security is viewed as important due to the company's public reputation; the availability of IT-systems; and the confidentiality of customer data; (2) the user role is an important addition to the technological security systems; (3) some of the users want to comply with requirements of the documented security systems (only mentioned at the bank); and (4) users have access to sensitive information.

Although the informants say they are motivated for information security in the sense that they believe their information security role is important, they state that they do not perform many practical security actions in their daily work nor are they aware of what practical actions they can contribute with. As illustrated in Table 1, the individual user could not point out many practical security actions he/she contributed with in the daily information security efforts. The overview in Table 1 is based on the informants answers to the open question 'What do you contribute with in the company's security work?'. The results in the table might not be the real amount of actions of each individual. A possible source of error can be present as the informants may contribute with more actions than those who came into mind at the moment of the interview. It can be assumed that if a list of security actions had been presented to the informants, more contributions would have been mapped. On the other hand, such an approach might have created biased answers as well. The purpose of asking an open question was to get an impression of the quality of users' information security knowledge on actions. Nevertheless, the sum of mentioned security actions per individual indicates that users' information security behaviour is not good enough compared to the expectations in the studied company's documented requirements of individual behaviour.

At the IT-company many of the informants in particular looked at cautiousness when orally and electronically handling sensitive customer information as their main contribution to information security. Beyond confidential treatment of information only a few contributions related to the use of the information systems (e.g. lock the computer and safe use of e-mail) were mentioned by the informants at the IT-company. In contrast, the informants at the bank identified

Table 1 – An overview of the informants' information security actions

	Informants, Bank									Informants, IT-company								
	€$_A$	€$_B$	€$_C$	€$_D$	€$_E$	€$_F$	€$_G$	€$_H$	€$_J$	@^{A}	@^{B}	@^{C}	@^{D}	@^{E}	@^{F}	@^{G}	@^{H}	@^{I}
Cautious use of e-mail	●			●	●			●							●			
Cautious use of mobile equipment[a]	●	●		●				●										
Reporting and awareness of unexpected situations		●		●		●	●	●	●			●						
Lock computer			●		●		●							●	●	●		
Handling of sensitive information			●			●	●		●	●	●	●	●	●	●	●		
Distinction of private and professional use								●										
Cautious use of internet								●							●			
Password etiquette														●				
Avoid access to someone else's																●		
Total	2	2	2	3	2	2	3	5	2	1	1	2	1	3	4	3	0	0

[a] Not relevant for the IT-company.

information security contributions with human-machine interaction, e.g. safe use of e-mail and locking of the computer.

There are variations in the extent of practical actions. "Frida", the informant at the IT-company that point out most security efforts (indexed @$_F$ in Table 1), explain that it is actually quite effortless and straightforward for users to perform information security actions. She was clearly the most aware user among the informants at the IT-company, as she was well-informed on information security issues and had high practical security skills:

> *It doesn't take much effort from us to do something about information security. It's simple to delete spam mail; to lock the computer when absent from it; and to avoid downloading stuff from the Internet. These are some of the things we can contribute with in our daily work – and they are simple actions.* Frida (36), ♀, IT-company.

Except for "Frida" at the IT-company and two male informants at the bank, who had a high security awareness and technical skills, the other informants could only point out a couple of security actions they performed in their daily work. The users who performed a limited amount of security actions explain this by: (1) poor communication from the information security professionals on how user security behaviour should be; (2) attributing the responsibility of information security as a technological discipline handled by security professionals, thus believing that technological measures take care of the security level; and (3) limited time to handle information security in the daily work. "Halvard", a well informed informant at the bank who had experience as a system engineer, and mentioned several security actions he contributed with, pointed out lack of knowledge as well as a conflict between functionality and security as the main reason for the poor quality of most users' security behaviour:

> *One of the greatest problems of information security is to find the balance between security and functionality. You can have a very strict IT-system that makes you unproductive in the sense that it is not possible to do your actual work tasks. I believe that's why so many have a poor information security behaviour. It is a combination of not knowing and a conflict between security and functionality… A lot of those working in the bank have no background knowledge of IT. They know how the systems they use on a daily basis should be used. Beyond that, they hardly know where the on/off switch of their computer is.* Halvard (29), ♂, bank.

4.3. *A latent conflict of interest between information security and functionality*

Neither at the IT-company nor at the bank was information security experienced as an obstacle for daily work at the current moment. The latter section showed that the interviewed users have a minor information security workload. The view on information security and functionality must thus be assumed to be coloured by this small security effort of users. Additionally, the interviews indicate that an increased workload for the users will ignite a currently latent conflict of interest between information security and functionality.

Although the informants at the two studied companies have a similar understanding of information security and functionality, the reasons for this comprehension differed between the two companies. At the IT-company, information security work was not considered to be an obstacle for daily work at the current moment. The informants at the IT-company believed that information security was an integrated and necessary part of customer services, especially related to oral and electronically handling of sensitive customer data. Several of the informants at the IT-company had previously worked with data quality implying that they were familiar with the consequences of incorrect data. At the bank the pattern for thinking of information security as an integral part of their work was somewhat different. As for the IT-company the bank employees did not see information security as an obstacle for their daily work at the current moment. In contrast to the IT-company, the informants at the bank did not think about information security to any extent in their daily work. Opposite to the IT-company as well was a tendency among the informants at the bank to attribute information security as a technical discipline handled by information security professionals, rather than looking at it as their personal co-responsibility, here exemplified by a citation of a male bank employee.

> *Information security is not my job. I have to concentrate on my own working tasks, and trust that the security system is in place. Information security is not something I should think about… How much should a user actually think about information security? It is not possible to be too cautious – it must be possible for us to carry out our work smoothly* Bjørn (43), ♂, bank.

The different views on information security as an integral part of other work tasks among the informants at the bank and the IT-company is explained by three patterns. First, the informants at the IT-company mainly associated information security with orally and electronically handling of sensitive customer data. The main task of the operators at the service centre is dealing with costumer information. Hence it is natural for the informants to recognize handling of sensitive information as an important information security contribution based on respect and loyalty to their costumers. In that sense the expressed security actions at the IT-company are integrated in other daily activates, while the actions at the bank are specifically related to information security. Second, the informants at the bank distributed the responsibility for information security to professionals to a higher degree than the informants at the IT-company. As a consequence, they overlooked their personal role. This difference of disclaiming responsibility is explained by the view of information security professionals. At the bank, the information security professionals were regarded as more visible and proximate than at the IT-company. Third, higher demand for efficiency of performance at the bank than at the IT-company can explain the difference in thinking about information security. According to the informants, there was simply no time available for the bank employees to think about information security:

> *We are measured by sale. Our salary depends on it, bonuses and stuff like that. Information security is definitively a second or third*

> *priority. If we have to use half an hour extra on information security per day – that simply doesn't function!* Halvard (29), ♂, bank.

There was one contrast to the overall pattern of information security not being an obstacle in the daily work both in the bank and in the IT-company: password overload. Some of the informants needed up to seven different passwords with various linguistic requirements and changing routines to carry out their work. As a result, the informants could tell of several post-it notes with passwords hidden in their drawers, as well as where colleagues had hidden their passwords.

> *There are too many passwords. It had been better to have only one password and changed it often. I must use post-it notes, it would have been impossible to function without them… I feel comfortable with the post-it notes. They're hidden in my drawer. It's not ok in a security perspective as functionality wins over information security. It's much more critical to me if I can't work for some hours than to ensure information security. The bank has constructed the problem itself by having several systems and passwords. It is a fake security*. Dag (61), ♂, bank.

In the latter section, it is argued that the current individual information security workload has a potential to rise. If users have to perform more information security actions, the users believe that difficulties regarding usability and efficiency will be experienced. This is exemplified by "Bjørn", "Halvard" and "Dag's" citations above, which all indicate that an increase in the current information security workload will create problems regarding work functionality and efficiency. The perceived password overload and the accompanying solutions of post-it notes show that the problem already exists. An increased workload will interfere with the informants' explanations for their current view on security and functionality: the users at the IT-company must perform other security actions than orally handling sensitive information; the users must be more personal responsible for the security work; and the high demand for work efficiency will collide with security tasks. Consequently, it is likely that increased security workload will make the users feel that information security on the one hand and functionality and efficiency on the other hand will be on collision course.

This tendency to prioritise functionality ahead of security is even an explanation of the shortage of information security actions among the informants described in the latter section. When it comes down to business: functionality, usability and efficiency are prioritized ahead of information security. Based on this argument it can be claimed that at the current time the informants feel comfortable with their information security workload due to satisfactory functionality.

4.4. *Users' evaluation of administrative information security measures*

In this section the informants' experiences of different administrative information security measures directed at individuals are presented. First, experiences of written rules and guidelines for individual behaviour are presented. Second, views on the effects of awareness campaigns are presented. Finally, the interviewed users' view of user participation as an effective strategy for changing awareness and behaviour is presented and argued for.

4.4.1. *Documented rules and guidelines*

Both the bank and the IT-company had detailed descriptions of expected individual information security behaviour available at their intranets. The security work at the bank is to a large extent centred on a security handbook. This document was revised half a year before the interviews were conducted. This revised documentation was not, similar to the old version, systematically communicated to the users. There had nonetheless been some sporadic meetings that presented some of the requirements in the documentation to some of the employees. At the IT-company everyone had signed information security rules when appointed to the job. The IT-company's security management even declared an expectation that all users should follow these rules and accompanying guidelines.

Nevertheless, most of the informants at the bank and all the informants at the IT-company were not familiar with the content of their companies' documented system for expected behaviour. "Erik" illustrates this pattern neatly by his reflecting on his own and his colleagues' relationship to the written rules and instructions:

> *Of course, there are rules and guidelines for information security behaviour. Nevertheless, I haven't heard about them or seen them. I believe they're available at the bank's intranet. I don't believe that everyone has read them… Our working day is too busy. There's a lot of information on all kinds of things all the time, but there is simply not time to read everything. There are instructions for everything in the bank, even on how to order a ball pen. To put it this way: I don't think everyone has read all these instructions… I believe my behaviour is approximately the same as the documented expected behaviour, although I don't know what is written. My behaviour is based on the experience I've acquired during my years here*. Erik (43), ♂, bank.

Although "Erik" have not heard about or seen the information security documentation, he thinks his behaviour is roughly the same as the documented behaviour. Several of the other informants shared this belief. Having this view on themselves, users tend to be unmotivated for studying the information security documentation: why study described expectations of behaviour if you think you already act in compliance with these documents? Another counter-incentive for studying the documents is found by the users' indications that it is sufficient to know that there are certain rules existing for how to behave, but it is not possible to comply with all the demands:

> *One should know that there are rules on how to behave. I believe the documentation is huge – it is not possible to read it all or to act in compliance with all the demands*. Bjørn (43), ♂, bank.

"Halvard" an ex-system engineer, who know the fundamental content of the rules and guidelines, state that lack of knowledge is another explanation for the poor relationship between users and the documented system:

> *IT-rules – they're boring. I don't know them word-for-word, but I know the essence. I don't believe my colleagues know the essence, they don't possess the necessary knowledge to understand it.* Halvard (29), ♂, bank.

To sum up, the pattern of not being familiar with requirements in the documented systems is explained by: (1) lack of time to read them; (2) lack of communication on where the documentation is available; (3) lack of incentives for studying the documentation; and (4) lack of knowledge for understanding the instructions.

As seen by the citation of ''Halvard'' above, he is a bit familiar with the content of the documented security system. Some of the bank employees knew parts of the documented system. This knowledge was mainly created by participation in group-based information meetings. Furthermore, these informants at the bank claimed that the banking business was dominated by a rule-based mindset. As a result it was natural for bank employees to act in accordance with the rules.

Although there was lack of knowledge on the contents of documented system among the informants, a lot of the informants at both companies believed they behaved in accordance with the rules and guidelines. These informants felt their behaviour was in compliance with the documented system due to the belief that the rules and guidelines are common sense and that the demands are similar to individual and group-based norms that were developed over time. This is illustrated by a quotation of a female at the IT-company:

> *I feel I know the rules and guidelines, but not the documentation. I think I know what I have to comply with. You know how you should behave when you've been here for a while.* Dina (30), ♀, IT-company.

4.4.2. *Awareness campaigns*

The recent years, the IT-company had arranged several general awareness campaigns, i.e. expert-based one-way communication directed towards many receivers. For example a campaign consisting of posters containing information security tips and a campaign where a coupon containing some security rules could be traded for a gift. The last campaign was arranged about half a year prior to the study. This campaign consisted of a box of chocolate containing a pamphlet regarding cautious use of e-mail that was delivered to all employees.

Only one of the nine informants at the IT-company believed that these awareness campaigns had any effect on their security behaviour. ''Frida'', the most security aware informant at the IT-company, is the only one who had a positive view on the campaigns. She perceived the campaigns as important reminders that are comprehensible and not too time-consuming. ''Frida'' was also the only informant to remember the last campaign with a box of chocolate without being asked directly about that particular campaign.

When the informants were asked directly if they remembered the last campaign, others than ''Frida'' remembered the campaign as well. Nevertheless, none of these remembered the message of the attached pamphlet:

> *I don't think any of my colleagues remember what information they got together with the chocolate box… I believe most of them ate the chocolate, and left the pamphlet in the box.* Camilla (30), ♀, IT-company.

The interviews showed that general awareness and attitude campaigns had not an effect on the information security behaviour of the users. The informants explained the poor effect of the campaigns by: (1) limited time to comprehend the message; (2) a belief that the gifts and the wrapping becomes more important than the message; (3) a tendency that the message is read, but quickly forgotten; and (4) a belief that the content of the message is nothing new related to what one already know.

4.4.3. *Involvement of users in the information security work*

Several of the informants at both companies pointed out that involving users is a much more effective approach for improvement of information security knowledge and awareness than awareness campaigns and written rules. Most of the interviewed users exemplified this approach by a request for user participation in small-sized information meetings, although most of them never had attended such meeting. This is argued for below by the citations of ''Camilla'' and ''Bente'' at the IT-company:

> *The campaigns are just a stunt. After the campaign, you never hear anything. I don't think any campaign has had an effect my security behaviour. The message of the campaign is quickly forgotten. Other tools than chocolate and pamphlets should be used. I think a course describing how one should behave should be arranged. I think it's easier to become aware if one meets information security professionals face to face.* Camilla (30), ♀, IT-company.

> *The security management department should give us some information about information security and themselves… Involving us is the best way to communicate. They have to make themselves visible to us. Then we will become more interested in information security as well… It is much better with information meetings than documents and mails.* Bente (53), ♀, IT-company.

At the bank, some of the informants had participated in such meetings. These informants emphasized the utility of reflecting on their personal situation:

> *After and during the meetings I reflect on my own situation: how do I use the IT-systems? Do I need to change my behaviour?… If you don't get updates on such information, then you will work happily in the same manner all the time. The last information meeting I participated in, gave me several aha-experiences* Bjørn (43), ♂, bank.

The interviewed users explain the belief in participatory meetings as the most effective tool for influencing user behaviour and awareness by three motives: (1) user participation in form of problem solving and the possibility to ask questions; (2) the possibility of users to reflect on their own situation: is there anything I could do different to improve information security and why should I act differently in a world of conflicting demands?; (3) meeting security professionals face-to-face, thus making information security management more visible.

5. Discussion

In Section 4, three main patterns of results are mapped: users do not perform many information security actions; users prioritise other work tasks in front of information security; and users experience current tools for influencing individuals as ineffective for that purpose. The interviews indicate that a main problem regarding users' role in the information security work is their lack of motivation and knowledge regarding information security and related work. This poor quality of users' motivation for and knowledge of information security might be explained by characteristics of individuals. On the other hand, following Douglas and Wildavsky's (1982) argument that risk is a collective construction, the indifferent attitude of the interviewed users can be explained by group-based values. Several of the interviewed users claim that information security very seldom is a topic for formal or informal discussions in their department. If perception of risk is a matter of social organisation, then management of risk is an organisational challenge (Douglas and Wildavsky, 1982). Accordingly, this section discusses the main patterns of results from the interviews mainly in an organisational perspective, it is, however, impossible to neglect the individual and technological factors. The section ends by presenting arguments for alternative approaches to information security management of users.

5.1. *Role and responsibility: gap between talk and action*

The results of the study showed that the interviewed users neither perform many specific information security actions nor are they aware of what security activities they can perform. Nevertheless, they state to be motivated for individual information security work. Most of the possible individual actions are simple and not time consuming, e.g. locking the computer when absent from it; password etiquette; safe and secure use of e-mail; cautious use of Internet; and avoidance of software for file sharing. As a result of the informants' gap between information security talk and action a question arises: *why do not the users put in much effort to make information security actions when they say they are motivated for individual information security work?*

The gap between information security talk and action among the informants can be explained by a combination of (1) users not being as motivated as they declare; (2) lack of knowledge on how to perform well due to poor information security management; and (3) a conflict of interest between functionality and information security that creates a hypocritical view on individual information security work.

First, one could question whether the users are as motivated for individual security work as they declare. The informants may have been biased by the theme of the interview, consequently stating that information security is important to themselves and the company. It might have been embarrassing to admit that they do not perceive information security as important to them and the company, since the interviews were directed at information security. As a result, the actual theory-in-use (Argyris and Schön, 1996) may not have been revealed during the interview. Individual risk perception may also explain the lack of motivation, as users do not see why information security is important. Slovic (2000) describes some factors that determine individual risk perception. Among these, risk characteristics such as not observable; unknown to those exposed; new risk; and uncontrollable for those exposed, provide explanations for the interviewed users' perceived indifference to information security.

Second, an explanation of the gap of talk and action is poor risk communication from the information security management. Information on information security issues has been ineffective as users are not well informed on what security actions they should make. Hence, the users can be as motivated as they declare, but they simply do not know what contributions they actually can make. Risk communication in the two companies has been an expert-based and one-to-many approach. In subsequent parts of this paper arguments for improved risk communication with users by a user involving approach is presented based on, e.g. Slovic (2000) and Shrader-Frechette (1991). An example of poor communication is that although there is information available for the users at the intranet, the users do not actively seek knowledge of information security behaviour there. Proper communication might have simplified user access to this documentation. On the other hand, as discussed later, planned behaviour and actual behaviour might differ nonetheless. This finding nevertheless indicates that communication and training on individual information security work have not been good enough. At the same time is this result an indication that the users are not as motivated as they declare, as they do not actively seek information that they request.

Third, the possible conflict of interest between functionality and work efficiency on the one side and information security on the other side may explain the gap between talk and action. In a work day full of different stakeholders and interests, there is no time to make many information security actions according to the informants. Hypocrisy is a way of handling several conflicting interests simultaneously (Brunsson, 2002). The informants state that increased information security workload will affect other working tasks in a negative way. Consequently, the users are happy with their current low security workload, but hypocritically state that they are motivated for contributing in the information security work in order to satisfy the security requirements of the companies. The conflict of information security and functionality is further discussed in the next section.

5.2. *The conflict of individual interest between information security and functionality*

Requirements of efficiency, usability and functionally is likely to make the quality of individual information security efforts poor (Besnard and Arief, 2004). At the current moment, the informants experience the information security workload as acceptable. At the same time they express that an increased security workload might create difficulties for the work functionality and efficiency. As shown previously, the current information security workload has a potential to increase, it is thus interesting to look into *why this possible conflict is generated*. This problem is discussed in light of Rasmussen's (1997) argument that one should not only pay attention to the human failures and violations, but on the mechanisms that generate behaviour in the actual, dynamic work context. Pressures toward efficiency and toward least effort are mechanisms that influence security related behaviour in a negative way, see Fig. 1. Additionally, there is a counter gradient from information security management that should influence user behaviour in a positive way.

One of the informants expressed that 'it is not possible to become too cautious as it will make us unable to do our regular work'. Both at the IT-company and the bank, the informants expressed that there was no time to perform many information security specific actions, not least in the bank where the employees' salaries are partly based on sale. This lack of time is mainly a result of efficiency demands, i.e. other tasks than information security must be dealt with in a busy day full of demands for effective customer service. Additionally, there are demands regarding usability, functionality and comfort resulting in a gradient toward least effort. Often these demands will result in a conflict with information security requirements (Besnard and Arief, 2004). For example, most of the informants had written their passwords down on post-it notes. In order to be capable of doing their actual work, several of the informants felt it was impossible to avoid writing down their passwords. These post-it notes are a nice example of functionality demands that conquer information security requirements.

In goal conflicts between acceptable risk and functionality at the sharp end, individuals tend to put emphasis on efficient and least-effort work instead of loss prevention (Rosness, 2001). In a work day full of different interests and demands, decision makers are likely to choose a satisficing strategy (March and Simon, 1958), i.e. they seek action that is good enough rather than choose the best alternative of action. This was the case for the interviewed users as well. In the set of demands for information security, functionality, usability and efficiency, the users tend to prioritise the latter three ahead of information security, particularly if the information security workload becomes unacceptable. Nevertheless, they perceive information security as important for the company, and hypocritically declare that their information security work is important in order to satisfy the information security requirements of the company. This bounded rationality of users is in conflict with Jaeger et al.'s (2001) characteristics of the rational actor paradigm of main stream risk management.

The conflict of individual interest between information security and functionality is created by a combination of interwoven motives: prioritisation of work tasks; individual motivation for information security and the quality of information security management strategies. Some information security measures are simple and not time-consuming, e.g. cautious use of the Internet. In contradiction, the interviewed users argue that there is no time to perform these actions. At the same time they indicate that the human desire for least effort as an equally important reason for not performing security actions. Based on the simple nature of many information security efforts, the motivation and knowledge of the users can be questioned: do they know how and why they should perform information security actions. These paradoxes lead to a question regarding the quality of the information security management regarding users. As a result of efficiency and least effort demands, the information security performance of the interviewed users is pushed toward a situation of unacceptable risk, Fig. 1. According to Rasmussen (1997) information security management should serve as a counterbalance to the negative influences of risky behaviour. The counter gradient of management of users seems to be somewhat week in the studied cases, as the informants are not sufficiently informed or trained in information security behaviour. The result is poor individual information security performance in the sense of lack of knowledge and motivation and an insufficient amount of individual information security actions. The quality of and possible implications for management of users is further discussed in the next section.

5.3. *Quality of and implications for information security management of users*

The studied companies had utilized technological inscriptions and documented rules as their main tools for influencing user behaviour. Additionally, the IT-company had used awareness campaigns. As revealed in the sections above, the quality of the methods used to influence information security attitudes and behaviour among users seem to be somewhat ineffective. This section discusses *why the quality has been poor and whether there are reliable arguments for alternative approaches to information security management in the interview users' view of information security*.

The interviews showed that the described expected behaviour in documented rules and guidelines have limited effect on users' information security behaviour due to the users' lack of knowledge about the documents and information security as well as their lack of motivation for viewing the documentation. An explanation for this pattern is found in research that has shown that it is not evident that everyone will act according to the management's objectives and structures (e.g. Brunsson, 2002; Lysgaard, 1961). Brunsson (2002) argues that in a busy working day of conflicting demands, organisational ideas and individual actions become loosely coupled or de-coupled. As previously described, this was the case among the studied users since the interviewed users prioritise other work tasks in front of organisational expectations of information security behaviour. Lysgaard (1961) describes how lay people and management have different mindsets. According to the interviewed users, this seems to be the case for this study as well. The informants experienced information security managers as invisible. Additionally, the current management approaches regarding users was experienced as expert-based, top-down approaches with no or moderate involvement of users. Braverman (1974) has explained such patterns by arguing that separated planning and work can lead to unmotivated and uncommitted operators, hence resulting in lack of emphasis for obedience to the documented requirements for behaviour. The informants of the study ask for other tools to influence their information security behaviour than documented rules and guidelines. This demand is given support by social science research material that questions the power of documented rule-based systems' ability to influence individual behaviour.

Mass-media based awareness campaigns have, according to the interviewed users, no significant long-term effects on users' behaviour and awareness. The informants state that such campaigns do not create individual and collective reflections on the subjects of the campaigns. This view is explained by impersonal one-way communicated messages and that the wrapping becomes more important than the content. This argument is given support within the field safety psychology. Aarø and Rise (1996) argue that pure information seldom has any effect on individual behaviour as behaviour is created by more factors than knowledge and attitudes. A literature review by Lund and Aarø (2004) show that information measures alone such as leaflets, booklets, films, postern or direct mail do not prove any effect on behaviour or reduced risk potential.

A challenge in the attempt to influence user's security behaviour is to cope with the possible conflict between functionality and information security. In order to deal with this problem, Rasmussen (1997) has argued for making the boundary for unacceptable risk visible for users. Are users familiar with their individual accepted level of risk level? Do users know the consequences of information security breaches? Consequently, one should influence users' perception of acceptable level of risk and what the consequences of information security breaches are. According to the theory of risk homeostasis (Wilde, 1982; Stanton and Glendon, 1996), perceived level of accepted risk contribute to an explanation of individual behaviour as well. The theory says that individual behaviour is explained by the individuals' comparison of perceived risk and individual risk acceptance criterion. Individuals adjust their behaviour in order to balance perceived risk and acceptable risk, which in turn is dependent on the individual's experienced costs and benefits of alternative actions. Acceptable risk is not only determined by perceived costs and benefits, but also by characteristics of risk such as voluntariness; ability to control the risk; familiarity; knowledge; whether it affects the individual; and immediacy (Fischoff et al., 2000a,b). Due to the interviewed users' lack of knowledge and motivation of information security, in addition to their experienced latent conflict of functionality and information security, the interviewed users consider the costs of cautious behaviour to be higher than the perceived benefits of cautious behaviour. Benefits on other areas such as usability, efficiency and functionality are achieved by a risky behaviour. In sum, risky behaviour has more benefits than cautious behaviour, which according to the risk homeostasis theory explains the poor information security behaviour of users.

The father of the risk homeostasis theory, Wilde (1982) has argued that the only factor that determines the individual long-term level of risk is their individual risk acceptance criteria. Wilde (1982) describes four ways of lowering the individual target level of risk: decrease the expected benefit of risky behaviour; decrease the expected cost of cautious behaviour; increase the expected benefit of cautious behaviour; and increase the expected cost of risky behaviour. Accepted level of risk is also dependent on other factors than benefits and costs (Fischoff et al., 2000b). Improving individuals' knowledge, familiarity and control of risk should influence users' perception of risk, which in turn can affect individual behaviour.

Informing users on the possible wide-range consequences of risky behaviour should influence the expected benefits of behaviour in a positive way for the security level as well as reducing the benefits from risky behaviour. Additionally, information of and training on personal information security actions, emphasising that most actions are simple and not time-consuming, should influence the expected costs of cautious behaviour. This calls for new approaches to management of the user role of information security, as the current used approaches seem to have had no considerate effect on the users' perceptions of benefits and expected costs of risky or cautious behaviour.

The individual's and the security management's perception of risk can differ (Slovic, 2000; Shrader-Frechette, 1991). Individuals might, e.g. not see the range of consequences in the same manner as the security management in an organisation does. An example of these different views is provided by Kuttschreuter and Gutteling (2004), who show that lay people assessed the risk related to Y2K as lower than experts. The information security management's perception of risk has not been studied in the current paper. However, the exciting structures of managing the human element of information security seem to have a different view on risk and risk mitigation than users have. Current risk management overemphasizes a rational actor paradigm (Jaeger et al., 2001), while the interviewed users, as indicated in sections above, have a bounded rationality regarding information security. In situations of dissimilar understandings of risk and risk mitigation between experts and public, Slovic (2000, p. 191) argues for a two-way interaction of information exchange, discussion and deepening of perspectives: ''...there is wisdom as well as error in public attitudes and perceptions. Laypeople sometimes lack certain information about hazards. However, their basic conceptualization if risk is much richer than that of the experts and reflects legitimate concerns that are typically omitted from expert risk assessments. As a result, risk communication efforts are destined to fail unless they are structured as a two-way process (Renn, 1991). Each side, expert and public, has something to contribute. Each side must respect the insights and intelligence of each other''. The interviewed users call for this approach themselves, an approach that seems somewhat neglected by the management at the studied companies.

5.3.1. *Arguments for a user-involving approach to information security management approaches*

This section has provided empirical and theoretical arguments for other approaches for managing the human element of information security than documentation and mass media-based awareness campaigns. First, the interviews indicate that a main problem regarding users' role in the information security work is their lack of motivation and knowledge regarding information security and related work. This signals the need to increase the quality of the users' role and responsibility. Second, the currently used approaches at the studied companies, documentations and mass media-based awareness campaigns, have no considerable effect on users' behaviour and awareness. Third, in order to cope with conflicting issues of security and other work tasks, it is argued for approaches that influence users' risk perception and perceptions of benefits and expected costs of risky or safe behaviour.

Another important argument for alternative management approaches is found in the informants' call for more user-involving approaches in the information security work. The informants' argument includes specific suggestions for this approach as well. They indicated that active participation in information security workshops was the key to successful influence of users' awareness and behaviour. Discussions, problem solving and scenario thinking should set up users to reflect on their personal information security situation. This approach calls for a discourse based risk management strategy (Klinke and Renn, 2002), i.e. building awareness and confidence, improving knowledge and utilize balanced risk communication in direct contact with the employees. Consequently, communication should lay emphasis on convincing rather than top-down persuasion, hence being based on a discursive ethical perspective rather than duty ethics (Hovden, 1998). This form of communication will aim at creating an understanding among users on why it is important for each user to pay attention to information security, which should make acceptance of technological, individual and administrative security measures smoother.

The study gives empirical support for a management strategy that involves the users to a wider extent than at the current moment of time. The issue of involvement of employees is not new. Research in several other fields of research indicates that a user involving approach is effective for change and development. In the field of system design it has been argued that dialogues between designers and users are beneficial for implementation and use of systems (Adler and Winograd, 1992; Ehn, 1992). In organisational development and change, involvement has been used for decades as one of the most important tools for change (Levin and Klev, 2002). In the field of safety psychology, involvement of employees in cross disciplinary group-based approaches utilizing local recourses has proved to be effective for influencing employees attitudes and behaviour (Lund and Aarø, 2004; Iversen et al., 2005). Numerous literature within the risk research area call for interactions between experts and lay people in order to create improved understanding and consensus on risk and risk mitigation (e.g. Douglas and Wildavsky, 1982; Shrader-Frechette, 1991; Beck, 1992; Klinke and Renn, 2002; Slovic, 2000). On the other hand, Adams and Sasse (1999, p. 45) have criticized the field of information security for not involving users in the endeavour for information security: ‘‘users have to be treated as partners in the endeavour to secure an organisation's systems, not as the enemy within’’. User involvement could, as indicated by the informants, be created by workshops with active involvement of users. In addition involvement can happen by active participation in risk assessments; user panels; and easily accessible lines for reporting and question making. According to Levin and Klev (2002) participation gives users as a group a direct and definite possibility to shape their own working conditions. At the same time it creates motivation and increased knowledge about work processes. Involvement of users will create positive effects for security management as well: utilization of users' hands-on knowledge; motivation and ownership for the security work among all organisational members. An important step in direction of increased involvement is a common platform of language and tools for users and professionals (Ehn, 1992). User involvement, e.g. in workshops, is a great possibility to create a common platform for users and information security professionals.

The study gives empirical support to the call (Dhillon and Backhouse, 2000, 2001) for new approaches to information security management in today's organisations. It is important to stress that the current information security tools and methods should not be thrown away. Information security is, and still will be, to a large extent a technological discipline. Hence, technological measures should be the foundation of the information security work. Additionally, a structural, administrative information security system is needed for control of the complexity of organisations. When these measures are in place, one can start talking about influencing individual and organisational behaviour and awareness, without losing sight to the other measures. On the other hand, the results in this study give empirical support for utilizing alternative measures for influencing users. Lund and Aarø (2004) argue for a combined approach of several different measures as the most effective loss prevention strategy. It is likely that a combined approach will increase the power of documentation and mass-media based awareness campaigns as well, as knowledge and motivation will increase by the influence of other more user-involving approaches.

6. Conclusion

The results of this qualitative study of users and information security should not be seen as generalized facts. Rather, the results are interpretations of some users' experiences of information security in their daily work. It should thus be considered whether the findings are transferable to certain organisations by comparing them to the context of this study. The results of this study are created by qualitative interviews of users in a service centre at an IT-company and in a consultancy department at a bank. The informants did not have much information security awareness; perform moderate amount of information security actions; did not have any management responsibility; and were working with different kinds of customer service where IT-systems were the most important working tool.

Independent of transferability, the empirical findings of the study open for interesting discussions on information security management. Some reflections on information security management of users are triggered. Should the users be treated as pieces in a game or should they be involved? Should users be generalized into a large population or should one treat them as individuals and groups?

The main patterns of results in the study are:

- Users are aware that their role in the total information security work is important. On the other hand, there is a gap between this intention and the actual behaviour of users as they do not perform many information security actions, nor are they familiar with what practical actions they could make.

- If the users have to increase their current low information security workload, a conflict of priority between usability, efficiency and functionality on the one side and information security on the other side will be created.
- Users perceived a user-involving approach as the most effective tool for influencing individual security awareness and behaviour, e.g. by information security workshops. Mass-media based awareness campaigns had low degree of influence on users, while documented rules and guidelines for expected behaviour were experienced as valueless by the users.

These patterns of results can be explained by some interwoven main causes. The interviewed users lack motivation for information security work and knowledge on information security risks and how they can handle these risks, which is partly explained by the informants' low perceived acceptable level of risk regarding their own role. In a busy working day of many demands, information security is given a lower prioritisation than other work tasks. This rationality of users is contradictory to the rationalistic approach of information security management at the studied companies, consequently currently used information security management approaches at the studied companies are not well suited the characteristics of users, social norms and the work context. Instead it is argued by the informants for a user-involving approach for utilizing human resources of users in the information security work.

A user-involving approach is given support by arguments from the interviewed users as well as from other fields of research such as organisational development, risks research and safety management. Paradoxical, users support a time-consuming participating approach to information security, while at the same time stating that they have no time to spend for information security. More research is thus needed to evaluate the cost-effectiveness of user participation in information security.

Acknowledgements

The author thanks Prof. Jan Hovden at the Norwegian University of Science and Technology for valuable input and discussions. The author also thanks the interviewed users and the security officers at the studied companies for sharing their experiences on information security. Eirik Albrechtsen's PhD project is financed by Vesta insurance company.

REFERENCES

Aarø LA, Rise J. Den menneskelige faktor, Norwegian [The human factor]. Bergen, Norway: Skadeforebyggende forum; 1996.

Adams A, Sasse MA. Users are not the enemy. Communications of the ACM 1999;42(12):41–6.

Adler PS, Winograd T. The usability challenge. In: Adler PS, Winograd TA, editors. Usability – turning technologies into tools. New York: Oxford University Press; 1992.

Albrechtsen E, Grøtan TO. Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner. Norwegian [old-fashioned thinking in modern organisations? On ICT-security in knowledge organisations]. In: Lydersen S, editor. Fra flis i fingeren til ragnarokk. Trondheim, Norway: Tapir Akademisk Forlag; 2004. p. 319–35.

Argyris C, Schön D. Organizational learning II. New York: Addison Wesley; 1996.

Beck U. Risk society: towards a new modernity. London: SAGE; 1992.

Besnard D, Arief B. Computer security impaired by legitimate users. Computers and Security 2004;23(3):253–64.

Braverman H. Labor and Monopoly Capital. New York: Monthly Review Press; 1974.

Brunsson N. The organization of hypocrisy, Talk, decisions and actions in organizations. 2nd ed. Oslo, Norway: Abstrakt forlag; 2002.

Dhillon G, Backhouse J. Information system security management in the new millennium. Communications of the ACM 2000;43(7):125–8.

Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 2001;11(2):127–53.

Douglas M, Wildavsky A. Risk and culture, An essay on the selection of technological and environmental dangers. Berkeley: University of California Press; 1982.

Ehn P. Scandinavian design: on participation and skill. In: Adler PS, Winograd TA, editors. Usability – turning technologies into tools. New York: Oxford University Press; 1992.

Fischoff B, Slovic P, Lichtenstein S, Read S, Combs B. How safe is safe enough? In: Slovic P, editor. A psychometric study of attitudes toward technological risk and benefits. The perception of risk. London: Earthscan Publications Ltd;2000a.

Fischoff B, Slovic P, Lichtenstein S. Weighing the risks: which risks are acceptable? In: Slovic P, editor. The perception of risk. London: Earthscan Publications Ltd; 2000b.

Hovden J. Ethics and safety: "mortal" questions for safety management. Paper at the conference Safety in Action. Melbourne; 1998.

ISF. The standard of good practise for information security. Version 4.1. Information security forum; 2005.

Iversen H, Rundmo T, Klempe H. Risk attitudes and behaviour among Norwegian adolescents. European Psychologist 2005; 10(1):25–38.

Jaeger CC, Renn O, Rosa EA, Webler T. Risk, uncertainty and rational action. London: Earthscan Publications Ltd; 2001.

Klinke A, Renn O. A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. Risk Analysis 2002;22(6):1071–94.

Kuttschreuter M, Gutteling JM. Experience-based processing of risk information: the case of the millennium bug. Journal of Risk Research 2004;7(1):3–16.

Kvale S. Interviews, An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage; 1996.

Leiulfsrud H, Hvinden B. Analyse av kvalitative data: Fikserbilde eller puslespill? Norwegian [Qualitative data analysis: puzzle picture or jigsaw puzzle?]. In: Holter H, Kalleberg R, editors. Kvalitative metoder i samfunnsvitenskapene. Oslo, Norway: Universitetsforlaget; 1996.

Levin M, Klev R. Forandring som praksis. Læring og utvikling i organisasjoner, Norwegian [Change as practise. Learning and development in organisations]. Bergen, Norway: Fagbokforlaget; 2002.

Lund J, Aarø LA. Accident prevention. Presentation of a model placing emphasis on human, structural and cultural factors. Safety Science 2004;42(4):271–324.

Lysgaard S. Arbeiderkollektivet, Norwegian [The workers' collective]. Oslo, Norway: Universitetsforlaget; 1961.

March J, Simon HA. Organizations. New York: John Wiley; 1958.

Miles MB, Huberman AM. Qualitative data analysis. Thousand Oaks, CA: Sage Publications; 1994.

OECD. OECD guidelines for the security of information systems and networks: towards a culture of security; 2002.

Rasmussen J. Human errors. A taxonomy for describing human malfunction in industrial installations. Journal of Occupational Accidents 1982;4:311–33.

Rasmussen J. Risk management in a dynamic society: a modeling problem. Safety Science 1997;27(2/3):183–213.

Renn O. Premises of risk communication: Results of two participatory experiments. In: Kasperson RE, Stallen PJ, editors. Communicating risk to the public: International perspectives. Amsterdam: Kluwer Academic; 1991. p. 457–81.

Rosness R., Om jeg hamrer eller hamres, like fullt så skal der jamres. Målkonflikter og sikkerhet. In: Norwegian [Goal conflicts and safety]; 2001 [SINTEF report no. STF38 A01408M].

Schneier B. Secrets & lies, Digital security in a networked world. New York: John Wiley; 2000.

Schultz E. Security training and awareness – fitting a square peg in a round hole. Computers and Security 2004;23(1):1–2.

Schultz E. The human factor in security. Computers and security 2005;24(6):425–6.

Shrader-Frechette KS. Risk and rationality. Oxford: University of California Press; 1991.

Slovic P. The perception of risk. London: Earthscan Publications Ltd; 2000.

Stanton N, Glendon I. Risk homeostasis and risk assessment. Safety Science 1996;22(1–3):1–13.

Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. Computers and Security 2005;24(2): 124–33.

Strauss A, Corbin J. Basics of qualitative research. Thousand Oaks, CA: SAGE Publications; 1998.

Thagaard T. Systematikk og innlevelse. En innføring i kvalitativ metode, Norwegian [Introduction to qualitative methods]. Bergen, Norway: Fagbokforlaget; 2002.

Wilde GJS. The theory of risk homeostasis: implications for safety and health. Risk Analysis 1982;2(4):209–25.

Eirik Albrechtsen is a PhD student at the Department of Industrial Economics and Technology Management at the Norwegian University of Science and Technology. He obtained his Master of Science degree at the same Department in 2002. His current research interests include human and organisational aspects of information security and information security management strategies.

PAPER II:

Albrechtsen, E. and Hovden, J.

“Information security digital divide in organisations: information security managers versus users”.

Accepted with revision march 2008
Computers & Security.

Unrevised document.

Information security digital divide in organisations: information security managers versus users

Eirik Albrechtsen*; Jan Hovden
Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology , N-7491 Trondheim, Norway

* E-mail address: eirik.albrechtsen@iot.ntnu.no

Key words: information security, digital divide, information security managers, users, qualitative research, risk perception

Abstract

Empirical findings from surveys and in-depth interviews with information security managers and users show a digital divide between information security managers and users regarding risk judgement and views and experience of information security practises. Information security professionals mainly view users as an information security threat, while users believe that they are an untapped resource for security work. The small number of interactions between users and information security managers results in lack of understanding for each other's point of view. Both users and managers experience the most commonly used information security measures directed at users as only moderately effective. These divergent views and interpretations of roles result in management approaches that are not in line with the dynamics of the users' working day. Greater awareness of the gap and greater understanding of each other's situation would improve information security performance.

1. Introduction

Traditionally, digital divide has been understood as a socio-economic perspective, regarding the access to information communication technology, in particular the Internet, and the ability to use this technology for fully participating in business, political and social life (Partridge, 2005). However, several authors argue that the digital divide should also be understood in psychological, cultural and sociological terms. For example, Warschauer (2002) has stated that the digital divide is not only about physical access to computers and connectivity, but also about people's ability to make full use of the systems. Jung et al (2001), Harittai (2002) and DiMaggio et al. (2004) argue that the question of unequal access must be expanded to address people's skills, scope of use, autonomy and ability to maximise the utility of the technology to achieve their goals. Based on these interpretations, a social digital divide (Partridge, 2005) can be understood as a product of differences in self-efficacy, individual skills and perceptions, cultural aspects and interpersonal relationships that all contribute to a gap in the use of information systems.

From a socio-technical perspective, an information security digital divide can be viewed as the differences in skills and knowledge of safe and secure behaviour; in perceptions of information security; in social norms; and in interpersonal relationships, any or all of which can result in differences in information security performance between individuals. An information security digital divide in organisations is thus not only a question of access to information systems that have implemented sufficient information security technology. It is a question of the considerable differences in skills, knowledge, responsibility, perception and interpersonal relationships between the various organisational members. From this perspective there may be several information security digital divides, related for example to age, gender, IT experience, education and occupation. In the present paper we will discuss the information security digital divide in terms of differences in views and expectations of information security between information security professionals and users.

An organisation consists of its members and their interactions. Each member has his own role and sphere of responsibility, which combine to realise the organisation's goals. Preserving information security is one of the many goals of an organisation; hence every member has a responsibility for ensuring such security. Information security managers have a particular responsibility because of their expert knowledge; but for users at all levels of the organisation, the responsibility for acting in a manner that is safe and secure for the organisation comes in addition to the other demands on their working day. It is therefore expected that an information security digital divide with regard to skills, knowledge and responsibilities should exist between users and information security managers.

This paper aims at discussing an information security digital divide between information security managers and users by considering *similarities and differences in information security managers' and users' views and experiences of information security practices in several organisations.* A two-fold approach is adopted. First, quantitative data from two different surveys of users' and information security managers' evaluation of IT-related risks are compared. Second, empirical findings from an interview study of information security managers are compared with the results of a similar interview study concerning users' views on information security (Albrechtsen, in press) and other relevant research results on the human aspects of information security.

The paper seeks to answer the following questions:

- How do users and information security managers evaluate risk?
- How do managers experience management of the human part of information security compared with users' opinions on administrative information security measures?
- How do managers experience the role of users compared with the users' view on their own role?
- How do managers consider their own role compared to with how users experience the manager's role?

The study is mainly based on a comparison between managers' views and experience of the administrative information security system and the role of users on the one hand and findings from other studies of users on the other. Focusing on non-technological issues of information security makes comparisons easier as well as richer, as many users probably do not have specific insight into the technological aspects of information security.

The data and analysis are presented in the next section, and the results and discussion for each of the research questions above are presented in the subsequent sections. First, the survey data are used to show how users and security managers judge IT-related risks, and some interpretations of these results are discussed. Second, on the basis of qualitative data, the ways in which security managers experience the human aspect of information security, user-directed measures, and their own role are presented and compared with how users view information security. These results and discussions are summarised and followed by a discussion on the information security digital divide between information security professionals and users. The paper concludes by stating that information security managers and users have different roles, responsibilities, approaches and spheres of authority. Because of these differences managers have unrealistic assumptions on which they base their practical management approach.

2. Data and analysis

The data used to answer the various research questions come from three sources: a survey of security managers in several Norwegian companies, a survey of users in a Norwegian public agency, and in-depth interviews of information security managers in large Norwegian companies.

2.1 Surveys

Data from two different surveys were used to reveal how users and information security professionals evaluate risk. The two surveys were developed to answer different questions from those in our study but they also include questions on risk evaluation. One survey evaluated the effects on users' awareness and behaviour of a participative training programme (Albrechtsen and Hovden, submitted). The other survey was the last in a time-series analysis of three surveys. The study covered an intervention group participating in the training programme and a control group not participating in the training programme. Independent-sample t-tests revealed no significant differences in the risk judgements between the intervention and control groups. The user group was therefore treated in the present study as a homogeneous population (N=157) with regard to risk judgement.

The other survey used in the present paper was distributed to security managers in Norwegian companies for the purpose of studying the effectiveness of organisational information security measures (Hagen and Albrechtsen, unpublished). N=87 managers responded. The quantitative data analysed in the present paper were not included in the other publications concerning the two surveys.

Both survey questionnaires contained the same set of questions for evaluating perceptions of threats and vulnerabilities. The respondents were asked to rate 14 threats and vulnerabilities on a 5-point scale from 1=no risk to 5=very high risk to the day-to-day operation of their organisation. The 14 threats and vulnerabilities included malicious attacks from outside the organisation; users as a vulnerability due to their lack of skills and knowledge; malicious acts inside the organisation; and incautious use of network connections and information.

Our hypothesis was that the quantitative analysis would reveal significant differences between users and information security managers. The hypothesis that no statistically significant difference in risk evaluation would be found between the two groups was tested by independent-sample t-tests.

2.2 Interview study of information security managers

The qualitative study consisted of 11 in-depth interviews with information security managers in large Norwegian companies. The objective was to discover how they interpreted management of the human aspect of information security. The managers' understandings were compared with a similar study of users' interpretations of information security (Albrechtsen, in press) and other studies on users' views on information security (e.g. Adams and Sasse, 1999; Besnard and Arief, 2004).

Topics such as the managers' views on users and managers' evaluations of measures, and on how the day-to-day information security work functioned were discussed during interviews lasting 60 to 90 minutes. The informants worked in four different fields of business: five in public agencies, two in oil and gas operators, two in manufacturing companies and two in logistics firms. All the informants' companies were distributed companies and had more than 1000 employees. Furthermore, the managers were experienced in the field of information security. Their roles and responsibilities were mainly concerned with the non-technological aspects of information security, e.g. developing documented systems, arranging awareness campaigns and supporting decision-makers at the line management level.

Qualitative research does not aim at generalised findings, but at providing insight into social processes (Straus and Corbin 1998; Thagaard 2003). Interviews make it possible for the informants to describe and explain processes experienced daily both broadly and in depth (Kvale, 2001). In qualitative data analysis, data reduction, data display and conclusion-drawing are interwoven before, during and after data collection (Miles and Huberman, 1994). This iterative approach was also used in the current study. The transcribed interviews were coded in HyperRESEARCH (a software tool for analysis of qualitative data) And the codes were categorised according to the research questions and analysed by switching between the whole picture and the details (Leiulfsrud and Hvinden, 1996) by: 1) testing registered ideas during data collection, transcription and coding; and 2) using detailed data as pieces in a jigsaw puzzle. The aim of this approach was to identify and examine patterns formed by the data, the reasons for the patterns, and differences between the patterns. The present paper presents the major patterns found by the analysis.

3. Risk judgement

This section presents the results of 151 users' and 87 information security managers' risk judgements of a set of threats/vulnerabilities to information security. Table 1 shows the demographic characteristics of the respondents and Table 2 the organisations to which the managers belonged. The users belonged to a Norwegian public agency with 500 employees, which was responsible for several national computerised registers used for support and services to businesses and the public administration.

Chi-square tests revealed significant differences in gender and age between users and managers. These differences could have influenced the results of the evaluations, but this cannot be definitely concluded since the groups differed with regard to other characteristics such as occupation and knowledge of information security. Multivariate analyses with risk evaluation as the dependent variable and demographic data as independent variables were not performed as it is outside the scope of the research questions.

Table 1. Demographic data for users and managers

	Users	Managers
N	151	87
Age		
18-29 years	6.0%	0%
30-39 years	40.4%	17.2%
40-49 years	33.8%	41.4 %
50-59 years	15.9%	34.5 %
>60 years	4.0 %	5.7 %
Gender		
Male	31.3%	79.1%
Female	68.7%	20.9%

Table 2. Demographic data for the managers' organisations

Organisations	
Public agencies	32.2%
Power suppliers & petroleum industry	27.5%
Finance industry	14.9%
IT and telecommunication	13.8%
Others	11.6%
No. of employees	
1-49	29.8%
50-499	26.3%
>500	43.7%

3.1 Results

The respondents were asked to assess whether 14 different threats/vulnerabilities posed 1) no risk, 2) little risk, 3) moderate risk 4) high risk or 5) very high risk to *the day-to-day operation of their organisation.* Figure 1 shows the mean value for each threat/vulnerability for each group. Independent-sample t-tests were performed to identify significant differences in the mean values of the respondents' risk judgments.

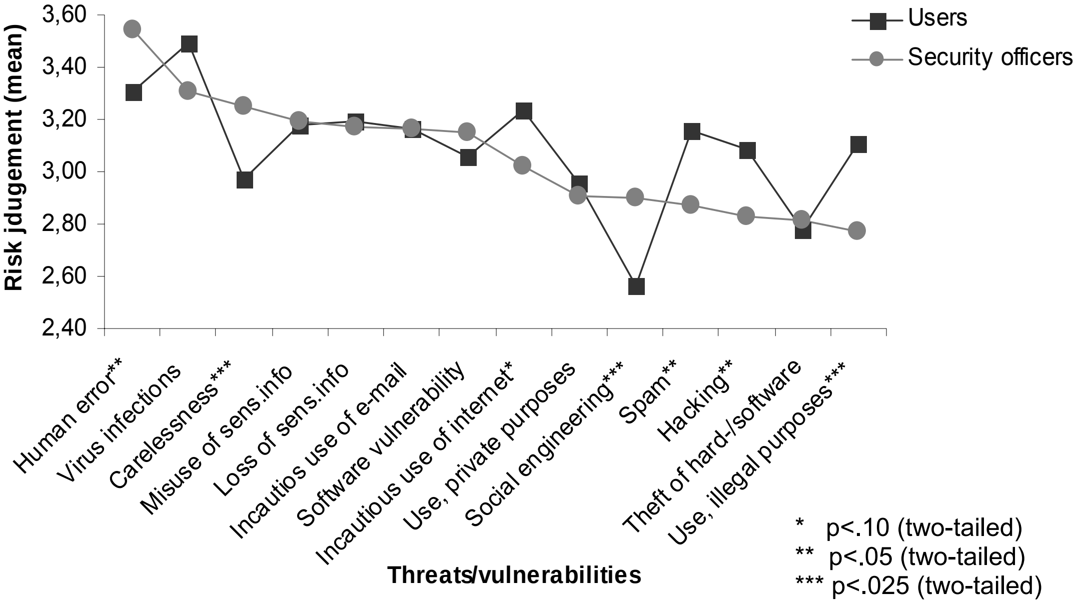

Figure 1. Mean values for judgments of IT-related risks by users (n=151) and information security professionals (n=87). Evaluated risk from 1= no risk to 5=very high risk

Half of the threats/vulnerabilities did not differ significantly between users and managers. These included technical items such as software vulnerabilities and virus infections. Treatment of sensitive information was also found in this group.

Seven mean values were significantly different. The security managers evaluated the risk level for four threats/vulnerabilities to be lower than users did: incautious use of the Internet (p<.10), spam mail (p<.05), use of the company's IT resources for illegal purposes (p<.025), and hacking (p<.05). The first two of these items may only affect individual performance, and do not necessarily have any effect on the organisation's day-to-day operation. Security managers ranked the risk level for three threats significantly higher than users did: IT-related human error (p<.05), user carelessness, e.g. leaving the computer unlocked (p<.025), and social engineering attempts, i.e. attempts to manipulate or deceive employees into making security breaches (p<.025). A common feature of these three vulnerabilities is that they are all related to users' lack of skills and knowledge.

The security managers considered users to be a greater problem, i.e. a threat, to information security than the users themselves did. The users did not believe that their lack of skills and knowledge posed a risk to the company to the same extent as managers did. With regard to the highest and lowest ranked risks in both groups, security managers ranked IT-related human error as the highest, and users ranked social engineering attempts as by far the lowest risk.

3.2 Discussion of the risk judgements

Few risk perception and risk judgement studies have been performed in the field of information security. One exception is a study by Kuttschreuter & Gutteling (2004) on the Y2K bug. The study showed that users perceived the likelihood that the millennium problem would have negative consequences to be greater, and worried more about it, than experts did. The opposing interpretations of risk between lay people and experts is, however, a much debated topic in general risk research (e.g. Shrader-Frechette, 1991; Slovic 2000; Sjöberg, 2002; Jäger et al., 2001), although without any particular emphasis on IT-related risks. These studies mainly consider global and societal aspects of risk, while we have investigated risk to organisations. Nevertheless, the general risk research literature does have some relevance to a discussion of the empirical results in our study.

Risk is normally defined in terms of two dimensions: the probability of an event occurring and the consequences of an event. However, individuals often evaluate risk subjectively and may be influenced by a wide range of psychological, social, institutional and cultural factors (Slovic, 2000). Slovic et al (2000) have identified 18 characteristics of risk that influence people’s risk perception, which they classified into three main groups: dread, familiarity and number of people exposed.

There has been a debate about which of these three components that is ranked highest by different groups (Rundmo and Moen, 2006), and there are different theories in the literature concerning the factors behind experts’ and lay peoples’ risk perception. Slovic (2000) argues that experts differ from non-experts as regards what they consider to be risk factors. On the other hand, Sjöberg (2002) argues that the factors behind the risk perceptions of experts and lay people are fairly similar. The present study shows that the differences in risk evaluation between users and experts diverge in both directions, but also that some risks are evaluated in a similar way. This seems to support Sjöberg’s argument (2002) that the factors explaining experts’ risk evaluation are similar to those influencing lay people.

The survey material analysed above did not contain questions about the risk characteristics on which the respondents based their evaluations. However, the present findings, together with those in the literature, allow certain conclusions to be drawn concerning the differences in risk evaluation.

Information security managers evaluate risks relating to user behaviour as being significantly higher than users do. The questionnaire distributed to the security managers included questions about specific incidents they had experienced during the previous year, and the results showed that about 50 per cent had experienced incidents caused by human error These accounted for by far the largest number of incidents most of the respondents had experienced. This could mean that security managers tend to emphasis the probability dimension when evaluating risk. Drottz-Sjöberg (1991) has also shown that experts tend to stress probability when asked about risk judgement, while lay people tend to stress consequences. The qualitative data and risk evaluations presented below confirm that security managers consider users to be a major threat to security, while users do not; they evaluate the consequences of their behaviour as being less serious than experts do, which is reflected in their own risk evaluation of their behaviour. This can be explained by the controllability factor (Slovic et al., 2000), since users feel that they have a high degree of control over situations in which they are involved.

According to Slovic (2000), people consult or refer to an affective pool containing all the positive and negative images associated with the objective or activity being judged, creating an inverse relationship between risk and benefit evaluations. Based on this argument it could be claimed that the high risk security managers associate with user behaviour is related to a low level of belief in the security benefits to be gained from users. This argument is supported by the qualitative results presented below, which show that managers tend to focus on users as a problem in information security.

The significant differences in risk evaluations presented in Figure 1 show that users evaluate situations that disturb their work, such as spam mail and incautious use of Internet and equipment, as being a higher risk than experts do. This may indicate that users are more self-centred in their evaluations and associate risk with the immediate consequences for them if something goes wrong. Users are also closer to and more familiar with such situations than with the wide-ranging consequences of human errors.

Users also evaluate hacking as a significantly higher risk than experts do. This is probably due to the fact that security managers are aware that defences against hacking are in place in the company’s technological configurations, and also that they have access to the statistics on avoided attacks. Users, on the other hand, do not possess this information and may be influenced by for example media reports of hacking on Internet banks and such. This argument is supported by our risk evaluation figures for virus infections, which are also extensively covered by the media. Again, information security managers have access to statistics showing the number of prevented virus infections in the organisation, which users do not. In addition, most anti-virus companies have up-to-date statistics on virus threats on their web-pages, which may also influence the experts’ risk evaluations. As a result, managers are aware of the large number of virus attempts. Again, this shows that experts tend to use probability in evaluating risk rather than consequences, since most companies today have up-to-date anti-virus software that seldom allows virus infections. Although users do not possess this knowledge, they still evaluate risk from viruses as the highest of the 14 threats and vulnerabilities. Media coverage on the virus threat can explain this as well.

4. The role of users in the information security work

4.1 Information security managers’ view of users

In the interview study of information security managers’ views the informants found it difficult to give details of their experience of user performance. Two main reasons were given for this superficial interpretation of users. First, the managers were from large organisations with a large number of users. This meant that there were great variations between the users in information security knowledge and skills, personal characteristics, and work tasks, which made it difficult to give specific details. Second, several of the informants felt they lacked the resources to systematically review the activities of different groups of users or to meet with them. As a result there was often little interaction between managers and users. Some of the interviewed managers felt that it was a paradox that on the one hand they know how important users are for overall security, while on the other they have no detailed knowledge of the quality of user performance or user experience of information security:

> “One of the main purposes of my work is to make our users aware of information security. So I certainly should know something about them - but I have to admit I don’t.” *Information security manager, public agency IV.*

The managers’ statement that it was difficult to be specific with regard to the security performance of users could have weakened the validity of our qualitative study, but when each interview had lasted for a while it turned out that the managers had some detailed knowledge about users and management of the human aspect of information security. Schön (1983) has argued that practitioners often know more than they can express in words. Using interviews as a research tool makes it possible to go more deeply into the informant’s everyday work (Kvale, 2001) and thus bring out their tacit knowledge.

The interviewed managers’ main expectations and experiences of users can be described as Janus-faced: they regarded users as both a resource and a problem, see Figure 2. Users were experienced as a potential resource in terms of their ability to behave cautiously; awareness of incidents, threats, vulnerabilities and problems; reporting of incidents or insecure factors; and compliance with rules. Some managers believed that users view information security as important, especially when dealing with information in accordance with the non-disclosure agreement in public agencies.

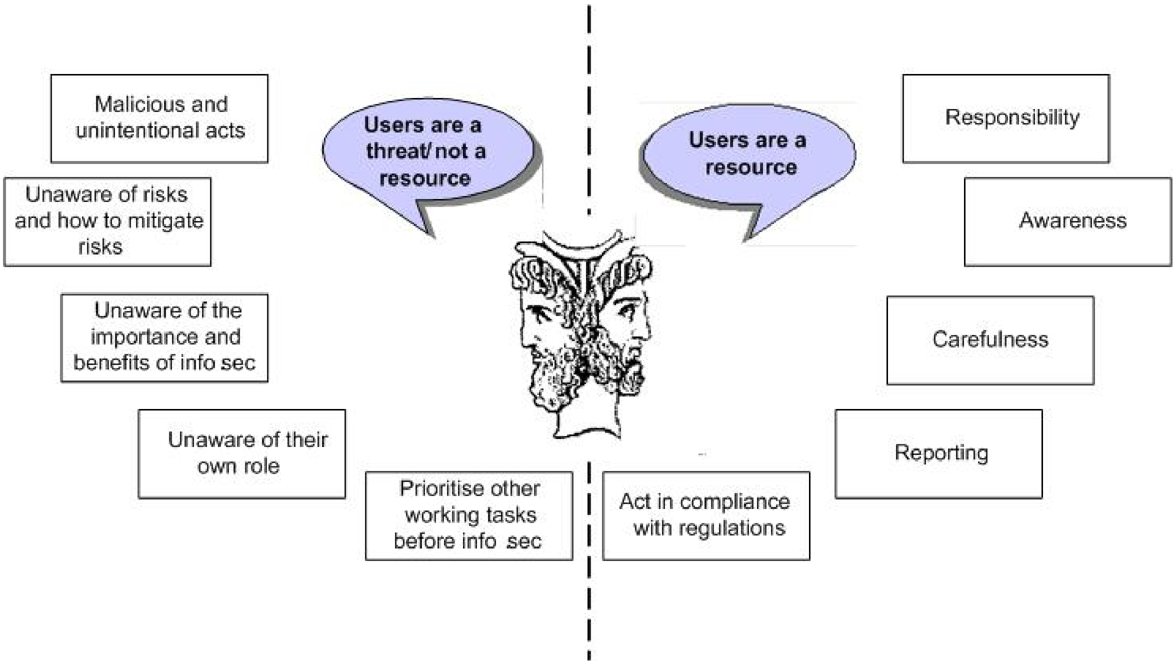
Malicious and unintentional acts
Unaware of risks and how to mitigate risks
Unaware of the importance and benefits of info sec
Unaware of their own role
Prioritise other working tasks before info sec
Users are a threat/not a resource
Users are a resource
Responsibility
Awareness
Carefulness
Reporting
Act in compliance with regulations

Figure 2. The Janus face of the users' role in information security. Interpreted from interviewed information security managers' experiences on users. In sum, the informants focused mainly on the left side of the Janus-face.

In all kinds of research and daily life it is usually easier to call to mind negative rather than positive factors. This common experience was reflected in the interviews, which tended to emphasise negative judgements of users rather than positive ones. One of the problems cited was the role of users in causing adverse incidents through malicious or unintentional behaviour. Most of the negative side of the Janus face of users was related to day-to-day operation, i.e. users caused problems because they lacked the necessary incentives, knowledge and skills for safe and secure behaviour.

Several of the managers had found that users were not aware of information security as it applied to them. Often they only took information security into consideration when an adverse incident occurred. Many of the informants felt that users did not realise the benefits of information security, and considered practicality and efficiency to be far more important for their work. The managers also believed that if it was possible to bypass a barrier or a documented requirement most users would do so. A security manager from the petroleum industry expressed this succinctly using the example of passwords:

> "On the one hand users do not want to have passwords. On the other hand they do not see the consequences of not having passwords." *Information security manager, Petroleum I.*

If users do not perform their work in a safe and secure manner, this can have considerable consequences, but according to some of the managers users do not realise this. Users often see their own work in isolation and are not aware of the implications of their use of IT systems. Users are often familiar with security measures they should be taking but they often do not take them, and tend to give lower priority or to be indifferent to security work. In this respect it is not lack of knowledge, but lack of motivation that is the main user-related problem. The principal reason given by the managers for why users do not regard information security as important and beneficial is that users tend to give more priority to other work tasks over information security. The managers also claimed that the users were not aware of the risks or of how to mitigate them. Some interviewed managers state that users often assume that responsibility for information security lies with the technology and the information security managers.

Most of the interviewees said that users give information security second or third priority in their everyday work and they explained this by saying that users are not used to thinking about anything more than their work tasks. Some of the managers claimed that the financial situation of the company prevented users from performing any tasks outside their main area of work.

4.2 Managers' experiences compared to users' views on the user role in information security

An interview study of users employed in a Norwegian bank and an IT company (Albrechtsen, in press) showed that users believe that they have an important role to play in information security but do not have the knowledge to act in a safe and secure manner. The interviewed managers in the present study shared this view of users as an important resource, but they still laid most stress on the negative sides of users. Both the interviewed groups agreed that users do not have the knowledge or skills for safe and secure behaviour, a lack that both groups believed to be to the result of insufficient training.

The two qualitative studies of users and managers also revealed some divergent opinions on the human aspect of information security. During the interviews, the managers mainly concentrated on the non-resource side of the Janus face of users. The users on the other hand focused on how they could serve as a resource in the information security work. Although some of the managers felt that users were unaware of the importance and benefits of information security, the results of the interview study of users (Albrechtsen, in press) showed that most users agree that information security is important to the company, especially with regard to the company's public image. One problem experienced by both interviewed groups was the same as that found by Adams and Sasse (1999), Besnard and Arief (2004) and Post and Kagan (in press), who claim that users trade off information security against efficiency and functionality.

5. Managing the human part of information security

5.1 Information security managers on measures for promoting secure behaviour and improving awareness

Our findings revealed that a wide range of measures were used by managers to influence user behaviour and awareness. Table 3 presents an overview of the categories of measures taken by the interviewed managers' companies.

Table 3. Information security measures targeted at users by the interviewed managers' companies

Group of measure:	Public agency I	Public agency II	Public agency III	Public agency IV	Public agency V	Manufacturing I	Manufacturing II	Petroleum I	Petroleum II	Logistics I	Logistics II	Total
Technological solutions (technological framework for what users are allowed to do, e.g. access control)	●	●	●	●	●	●	●	●	●	●	●	**11**
Documented system** (documents describing expected behaviour: e.g. policies, guidelines, instructions)	●	●	●	●	●	●	●	●	●	●	●	**11**
Electronic information (e-mail, intranet messages, screen saver)	●	●	●	●	●	●	●	●	●	●	●	**11**
Information material (newsletters, posters, leaflets, objects)	●		●		●	●		●			●	**6**
Education and competitions (interactive training, training new employees, interactive competitions)	●	●			●	●			●			**5**
Personal presence (informal conversations, observation)	●	●									●	**3**
Gatherings (large plenary sessions, small information meetings)	●	●	●		●				●		●	**6**
User participation (active involvement of employees in info.sec. activities)			●									**1**

Technological tools that seek to control and monitor user behaviour were used by all the interviewees' organisations. Technology is mainly used because it is a foolproof system for preventing many of the intentional and unintentional actions of users, since it limits what users are and are not allowed to do, e.g. by access control. It is also believed to be more sound and reliable than users:

> "The advantage of technological solutions is that there are no human parts that can fail. Of course they sometimes fail, but not in the same way as humans do. You don't have to inform the technology, which is a clear advantage. Technology definitively reduces risk more than you can train a user to do." *Information security manager, Public agency I*

All the interviewed managers said that they used security policy, the non-disclosure agreement, guidelines and/or instructions. These documented systems were intended to describe what users were expected to do or not do. In the informants' experience it was important to notify users of the existence of a system of requirements regarding user behaviour. However, they believed that few users read the documents and doubted whether the documents had any notable effect on awareness or behaviour among those who did read them. The interviews with the managers indicated four reasons for the poor effect of information security documents on users' security behaviour: 1) users prioritise other work tasks; 2) it is difficult for users to understand the content because it is poorly presented; 3) the documentation is not readily available or difficult to find; and 4) the tone of the documentation is admonitory and puts people off. Nevertheless, the managers emphasised that the documents were important because they formed the basis for other measures. The documentation is also important because it serves as a reference point when sanctions have to be imposed.

Formal one-way communication methods such as information material, electronic information and interactive training were used by all companies. The intranet was particularly widely used for spreading information, but several of the companies used other means as well, like screen savers, e-mails and leaflets. Information on security was made available to users, but this requires users to read it and make an effort to obtain the knowledge. According to the interviewed managers users often lacked the motivation and awareness to do so. Users are also bombarded with information from other parts of the organisation, which makes it even harder for information security messages to reach the targeted group. As users tend to be uninterested and unmotivated as regards information security, this kind of information is filtered out in the total information overload. Although the informants had no belief in the effect of these formal one-way information measures, they develop and use them a great deal. This paradox can be explained by the fact that the measures are simple and do not require many resources, and some of the informants believed that even if the information reached only 10 per cent of users, this was still better than none at all.

According to the informants, the most efficient method of influencing user awareness and behaviour is some form of interaction between users and security managers, e.g. in small-sized information meetings where they meet face-to-face. Table 3 shows, however, that this kind of measure is among the least used, mainly because of the cost. Some of the managers found that simply being present and visible, e.g. spending time in public spaces in the organisation and conducting informal conversations, was very effective.

> "Meeting people is something else than sending electronic information. This approach is important, not least regarding making myself and my role visible… There are always a lot of questions regarding information security when I meet people. This indicates that they are interested and see the benefits of information security when they are approached this way. Both formal and informal contact with employees has been useful, in particular informal personal conversations… The approach requires a lot of me, but I nevertheless rate visibility as very important." *Information security manager, Public agency II*

Although few of the managers had actually made use of it, user participation was rated the most effective tool for improving user performance by several interviewed security managers. Only one of the interviewed managers had experience of getting users to participate in information security work. He had involved employees and managers in simple risk analysis processes for each department in the public agency where he worked:

> “There have been several aha experiences for the users, the top management and me when such analyses have been carried out… When they [users and managers] discuss security problems or solutions, they have to use their own working conditions as a background. There is no one who knows this condition better than the users themselves… Creating discussion is the most important thing. If I participate in the processes myself, I get an important impression of the information security reality of the organisation” *Information security manager, Public agency III*

There was a relation between the informants’ evaluation of the effects and their choice of measures. The most widely used measures in Table 3 were regarded as the least effective, while the measures considered to be most effective were the least used. The degree of involvement of users was related to the degree of effect on individual security awareness. The managers seemed to go through a number of stages with regard to the measures they used: from documents to formal information to human interaction to user participation. The experienced security manager who had used a participative approach had not always approached users this way, and described the development of his information security approach to users:

> “When I started my job as a security manager I looked on myself as a missionary, I was going to rescue the organisation. After a while, I understood that I was the only one interested in this. I wrote two information security handbooks that were distributed in the organisation. It became top-down information, which wasn’t followed up over time. I arranged information meetings with one-way communication, where I told people how they should act. My experience was that these approaches were wrong, they did not function. I’ve learned from this, and now believe in involving users in the information security process.” *Information security manager, Public agency III*

5.2 Users’ experience of administrative information security management measures

An interview study of users at a Norwegian bank and an IT company resulted in the following patterns regarding how users experienced administrative information security measures (Albrechtsen, in press):

- Users tended to leave responsibility for information security to the technology and information security professionals. They had confidence in the technological security systems.
- Most of the users were not familiar with the content or availability of their companies’ documentation on expected behaviour.
- The IT company had organised several formal awareness campaigns with one-way communication for several years before the study. Almost all the interviewed employees at this company felt that the awareness campaigns had no effect on their situation, and had no memory of the previous campaigns.
- Several of the users at both companies believed that involving users and interacting with security managers is a much more efficient method of improving user behaviour and knowledge than awareness campaigns and written rules and guidelines. Adams and Blanford (2005) have shown by

qualitative studies in hospitals that all involved actors gain by this in terms of involvement and openness.

The users' views on information security measures were similar to those of the information security managers. The reasons given for the views were also the same. Both groups found that documents and one-way information had no effect, and both groups considered technology a solid and necessary foundation for a high information security level at an organisation. Users and managers agreed that user participation and interaction between users and managers were the most efficient tools for raising awareness among users; however users were not aware of the resources required by participation.

6. The role of information security managers

Several of the security managers stated that they did not consider their role to be that of a policeman or a janitor. Security managers neither impose sanctions nor do they clean up after users.

> "Users often have inadequate security awareness. What they should do is in reality simple; nevertheless they don't do these things. I cannot walk around in the organisation and tell people what to do or fix problems they have created. You have to carefully approach the [organisational] culture, being too much of a policeman or janitor can hit back at you. This is a challenge. I've learned that you have to wear different hats than the hat of a policeman or a janitor."
> *Information security manager, public agency II*

Although it was claimed that "IT security is not IT policing", the most widely used measures and strategies implemented to influence users (Table 3) were duty-oriented, i.e. they focused on what users are allowed or not allowed to do, and on surveillance and control. Since these characteristics can be described as "IT policing", this shows that there was a difference between the reasoning behind the most commonly used measures and the way in which information security managers wished to appear.

The interviewed managers said that policing was built into technological tools and carried out by others in the organisation who were responsible for imposing sanctions, while the janitor's job was done by the IT department, which was also the technical operative for information security. According to the informants, the information security manager's role is to:

- give advice regarding information security to all parts of the organisation
- give input to decisions made by others, e.g. the line manager or the IT department.
- develop documentary information on security systems.
- be flexible and adapt to the requirements of the organisation while at the same time ensuring security.
- communicate the importance of information security in an understandable way to all members of the organisation.

Visibility was also considered important by users (Albrechtsen, in press). Some of the interviewed users said that the information security managers were invisible, and that this resulted in a lack of knowledge about information security work in the organisation. The users stated that it was important to know who worked with information security since this made it easier to report problems and ask questions. It was also claimed that seeing a manager is important for raising awareness.

7. Information security digital divide within organisations

The empirical findings reveal different experiences and views between security managers and users, indicating an information security digital divide within organisations:

- Both the interviews and the risk evaluations showed that managers focus most on the problem aspect of users. Users, on the other hand, are interested in being a resource in the information security work, and do not see themselves as a threat. Information security managers mainly concentrate on the threat side of the Janus-face of users, while users focus on the other side, the resource-part.
- Security professionals and users have different opinions on the human part of information security as users experience information security as important to the organisation and its reputation, while professionals feel users are not aware of the impriotance of infomraiton security.
- Paradoxically, at the same time the interviewed managers stated that users are important for security, most of them also said that they had no explicit, detailed knowledge of their users' information security performance, which indicates that there is a gap between their professional knowledge and real-world practice.
- The studies revealed little interaction between users and information security managers, who seldom had contact with one another. As a result the users regarded the security managers as remote, invisible and secretive; in spite of this they continued to leave the responsibility for information security up to the managers. Both groups considered interaction to be the most efficient tool for influencing user behaviour and awareness.
- Users and information security managers had different priorities regarding information security. The managers had the impression that the users gave information security lower priority than other work tasks, which was borne out by the user study (Adams and Sasse, 1999; Besnard and Arief, 2004). Security managers on the other hand had information security as their main work task.
- There is no mutual trust between users and information security managers. Although the users trusted the information security managers and the technology to take care of security, the managers did not trust the users.

The empirical findings also showed that information security managers and users have some points of agreement. They agree on the effectiveness of certain information security activities aimed at users, and both groups had little belief in the effectiveness of documentation and formal one-way information measures on user awareness and behaviour. They both felt that the participative approach is most likely to modify awareness and behaviour. The managers viewed technological solutions as an important means of controlling and monitoring user behaviour, while users viewed technology as a means of ensuring information security .

7.1 Different work situations and rationalites

Figure 3 shows the levels of information security professionals and users in relation to information security tasks. The differences may explain the information security digital divide in an organisation. The professionals mainly operated at a distance from the everyday work tasks and vulnerabilities in the organisation, but could find themselves at the sharp end in situations requiring crisis management. Users, on the other hand, normally operated at the sharp end, close to threats and vulnerabilities.

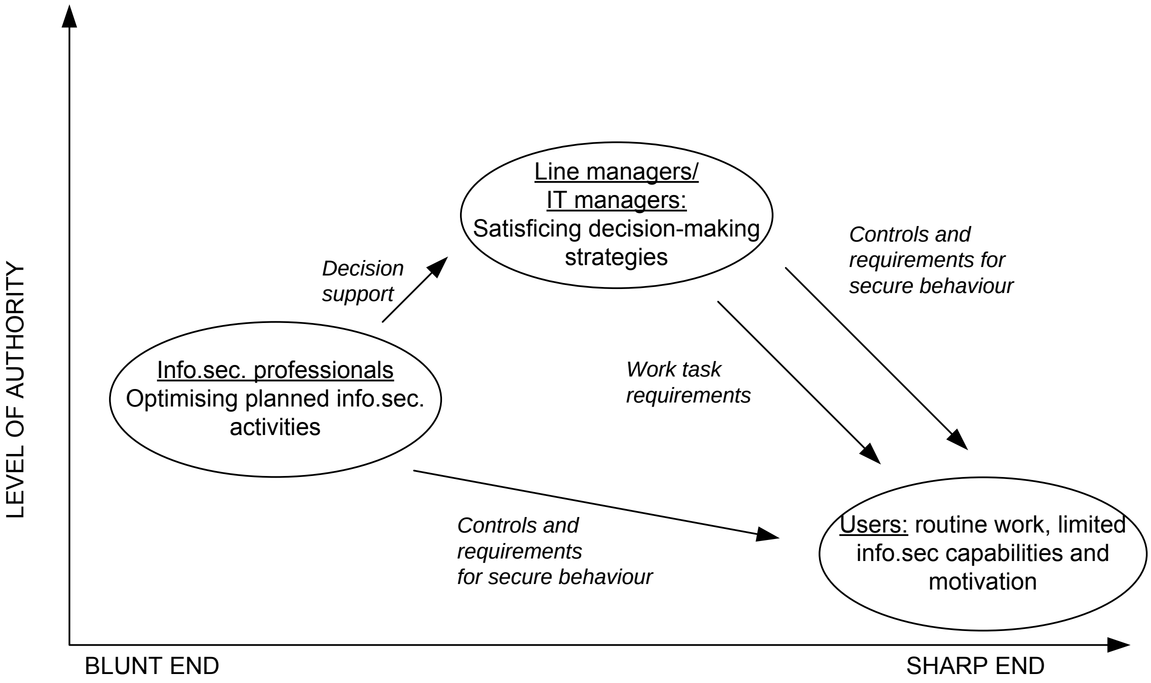
LEVEL OF AUTHORITY
Line managers/
IT managers:
Satisficing decision-making strategies
Decision support
Controls and requirements for secure behaviour
Info.sec. professionals
Optimising planned info.sec. activities
Work task requirements
Controls and requirements for secure behaviour
Users: routine work, limited info.sec capabilities and motivation
BLUNT END
SHARP END

Figure 3. Work situations in operative information security work. Based on Rosness (2001)

The information security professionals have degree of specialisation, access to expert knowledge, time and resources for collecting and processing information, and sophisticated tools and methods for information processing. Consequently, they have time and space to optimise planned information security activities. On the other hand, since they are at the blunt end they often lack hands-on experience of the systems they influence or develop since they are not close to threats, vulnerabilities or actual working situations (Rosness, 2001; Rosness et al., 2004). The interviewed managers confirmed this by their statements that they knew little about the users' situation and that they had little interaction with users. They said that they were seldom decision-makers; their task was to provide input to decisions made by managers in other parts of the organisation. Besides decision input, the information security professionals influenced users by developing strategic documents, e.g. instructions for safe and secure behaviour and formal one-way communication, e.g. e-mails.

In addition to the roles of users and information security professional, those of line managers and IT managers are also shown in Figure 3. This role has not been given much attention in the present paper, although these managers have an important role in the information security work of an organisation. According to the information security professionals, many of the strategic and operative information security decision are made by line and IT managers, often on the basis of expert evaluations made by the professionals. The decision-making situations of line and IT managers were often characterised by lack of time, information overload and the frequent necessity to make rapid decisions (Rosness, 2001). Under such conditions decision-makers are likely to base decisions on a satisficing strategy (March and Simon 1958), i.e. they make decisions that are good enough but not necessarily the best option. Kørte et al. (2002) have shown that decisions made at the management level based on results from risk analysis made by experts at the blunt end tend to be satisficing decisions.

The low priority users give to information security is the result of a range of different management decisions influencing the users' total work situation. Users at the sharp end are recipients of outputs from decisions concerning information security and other work tasks made by both professionals and other management. One output of management decisions takes the form of information security measures that directly influence the working day of users at the sharp end, e.g. new technological security solutions and mandatory training programmes. However, this tends to conflict with management decisions to impose work tasks other than information security, e.g. requirements with respect to sales and efficiency. Rasmussen (1997) has shown that individual performance is the result of pressure to achieve work efficiency, the line of least possible effort, and risk mitigation. Adams and Sasse (1999), Besnard and Arief (2004); Albrechtsen (in press), and Post and Kagan (in press) have shown that users consider other work demands to be more important than information security tasks in their day-to-day work.

7.2 Information security measures

The most commonly employed user-targeted measures are technological solutions, documented requirements and formal one-way communication of information, see Table 3. Both users (Albrechtsen, in press) and managers stated that documents and formal information had little effect on awareness and behaviour. This can be partly explained by the unrealistic expectations of those developing the measures and the practical management models they use (Rosness, 2001) owing to their limited hands-on knowledge of the everyday work and information security practices in the organisation. For example, in order to have effect, formal information must be read by users. Users at the sharp end, however, are likely to have most of their working time occupied by other, work tasks. Security information is only one of many different kinds of information that users have to process. Users at the sharp end thus have a limited motivation and capability for information security processing.

Technological measures frame and control what users are allowed and not allowed to do; documented requirements and passive information measures are based on the assumption that users are rational actors who always behave in accordance with information security requirements and who acquire the necessary knowledge by reading the documentation or from other communicated information (Albrechtsen and Grøtan, 2004). These assumptions by managers have many similarities with Morgan’s (1998) metaphor of organisations as machines, i.e. the information security organisation is seen as a stable machine where humans and technology are components that will make the organisation work efficiently and predictably in a safe and secure manner.

This reasoning is in conflict with both the normal working day of users and the characteristics of modern organisations. Schön (1991) has argued that a technical rationality is not adequate for environments characterised by uniqueness and uncertainty. Organisations and their stakeholders are living organisms, not stable, efficient, predictable systems. Mechanical approaches to organisations and management do not pay attention to human resources and values, unlike the information security measures considered effective by our managers, e.g. face-to-face information and user participation.

As shown by the vertical axis of Figure 3, information security activities are also closely related to power and authority, and this contributes to the information security digital divide within the organisation. Users are not in a position to influence information security issues since they are mainly passive recipients of information on already decided measures. There are no discourse-based power mechanisms that form identity and allow change at an individual and organisational level. This is supported by Bachrach and Baratz’ second face of power argument (Clegg, 1989): latent conflicts over information security do not become visible because users are prevented from raising information security issues, e.g. the problem of security measures as an obstacle to everyday work or the fact that security measures do not function as intended.

A strategic approach to power, represented by e.g. Foucalt, sees power as a matter of instruments, techniques and procedures attempting to influence the actions of those who have a choice about how they might behave (Hindess, 1996). In the present context both technological and administrative measures were used to direct users. Information security managers had the power to influence the development of these measures, in the sense of Dahl’s (1963) view of power: “A has power over B to the extent he can get B to do something B would not otherwise do.” Although they were not themselves decision-makers, and only provided input to other managers’ decisions, the information security managers did have a certain amount of power. Their expert knowledge and specialised terminology put them in a position that made it difficult for others to influence security work.

8. Conclusion

Users and information security managers have different responsibilities and spheres of authority, and employ a different rationality. Maintaining information security in an organisation is the information security manager’s main work task. Users, on the other hand, have other, equally important, work tasks, mainly achieving the organisation’s goals of profit and productivity. However, users do have a responsibility to maintain information security since this is also one of the organisation’s goals.

The information security digital divide within organisations discussed in this paper is not in itself a threat to the functionality of information security management. However, the differences in approach, experience and priorities between managers and users in this field result in management strategies based on the prejudiced view that users are more of a security threat than a resource.

Both security managers and users call for greater interaction and dialogue. Such an approach is likely to improve each group’s understanding of the work of the other and to bridge the divide between them, thus making information security measures more effective.

Acknowledgements

The authors thank the interviewed security managers for sharing their experience on information security. Eirik Albrechtsen's PhD project is financed by Vesta insurance company.

References

Adams A, Blanford, A. Bridging the gap between organizational and user perspective of security in the clinical domain. International Journal of Human-Computer Studies 2005; 63(1-2): 175-202

Adams A, Sasse MA. Users are not the enemy. Communications of the ACM 1999; 42(12):41-46

Albrechtsen E, A qualitative study of users’ view on information security, Computers & Security; in press, doi:10.1016/j.cose.2006.11.004

Albrechtsen E, Grøtan, TO. Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner. In Norwegian [Old-fashioned thinking in modern organisations? On ICT-security in knowledge organisations]. In Lydersen S (ed.). Fra flis I fingeren til ragnarokk. Trondheim, Norway: Tapir Akademisk Forlag; 2004: 319-335

Albrechtsen E, Hovden J. Improving information security awareness and behaviour by a user participative approach: an intervention study. Submitted article

Besnard D, Arief B. 2004. Computer security impaired by legitimate users. Computers and Security 2004; 23(3):253-264.

Clegg, SR. Frameworks of power. London: SAGE Publications; 1989

Dahl RA. Modern Political Analysis. Englewood Cliffs, New Jersey: Prentice-Hall Inc; 1963

DiMaggio P., Hargittai E., Celeste C. Shafer S. Digital Inequality: From Unequal Access to Differentiated Use In Social Inequality. Edited by Kathryn Neckerman. New York: Russell Sage Foundation. pp. 355-400. 2004.

Drottz-Sjöberg BM. Non-experts definitions of risk and risk perception. In: RHIZIKON: Risk Research Reports no.3 (Stockholm: Centre for Risk Research. 1991

Hagen J, Albrechtsen E. Use and effectiveness of organizational information security practices. Unpublished.

Harittai E. Second-Level Digital Divide: Differences in People's Online Skills. First Monday 2002; 7(4).

Hindess B. Discourses of Power. From Hobbes to Foucault. Oxford: Blackwell Publishers Ltd; 1996

Jaeger CC, Renn O, Rosa EA, Webler, T. Risk, Uncertainty and Rational Action. London: Earthscan Publications Ltd; 2001.

Jung JY, Qiu JL, Kim YC. Internet Connectedness and Inequality: Beyond the "Divide". Communication Research 2001; 28(4): 507-535

Kørte J, Aven T, Rosness R. On the use of risk analysis in different decision settings. Presented at ESREL2002.

Kuttschreuter M, Gutteling JM. Experience-based processing of risk information: the case of the millennium bug. Journal of Risk Research, 2004; 7(1): 3-16

Kvale S. Interviews. An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage; 1996.

Leiulfrud H, Hvinden, B. Analyse av kvalitative data: Fikserbilde eller puslespill? In Norwegian [Qualitative data analysis: puzzle picture or jigsaw puzzle?] In Holter H, Kalleberg R. (eds.) Kvalitative metoder i samfunnsvitenskapene. Oslo, Norway: Universitetsforlaget; 1996.

March J, Simon, HA. Organizations. New York: John Wiley; 1958

Miles MB, Huberman AM. Qualitative Data Analysis. Thousand Oaks, CA: Sage Publications; 1994, doi:10.1016/j.cose.2006.10.004

Morgan G.. Images of Organization. San Francisco : Berrett-Koehler Publishers; 1998
Partridge H. Establishing the human dimension of the digital divide. In Quigley E (ed) Information Security and Ethics: Social and Organizational Issues. Hersey, US: RM Press; 2005: pp. 23-47.

Post GV, Kagan A. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Computers & Security; in press.

Rasmussen J. Risk management in a dynamic society: A modeling problem. Safety Science 1997;27(2/3):183-213

Rosness R. Om jeg hamrer eller hamres, like fullt så skal der jamres. Målkonflikter og sikkerhet. In Norwegian [Goal conflicts and safety]. SINTEF report no. STF38 A01408M; 2001.

Rosness R, Guttormsen G, Steiro T, Tinmannsvik RK, Herrera IA. Organisational Accidents and Resilient Organisations: Five Perspectives. 2004. SINTEF report no. STF38 A04403

Rundmo T, Moen BE. Risk Perception and Demand for Risk Mitigation in Transport: A comparison of Lay People, Politicians and Experts. Journal of Risk Research 2006; 9(6): 623-640

Schön DA. The reflective practitioner : how professionals think in action. New York : Basic Books; 1983

Shrader-Frechette KS.. Risk and rationality. Oxford: University of California Press; 1991

Sjöberg L. The Allegedly Simple Structure of Experts' Risk Perception: An Urban Legend in Risk Research. Science, Technology & Human Values 2002; 27(4): 443-459

Slovic P. The perception of Risk. London: Earthscan Publications Ltd; 2000

Slovic P, Fischhoff B, Lichtenstein S. Facts and Fears: Understanding Perceived Risk. In Slovic P. The perception of Risk. London: Earthscan Publications Ltd; 2000; pp.137-153

Strauss A, Corbin J. Basics of Qualitative Research. Thousand Oaks, CA: SAGE Publications; 1998

Thagaard T. Systematikk og innlevelse. En innføring i kvalitativ metode. In Norwegian [Introduction to qualitative methods]. Bergen, Norway: Fagbokforlaget; 2002.

Warschauer M. Reconceptualizing the Digital Divide. First Monday 2002; 7(7)

PAPER III:

Albrechtsen, E. and Hovden, J.

“Improving information security awareness and behaviour by a user participative approach: an intervention study”.

Accepted for review in *Information & Management*

Is not included due to copyright

PAPER IV:

Hagen, J., Albrechtsen, E. and Hovden, J.

“Implementation and effectiveness of organisational information security measures”.

Accepted paper march 2008
Information Management & Computer Security

Implementation and effectiveness of organizational information security measures

Hagen, J.* ; Albrechtsen, E.; Hovden, J.****
* Gjøvik University College, Gjøvik, Norway
** Norwegian University of Science and Technology, Trondheim. Norway

Abstract

Purpose: Study the implementation of organizational information security measures and assess the effectiveness of such measures.
Methodology/approach: A survey was designed and data were collected from information security managers in a selection of Norwegian organizations.
Findings: Technical-administrative security measures such as security policies, procedures, and methods are the most commonly implemented organizational information security measures in a sample of Norwegian organizations. Awareness-creating activities are applied by the organizations to a considerably lesser extent, but are at the same time these are assessed as being more effective organizational measures than technical-administrative ones. Consequently, the study shows an inverse relationship between the implementation of organizational information security measures and assessed effectiveness of the organizational information security measures.
Originality/value: Provides insight into the non-technological side of information security. While most other studies look at the effectiveness of single organizational security measures, the present study considers combinations of organizational security measures.
Keywords: Information security; effectiveness; implementation; organization; policy; awareness
Paper type: Research paper.

1 Introduction

Information security includes organizational aspects, legal aspects, institutionalization and applications of best practices in addition to security technologies (Von Solms, 2000, 2001, 2006; Siponen and Oinas-Kukkonen, 2007). A study by Siponen and Oinas-Kukkonen (2007) reveals that research on information security traditionally has been dedicated to technological aspects, and that more research on the non-technical aspects is needed. The aim of this article is to contribute to knowledge about the organizational aspects of information security. This is achieved by empirical research on the implementation and the effectiveness of organizational security measures.

Standards and public guidelines for information security management, e.g. ISO/IEC 27001 and the guidelines generated by Bundesamt für Sicherheit in der Informationstechnik (BSI) provide, among other things, a wide range of different organizational information security measures and activities. In order to minimize the complexity of the studied organizational security measures in this paper, the measures are categorized into four main groups: security policy; procedures and control; non-technological tools and methods; and organizational and individual awareness creation and maintenance.

- The *security policy* is the foundation of any security regime. It specifies the strategies behind an organization's information security approach by a written document, directly linked to the overall strategy of the company (Höne and Eloff, 2002; Doherty and Fulford,

2005). Although this is a single measure, it is regarded to be so essential to information security management that it is worth its own category of organizational measures.
- *Procedures and control* are directly derived from the security policy. This group of measures consists of documents guiding individual and organizational behaviour such as user instructions, security plans and non-disclosure agreements, as well as controls and follow-up activities of the documented systems e.g. by disciplinary processes.
- *Administrative tools and methods* are both proactive and reactive means such as asset classification, risk analysis, audits, and incident reporting systems.
- *Creation and maintenance of security awareness* include both individual and collective activities, i.e. education and awareness-raising initiatives. E.g.: emails, pamphlets, mouse pads, formal presentations and discussion groups (Voss, 2001; Hubbard, 2002).

The study of implementation and assessment of organizational information security measures is approached by considering the following research questions:
- What organizational security measures are implemented in a sample of Norwegian organizations?
- How is the effectiveness of different groups of organizational security measures assessed?
- What are the relations between the implementation of organizational measures and the assessed effectiveness of the security measures?

The research questions were answered by analysing the answers from 87 information security managers in Norwegian organizations. Due to the modest sample size, the present study does not aim to present a representative picture of organizational information security measures, but rather explore relations between implementation and effectiveness of measures, which should be independent of sample size.

The rest of the paper is structured in the following way. First, a brief literature review on effectiveness of organizational security measures is given, including theoretical and empirical understandings of effectiveness of security measures. This section is followed by a description and argumentation of the method used in the study. Results and discussion are interwoven in the subsequent sections; descriptive statistics about implementation of groups of organizational measures are presented, followed by a discussion of the relationship between implementation of measures and how security performance is assessed. Thereafter, subjective assessments of measures are presented. The assessments were made independent of whether the measures were implemented or not. The paper concludes by comparing the implementation of organizational measures with the assessed effectiveness of organizational measures.

2 Effectiveness of organizational security measures

In business terms, managerial success is often measured by effectiveness, such as whether objectives are accomplished or not, but it can also be expressed in terms of achieving a certain result. A literature search on effectiveness and information security reveals four interrelated perspectives on effectiveness of information security measures:
- *The risk management perspective:* information security measures reduce the risk of unwanted incidents. Failures of information security are clearly adverse events which cause losses to businesses; information security is thus a risk management discipline that manages the cost of information risk to the business (Blakely et al., 2001). In this perspective, effectiveness is understood as the ability of a measure to reduce risk to an acceptable level.
- *The economic perspective:* information security measures give positive return of investment. An economic approach to information security is suggested by Gordon and Loeb (2002), who have developed an economic model for information security. They argue that a company

should maximize the expected benefits from investment to protect their information. In this perspective, effectiveness of information security measures is understood as the ability of a measure to give a positive return of investment, i.e. the ratio of money gained relative to the amount of money invested.

- *The legal perspective:* information security measures avoid violations of legal requirements. Efforts must be made to meet legal requirements, which in turn should prevent possible security breaches (Lobree, 2002). In this perspective effectiveness is understood as the ability of a measure to assist the organization to meet legal requirements.
- *The cultural perspective:* information security measures create a good security culture. In this perspective, effectiveness is understood as the influence of a measure on individual and organizational awareness and behaviour in a positive direction.

The four perspectives are clearly interrelated, although they describe different expectations of the performance of the information security measures. How legal and regulatory requirements are met will for instance depend more on people and procedures than on technical security measures. What is needed is the right combination of measures that reduce the business risks to an acceptable level and at the same time ensure compliance to the law (Sundt, 2006; Berghel, 2005). In the present study we have not used an unambiguous definition of the notion of effectiveness, but have made this an empirical question: how do the respondents define effectiveness of security measures? This question is addressed in Section 7, and shows that the survey respondents mainly associate effectiveness of information security measures within a risk management and cultural perspective.

There are few empirical studies of the effectiveness of organizational information security measures. A literature review shows that most of the current studies are focused on single measures, in particular policies and awareness creation, but few studies have addressed the effectiveness of procedures and tools

Several authors have studied the effectiveness of the information security policy. The effectiveness of the policy is dependent on the way the security contents are addressed in the policy document and how the content is communicated to users (Höne & Eloff, 2002). Kemp (2005) argues that a security policy is not effective unless it is supported by the management, Thomson and von Solms (2006) also add that effectiveness is created when the policy is adopted by employees in practical actions, Doherty and Fulford (2005) argue that the specific alignment of the information security policy with the strategic information system plan might be one constructive way of making the policy more relevant for managers. According to Karida et al. (2004), the organizational characteristics play an important role for the successful implementation and adoption of the security policy. The success criteria are to have a coherent organization where employees follow a code of best practice or a culture where employees participate in the security work. Wiant (2005) views the security policy as a deterrent measure, and argues that the information security policy is effective when computer abuse incidents and the seriousness of those incidents are reported.

Few authors have carried out research on the effectiveness of organizational measures such as procedures, tools and methods. Siponen (2000) and Albrechtsen (2007) show that although information security guidelines are of a prescriptive nature and imperative to the users, users often fail to apply them as intended. As a result, the guidelines are often not effective for the purpose of influencing human behaviour and attitudes.

There is some research on organizational measures aiming at improving security awareness. People are an important resource in coping with information security, as the success of an information security programme depends on the commitment from all users. If this commitment is not in place, the security mechanisms could be bypassed or diminished by employees (Ward and Smith, 2002; Schneier, 2004). Thomson and von Solms (2006) claim in an ambitious manner that to achieve effectiveness, information security should be transferred into tacit knowledge and unconscious consciousness. Security awareness programmes are one method to raise users' knowledge and commitment. Johnson (2006) argues that there are several beneficial effects of a security awareness programme: increased confidence, better protection, correctness and reliability of information, fewer internal undesired incidents, improved moral and detection capability, and improved compliance with laws and regulations.

3 Method

3.1 The survey

A web-based questionnaire was distributed by email to 658 persons responsible for information security in a target population consisting of Norwegians. The questionnaire addressed questions on whether different organizational measures were implemented or not. Some of these measures were accompanied by more detailed questions regarding how they were used. Furthermore, the respondents were asked to subjectively assess the effectiveness of different measures independent of whether the measures were implemented or not in addition to specifying what they understood by effectiveness of information security measures. Additionally, the questionnaire contained questions regarding perceived information security performance of the organization. The questionnaire was pre-tested among ten security managers and adjusted according to feedback on the questionnaire and the distribution of the answers in the pre-test. The questionnaire was constructed based on known principles in social science research literature (e.g. Ilstad et al., 1977; Ringdal, 2001). Two email reminders were sent to the respondents before access to the questionnaire was closed.

Table I shows the distribution of type and size for the respondents' organizations. The respondents are well distributed among these variables. As for their personal background, 80% of the respondents are schooled in information technology, 4 of 5 respondents are men and more than 70% have at least 5 years of work experience with information security. The respondents have different positions, roles and responsibilities in their organizations; some were general managers, while others were line managers and consultants. In this paper all respondents have been named information security managers regardless of their role and position.

Table I. Demographic data of the organizations represented in the study

Organization (N=87)	
Public agencies	32%
Power suppliers & petroleum industry	27%
Finance industry	15%
IT and telecommunication	14%
Others	12%
Size (N=87)	
1-49	30%
50-499	26%
>500	44%

The questionnaire was emailed to members of three national information security interest groups or those subject to two different regulatory authorities (the Norwegian Water Resource and Energy Directorate and the Financial Supervisory Authority of Norway). As a consequence, the respondents had either a personal motivation for information security by their membership of an interest group, and/or their organizations were subject to specific information security regulations as they operated critical information infrastructure. It can thus be assumed that the respondents were well-informed and interested in information security, and that their organizations represented businesses where information security is essential. This statement is supported by the respondents' personal background described in the paragraph above.

105 respondents answered the questionnaire, which provided a response rate of 16%. 87 of these were useful for reasonable analysis, which is a small sample with limited potential for generalizing. Kotulic and Clark (2004) experienced the same problems regarding response rate in a US study of information security management effectiveness. They received only 67 questionnaires of 1474 possible respondents. Their low response rate was followed up by a study showing that the main reasons for the non-responses to the companies' volume of survey requests were policies of not sharing information about their information security performance and a desire not to spend valuable manager time on the particular research project. These findings might explain the low response rate in the present study as well, as the objectives of the studies are related. For example, some of those who received our questionnaire replied by email that they could not answer due to the security policy of their organizations. No similar follow-up activity was performed to address the low response rate in our study, as the purpose of this paper can be approached in a satisfactory way based on the data material provided by the survey, as is argued below.

In addition to the small size, the sample is skewed. Table 2 in a later section shows how the security performance of the respondent's organizations is assessed. Just about all the respondents assess their performance to be high or average. Hence, the respondents believe that they are "the best of the class", which often is the case for voluntary self-assessments. This might partly explain our low response rate, as it can be assumed that those who have knowledge and interest in information security responded to the survey. However, the skewness and size of the sample should not be too important for the relations between implementation and effectiveness studied in the present paper. Our study does not aim at presenting a representative picture of organizational information security measures, but rather aims at exploring relations between implementation and effectiveness of measures, which should be independent of the sample size. Since it can be assumed that the respondents are competent and interested in information security, we can also assume that they give a reliable and correct assessment of the effectiveness. Hence, the quality and reliability of the study also improves, which might not have been the case for a broader sample of respondents regarding knowledge and experience.

3.2 Statistical analysis

The data material from the survey can be divided into three main groups:

- Use and implementation of different organizational measures
- Subjective evaluation of the security performance of the organization
- Subjective assessment of the effectiveness of information security measures.

The survey data were first approached by a descriptive analysis of single security measures that were implemented to get an overview of how organizational measures were used. Additionally, Chi-square tests were performed to study if there were significant differences regarding security practices among the different categories of respondents.

To reduce the complexity of the data material, factor analyses with varimax rotation.was performed in order to provide indexes. Two types of indexes were derived: implementation indexes and effectiveness indexes. The implementation indexes were constructed from binary data describing whether organizational measures were implemented or not, while the effectiveness indexes were derived from judgements of the effectiveness of measures (5-point scale). The indexes were tested for reliability by measuring Cronbach's alpha.

Furthermore, a Spearman correlation analysis was performed among the groups of security measures; first with the assessed security performance of the organization as the dependent variable, and then with the effectiveness index as the dependent variable. In order to study the relative contribution from different security measures, a linear regression analysis was performed with the assessed security performance of the organization as the dependent variable and single measures as the independent variables.

4 Assessed information security performance

The respondents were asked to assess their organizations' information security performance compared to other organizations in the same business by subjectively assessing whether their organization's security performance was better than average or worse than other organizations in the same type of business. Table II shows that nearly half of the respondents have an average performance compared to others in the business they operate in, while the other half claim to be better than the average performance in the same business. Only two per cent feel that they have a poor security performance compared to others, implying that most respondents experience the security performance in their organizations to be good enough. In subjective assessments regarding own performance, respondents are often inclined to assess themselves positively. It is often hard to admit that you are not good enough or have made mistakes.

Table II. The respondents' subjective assessment of their organizations' information security performance compared to other organizations in the same business (N=87)

Assessed security performance	Percentage
Worse than the average	3%
Average	45%
Better than the average	33%
Much better than the average	18%
Best in the business	1%

69% of the respondents are members of cross-organizational information security forums, which should make them capable of comparing themselves with other similar companies. However, Chi-square tests on assessed security performance did not show any significant differences regarding such memberships.

5 Implemented organizational information security measures

Table III provides an overview of the percentage of respondents who have implemented different organizational information security measures. The most used measures are information security policy and measures that are directly decomposed from the policy: routines for hired staff and telecommuters; non-disclosure agreements; and user guidelines.

Additionally, participation in information security interest groups is widespread, which is not surprising since a large fraction of the respondents are members of such associations.

Table III. Implementation of organizational security measures (N=87)

Organizational security measure	Respondents who have implemented measure
Security routines for hired staff	90%
Policy	84%
Non-disclosure agreement	84%
Participation in info.security interest groups	84%
User instructions/guidelines	81%
Internal audits	78%
Risk analyses	72%
Security routines for telecommuters	71%
Incident response plans	70%
User training and education	65%
Top management's engagement	61%
User participation	55%
Awareness campaigns	55%
Systems for reporting incidents/conditions	52%
External audits	48%
Asset and personnel classification	47%
Disciplinary processes	45%
Key performance indicators	16%

Chi-square tests were performed regarding the use of measures and characteristics of the organization. The tests revealed some significant differences regarding size of and type of organization:

- Respondents in the manufacturing, power supply and the petroleum industries do not use non-disclosure agreements to the same extent as respondents in other businesses. There are also fewer organizations with less than 500 employees who require their members to sign non-disclosure agreements than organizations with more than 500 employees.
- Asset classification is used less among respondents within the ICT sector than other types of organizations.
- Few of the respondents use Key Performance Indicators, but the financial business and public agencies use KPIs more than other business.
- Use of risk analysis, internal audits and external audits is significantly more widespread in the financial business than other sectors.
- Small organizations have had external audits more often than large organizations.
- Public agencies do not have plans for incident handling in place to the same extent as other businesses.

The introduction of this article classifies organizational measures into four groups: policy; procedures and control; tools and methods; and awareness creation. By performing a factor analysis with varimax rotation in combination with subjective interpretations, the measures presented in Table III were reduced to four indexes reflecting this theoretical categorization:

- *Implemented information security policy*. Single item
- *Implemented procedures and control*, consisting of four items: security routines for hired staff and telecommuters; user instructions; non-disclosure agreements and disciplinary processes.
- *Implemented tools and methods*, consisting of seven items: asset classification, risk analysis; internal and external audits, key performance indicators, systems for reporting, and incident

handling plans. The reliability of the index is below the desired level, but is nevertheless included in our analysis since it is important for the comparison between implementation and assessed effectiveness made in the final discussion.

- *Implemented awareness measures*, consisting of five items: training/education; awareness campaigns; user participation; top management's engagement; involvement of all parts of the organization in learning processes from incidents.

The indexes were created by adding the binary items (1= implemented, 0=not implemented) included in one index, and dividing them by the number of items included. Hence, the index ranged from 0 (no measures implemented at all) to 1 (all measures in the index implemented).

Table IV shows the mean score for each of the four indexes. 'Security policy' is the most implemented index along with formalized documents and control activities. 'Awareness creation' and 'tools and methods' have a considerable lower score than the two first indexes.

Table IV. Implementation indexes of security measures (N=87). Ranging from 0 (no measures implemented at all) to 1 (all measures included in the index implemented)

Indexes	Mean (SD)	Cronbach's alpha
Implemented information security policy	0.84 (0.37)	-
Implemented procedures and control	0.77 (0.27)	.713
Implemented tools and method	0.60 (0.24)	.618
Implemented awareness measures	0.59 (0.34)	.702

5.1 Discussion of implementation of measures

Written security policies are the most implemented organizational information security measure in our study. Several authors (e.g. Höne and Eloff, 2002; Doherty and Fulford, 2005; Wiant, 2005) and public standards and guidelines have emphasized the importance of the security policy. They state that the information security policy is the foundation of any administrative information security system. In addition to policies, accompanying documents such as instructions and non-disclosure agreements are used to a wide extent among the respondents.

Our findings are in line with Dhillon and Backhouse (2001), who argue that the traditional organizational view on information security has been on formalized, documented systems. Albrechtsen and Grøtan (2004) have argued that such a formalized approach is one of the contributors to a mechanical organizational view on information security.

There is however more perspectives on organizations than the structural, formalized part (Bolman and Deal, 2003; Morgan, 1998), e.g. organizational culture; human resources; decision-making processes; politics and power; and internal and external dynamics. This argument has also reached the information security domain in the last few years so that there is increasing emphasis on security culture, awareness, education and training, e.g. OECD (2002). Our findings show that such activities are not implemented to the same extent as the formalized systems. About half of the respondents say that they have educated employees or arranged awareness campaigns. This finding is supported by another survey of Norwegian companies (Hagen, 2007), which shows that educating users is less adopted compared to formal routines and preventive security technologies. There might be several reasons for the findings in the survey. One hypothesis is that awareness training is resource demanding; it must be repeated to be effective (Thomson and von Solms, 2006). It may also reduce the production capacity by removing the employees from the production line during training. Another explanation elaborated by Albrechtsen and Hovden (unpubl.) might be that those responsible for information security do not see the information security resource that users represent.

It is argued that top management's engagement is one of the most important dimensions of a loss prevention culture (Hale, 2000), but only 60% of the respondents in our survey feel that the top managers actually are engaged in the information security work in their companies. One explanation could be that the information security executive position is placed at a low level in the organizational hierarchy. Another explanation is that information security has traditionally been a technical domain, and that top management, just like most users, lack the technical knowledge and understanding of information security. They simply do not speak the same language as the IT professionals.

By a wide margin, the least used single measure is Key Performance Indicators (KPIs). Cashell et al. (2004) give a possible explanation of this finding. Organizations have strong motives for not measuring information security: fear of the impact on the financial markets, damage of reputation, risk for legal disputes afterwards, risks that hackers get information that can be used in an attack and finally that IT personnel fear losing their job. Good metrics or indicators are however important. Good metrics should measure the system resistance to attacks, the ability of the system to recognize and react to attacks, maintain services, restrict damage and recover services from attacks (Reznic, 2003). The main argument for measuring security has been that you cannot manage what you cannot measure, and that good metrics can be used to establish a bottom line for security, justify the security budget, translate technical details to a management level, improve security practice and integrate security into the business process (Netsec, 2004).

6 Relationship between implemented security measures and assessed security performance

A correlation analysis revealed that there were some significant correlations between the indexes of the implemented security measures (Section 5) and the subjectively assessed security performance of the organization (Section 4). However, the correlation coefficients were weak, all below 0.5, as shown in Table V. Despite the weak correlations, it can be argued that organizations putting more effort and investments into security also assess their performance as better compared to those who put less effort and investment into security.

Table V. Correlations between assessed security performance of the organization and indexes of implemented security measures

Indexes	Significance level	Correlation coefficients	N
Implemented information security policy	0.028	0.239	84
Implemented procedures and control	0.002	0.351	84
Implemented tools and method	0.001	0.356	83
Implemented awareness measures	0.001	0.321	74

Multiple linear regression analyses were performed to study the relative contribution from implemented measures to the assessed security performance. The analysis was based on an assumption that implemented security measures create an effective security performance of the organization. A multiple linear regression analysis with security performance of the organization as the dependent variable and the implementation indexes as the independent variables failed to produce any significant contributions. By changing the independent variables to single organizational measures the regression analysis resulted in a model with significant linear relations and explanation power R^2=0.29, see Table VI. The test revealed that the single organizational activities “Involvement of employees in the information security work”, “Performing a risk analysis more frequently than every third year” and “Having a written security policy” are independent significant contributors to how the respondents assess the security performance of their organizations. Consequently, the implementation of these three measures is regarded to be most effective for producing a high perceived level of information security. The results in Table VI show that the most important single contributor is involving the employees in information security work, followed by having a written security policy.

Table VI. A linear regression model of organizational security performance

	Unstandardized coefficients		**Standardized coefficients**		
	B	Std.error	Beta	t	Sig
Constant	1.702	0.233			0.000
Involve the employees in the information security work	0.564	0.177	0.332	7.309	0.002
Perform risk analysis more frequently than every third year	0.436	0.190	0.239	3.187	0.025
Have a written security policy	0.516	0.229	0.233	0.253	0.027

6.1 Discussion of the effectiveness of implemented measures

The three effective implemented measures identified in the regression analysis are all important principles in an administrative information security system. Security policy is the basic document for a security management system, linking the security ambitions to the business strategy and outlining e.g. the security measures and responsibilities (Höne and Eloff, 2002; Doherty and Fulford, 2005). Several other organizational and technological information security measures and activities are directly based on the policy. However, the subsequent sections of this paper show that this finding is in contrast to how the respondents assessed the effectiveness of the security policy compared with other measures.

Risk-based management is a widespread approach in all kinds of loss prevention management, including information security management (Blakely, McDermott and Geer, 2001). Within the risk management approach, a risk analysis is the basic tool to identify the threats, assess the consequences/losses and identify the relevant measures that mitigate risk. Several methods and tools for risk analysis of IT systems can be applied (Wiencke, Aven and Hagen, 2006).

The information security field has a modest focus on worker participation in public guidelines (Albrechtsen and Hovden, 2007a). However, several relevant fields of practice present arguments for worker participation, e.g. organizational development (e.g. Levin and Klev, 2001); health and safety management (e.g. Hovden et al., in press); and system development (e.g. Ehn, 1992), These arguments, which could explain the finding of worker participation as a significant contributor to good security performance, are related to democratic ideas of the possibility to influence one's own working conditions and utility-driven ideas of improved ownership and motivation among workers; improved decision-making; improved development and implementation of technological and administrative solutions and changes; and reduced level of risk. User participation in information security is thus likely to improve the usability and functionality of information security technology; improve individual awareness, ownership, motivation and acceptance of information security; improve decision-making processes; and ensure democratic rights to have influence over personal working conditions (Albrechtsen and Hovden, 2007a). There is however a difficult balance between the need for keeping security management features secret according to the need-to-know principle and the involvement of employees.

7 The effectiveness of organizational security measures

Based on the four theoretical interpretations of information security effectiveness presented in Section 2, the respondents were asked what they understood by the effectiveness of information security measures. The overall majority of the respondents (98%) defined the effectiveness of information security measures within a risk management and security culture perspective, while 61% define effectiveness from a legal compliance and deterrent perspective. Only 47% define the effectiveness from an economic perspective. This means that within our group of respondents, those responsible for IT security are more concerned with managing the business risks and serving the end-users in contrast to worrying about legal requirements and economic profit. Possible reasons for these findings are that the job description complies more with risk handling and serving users, and that economy and legal affairs are dedicated to other management positions.

Furthermore, the respondents were asked to assess the effectiveness of 20 different information security measures and activities. The assessment was made independent of whether the respondent had implemented the measures or not. Five of these were technological measures. The effectiveness was assessed on a 5-point scale from 1= no effect to 5=very good effect. To reduce the number of measures assessed, the following indexes were constructed based on factor analysis with varimax rotation and subjective comprehension:

- *Awareness measures* consisting of four items: training, awareness programmes, user participation and top management's commitment.
- *Technological measures* consisting of five items: personal passwords, redundancy of critical systems, intruder detection systems, anti-virus software and firewalls.
- *Tools and methods* consisting of the six items: incident handling, reporting, risk analysis, asset classification and audits by regulatory authorities and internal audits. The reliability of the index is somewhat low, but is nevertheless included in the comparison as it should provide sufficient reliability for meaningful comparison later sections of the paper.
- *Information security policy.* Single item.
- *Procedures and control* consisting of four items: instructions for individual behaviour, non-disclosure agreement, requirements for outsourced activities and disciplinary actions.

Table VII presents the results of the assessment. All of the indexes have a high mean value, i.e. none of the groups of organizational measures are assessed to have a poor effectiveness on the security level. Creation and maintenance of awareness is the group of measures that has the highest mean value along with technological measures. The rest of the measures have a considerable lower mean score.

Table VII. Indexes for the assessment of the information security measures, ranging from 1=no effect to 5 =very good effect

Index	Mean (SD)	Cronbach's alpha
Assessed awareness creation measures	4.18 (0.60)	.786
Assessed technological measures	4.14 (0.51)	.716
Assessed tools and methods	3.68 (0.60)	.816
Assessed information security policy	3.60 (0.82)	-
Assessed procedures and control	3.55 (0.58)	.648

Due to the design of the questionnaire, the effectiveness indexes in Table VII are not completely the same as the implemented indexes presented in Table IV. However, the main contents of the implementation indexes and the assessment indexes are basically the same. This makes it possible to perform some meaningful comparisons, presented later in the article.

Independent-sample t-tests were performed to assess whether there were differences in the assessments of measures regarding some organizational characteristics. Significant differences regarding company size were found. The t-tests indicated that respondents in large organizations (>500 employees) assessed awareness creation as significantly more effective (p<.05) than companies with less than 500 employees. On the other hand, large organizations assessed the effect of policies (p<.05) as lower than small organizations. Other tests revealed no significant differences in assessments and organizational characteristics.

7.1 Discussion of subjectively assessed effectiveness of measures

Table VII, the creation and maintenance of awareness is valued as the most effective organizational measure in addition to technological measures. There is a considerable step down to the next ones; tools and methods, procedures and control and security policy. *Why are awareness creation and technological solutions assessed to be more effective than the other measures?*

One explanation is found in how the respondents understand the notion of effectiveness. Almost all of the respondents agree that the effectiveness of a security measure is understood as 1) risk reducing and 2) developing a good security culture. There is obviously a logical link between understanding effectiveness as developing a culture and the high score of the effectiveness of awareness creation. The risk-reducing dimension of effectiveness also contributes to an explanation of the results of the subjective assessment. A security manager is capable of seeing that changes have occurred in the awareness level in the organization. It is also possible to see and even measure that technological solutions reduce the risk for virus infections and spam, for example. One can also determine the number of virus infections that have been stopped during a day, which should provide information about the risk and security.

Information security has traditionally been a technological discipline (Siponen and Oinas-Kukkonen, 2007), where security technologies form the basis of a security system. It is thus not surprising that technological measures are assessed high compared to administrative measures. Technology is also the main defensive system of an organization; it is technological solutions that detect and react to virus and spam attacks, the most frequent threats that organizations face (Hagen, 2007). Information security managers tend to understand technology as a fool-proof system protecting an organization’s resources for whatever possible acts users can do (Albrechtsen and Hovden, unpubl.), implying that the effectiveness should be good as well.

Another interpretation of the assessments in Table VII is that administrative measures and documents are taken for granted. What actually creates a high-class security performance is when organizational members and interactions among them change and comply with the security policy. Security policy, procedures and control, and tools and methods constitutes a part of formal activities that enables good security but do not provide any guaranties for security. There are two ways employees may damage the company’s information systems. Unintentionally by downloading virus-infected files via email or surfing on the web. Employees can also inflict damage to the information systems in the organization on purpose.

Keeney et al. (2005) show that the majority of such incidents were planned. The insiders leaked information about their lack of job satisfaction and often their plans before committing the crime. Increased consciousness among colleagues can improve the detection capability of the organization (Randazzo et al., 2004, Keeney et al., 2005). This view is supported by Mitropuolus et al. (2005) who argue that although system logs are useful, it is in most cases humans who are best at recognizing abnormal activities in the organization when they occur. As a result, well-trained employees may become the strongest links in terms of information security. This means that by training the employees they can be moved from a state of "unconscious incompetence" to a state of "conscious competence" in their security practices, and become part of a de facto security behaviour and culture (Thomson and von Solms, 2006). Conscious users adhering to the security behaviour described by the policy will have a positive influence on the behaviour of their colleges. Additionally, they can become a detection capability for security incidents, when or even before incidents occur.

8 The relation between implementation and assessment of the effectiveness of organizational security measures

In Figure 1, implementation of organizational measures is combined with how these measures are assessed, by plotting the implementation indexes in Table IV along the horizontal axis and the effectiveness indexes in Table VII along the vertical axis.

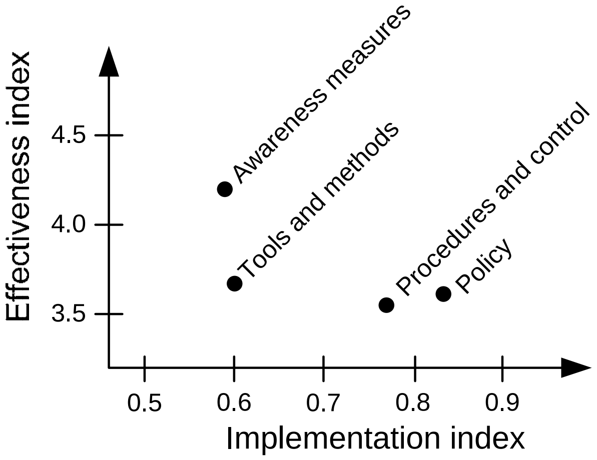

Figure 1. Implementation and assessed effectiveness

Figure 1 shows that there is a deviation between which measures the respondents used and how they assessed the effectiveness of the security measures. The group of measures assessed to be most effective on the security level is also the group that is least implemented among the respondents. Similarly, the most used measures, i.e. policies and procedures, are assessed as the least effective. *Why is there such an inverse relationship between implementation and assessed effectiveness of organizational security measures?*

The relations between the groups of organizational measures looks like a staircase metaphorically, see Figure 2. The staircase is constructed based on the degree of implementation and the subjective assessment of its effectiveness. The metaphor, which sums up the major arguments presented in the article, is helpful for discussing the inverse relationship between implementation and effectiveness of measures.

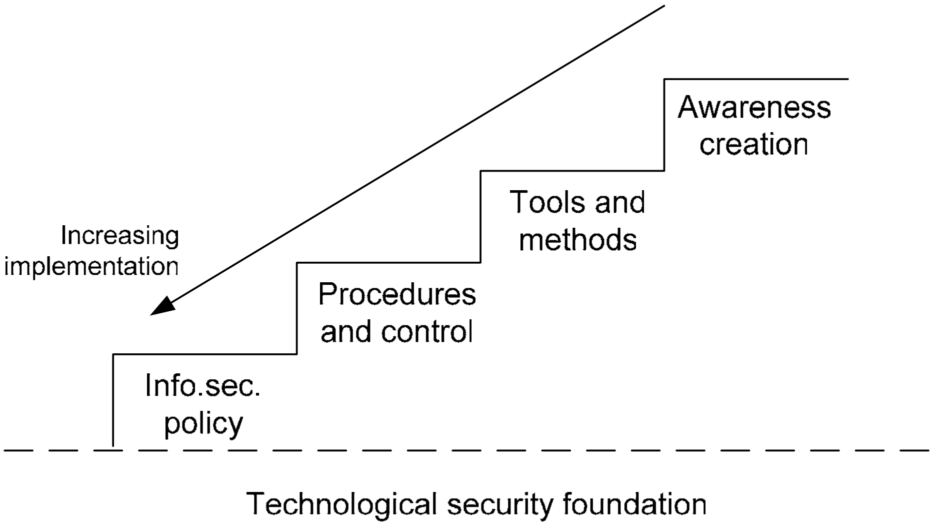

Figure 2. Organizational information security staircase. Based on empirical findings.

The staircase is built on a technological foundation that always must be in place. Without the technological security solutions there would be no need to have administrative measures either, since it is technological solutions that prevent, detect and react to unwanted incidents where technology is used in some way. This argument is supported by the high effectiveness assessment of technological solutions in this article. The present study does not ask about the implementation of technological solutions, but other studies show a high degree of implementation of basic technological security measures, e.g. The Norwegian Computer Crime Survey (2006).

Information security policy is claimed to be the baseline in every administrative security regime. The findings in the present study show that policies are used to a wide extent. Documents and control activities directly based on the security policy are also used quite extensively. These two groups of organizational measures form the two lowest steps in our staircase. Following the scores in Table VII the third step is tools and methods. And finally, the top step is awareness creation. The three first steps are assessed to have approximately the same effectiveness on the security level, while the top step is assessed to be considerably more effective.

Another explanation to the staircase is the use of resources. There is clearly an inverse relationship between implementation and the costs of the groups of measures. The most implemented measures, i.e. policies and procedures, are also the least resource-demanding measures to develop. The work requires less employee involvement compared to e.g. risk analysis where users may be represented in working groups and user training which involves all employees. Awareness creation is thus effective for security performance but at the same time may not be very cost-effective.

The implementation of organizational measures follows a logical development. A policy needs to be in place before you can generate more detailed documents with associated control and disciplinary activities. When you have these things in place you can develop plans regarding e.g. incident handling or risk analysis. The sequence of steps can also be explained in a historical perspective which shows that administrative measures have been utilized more than awareness-raising measures (Dhillon and Backhouse, 2001). During the last decade there has been an increased emphasis on humans and organizational interplay regarding information security, which implies that awareness creation can be placed at the top of the staircase.

The effectiveness of awareness creation is assessed to be higher than the rest of the organizational measures, although it is less implemented than the other measures. The staircase metaphor helps to explain this. None of the respondents state that they have poor security performance. It must thus be assumed that all the respondents' organizations have an adequate level of security, which should indicate that the implemented information security measures at these organizations, is effective. However, when the respondents are asked to assess the effectiveness of different organizational measures they assess the measures they have not implemented to be more effective than the measures already implemented. A possible interpretation of this is that the three first steps in Figure 2 are taken for granted and accepted as contributors to an adequate security level. Standing at step 3 being satisfied with the current security performance the question becomes how to get from being good to become even better. The answer is to deal with the human part of information security. Consequently, the awareness-creation measures are assessed to be very effective compared to the basic, formal security systems in the three first steps.

In that sense, there might be a fifth understanding of security effectiveness that is neither proposed in the theoretical framework nor in the questionnaire: effectiveness of a security measure improves the security level and adds something new to the current security work.
Is there a next step on the staircase? Within the field of industrial safety there has been increased focus on managing the challenge of change (Hale and Baram, 1998). This field of research and practice is based on the same basic idea as information security: loss prevention. Ideas should consequently be transferable, and inspire current information security approaches since the industrial safety discipline has more mature socio-organizational perspectives (Albrechtsen and Hovden, 2007b). Such an approach includes resilience (Hollnagel et al., 2006) and adaptation (Rasmussen, 1997) as important principles. Resilience engineering looks for ways to enhance the ability of organizations to create processes that are robust yet flexible, to revise risk models, and to use resources proactively in the face of disruptions in ongoing production and economic pressures. Organizational resilience is proactive. It looks at incidents as a result of nontrivial couplings and functional resonance; recognizes that safety emerges from everyday actions; views variability as a risk as well as a resource; and solutions are based on harnessing variability. This is in contrast to conventional risk management approaches that are mainly reactive. They look at accidents as results of a chain of events, view variability as a threat, and solutions try to constrain variability (norms, routines, and standards).

9 Conclusion

The companies participating in the study have emphasized developing and applying formal systems, like security policies, procedures and controls, while awareness activities are less applied in the organizations. This indicates a formal, mechanical view of information security management as argued by Dhillon and Backhouse (2001) and Albrechtsen and Grøtan (2004). The least implemented of the measures, awareness creation, is assessed to be the most effective group of organizational measures. Technical-administrative measures (policy; procedures; control; and administrative tools) are the most implemented measures, but are at the same time assessed to have lower effectiveness than awareness creation. There is thus an inverse relationship between the implementation of organizational information security measures and how the effectiveness of the measures is assessed. This inverse relationship is interpreted as a metaphorical staircase of four steps: 1) security policy; 2) procedures and control; 3) tools and methods and 4) awareness creation. The higher the position on the staircase, the more effective is the information security management. The steps in the staircase follow a logical order: policies must be the foundation to develop rules, guidelines and plans which must be in place to develop tools and methods. When these formal systems are implemented, one can deal with the human element of information security.

The inverse relationship between implementation and assessed effectiveness is explained by this logical relationship between the traditional approaches of the groups of measures, the required resources and employee involvement, and the interpretation of effectiveness. Information security management has traditionally emphasized formal management approaches (Dhillon and Backhouse, 2001), which explains the amount of such measures used by the respondents. These formal measures are also less resource demanding to develop compared to awareness-creation activities.

The respondents assess awareness creation to be more effective than other measures. This implies that measures that are not implemented are assessed to be more effective than implemented measures. One interpretation of this is that when the formal management system (i.e. policies, procedures and tools) is in place, these measures are taken for granted and accepted as contributors to an adequate security level. The question for a practitioner is then how to get from being good to becoming even better. The answer is to deal with the human part of information security. Consequently, the awareness-creation measures are assessed to be very effective compared to the basic, formal security systems in the three first steps. The effectiveness of information security measure can thus be understood as a measure that improves the security level and adds something new to the current security approaches, in addition to being understood as an effective reduction of risk and effective development of a security culture.

The results indicate that in order for information security measures to become effective, security should be built like a staircase of combined measures. To produce any effect, security measures are mutually dependent on each other (Sundt, 2005; Berghel, 2005). The staircase model shows that the technological security foundation must be in place. Without the technological security solutions there would be no need to have administrative measures either, since it is technological solutions that prevent, detect and react to unwanted incidents where technology is used in some way. The same arguments can be applied on administrative measures; it is the employees that give life to the administrative security routines by applying them in their day to day work.

For further research on this topic other research designs are required. There are two reasons for this. First, it proved to be difficult to get a representative sample of an adequate size. Second, to explore the results in more detail a triangulating approach is needed, which combines quantitative data with qualitative research methods. Such research designs can include in-depth case studies or interdisciplinary expert judgements.

References

Albrechtsen, E. (2007), “A qualitative study of users’ view on information security”, Computers & Security, Vol 26 No 4, pp. 276-289

Albrechtsen, E. and Grøtan, T.O. (2004), ”Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner”, in Norwegian [Old-fashioned thinking in modern organizations? On ICT-security in knowledge organizations], in Lydersen, S. (Ed.), Fra flis I fingeren til ragnarokk, Tapir Akademisk, Trondheim, pp. 335-355

Albrechtsen, E. and Hovden, J. (2007a), “User participation in information security”, in the proceedings of ESREL2007

Albrechtsen, E. and Hovden, J. (2007b), “Industrial safety management and information security management: risk characteristics and management approaches”, in the proceedings of ESREL2007

Albrechtsen, E. and Hovden, J. (unpublished), “Information security digital divide in organizations: information security managers versus users”, manuscript submitted to Computers & Security

Blakely, B.; McDermott, E. and Geer, D. (2001), “Information Security is Information Risk Management”, in Proceedings of the 2001 workshop on New security paradigms, ACM Press, New York, pp.97-104

Berghel, H. (2005), “The Two Sides of RoI: Return on Investment vs. Risk of Incarceration”, Communications of the ACM, Vol 48 No 4, pp.15-20.

Bolman, L.G. and Deal, T.E. (2003), Reframing organizations: artistry, choice, and leadership, Jossey-Bass, San Francisco, California

BSI, Bundesamt für Sicherheit in der Informationstechnik (2004), IT Security Guidelines. IT Baseline Protection in brief.

Cashell, B.; Jackson, W.; Jickling, M. and Webl, B. (2004), The economic impact of cyberattacks, Congressional Research Service Report for Congress Available at http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

Dhillon, G. and Backhose, J. (2001), “Current directions in IS security research: towards socio-organizational perspectives”, Information Systems Journal, Vol 11 No 2, pp.127-153.

Doherty, N.F. and Fulford, H. (2006), “Aligning the information security policy with the strategic information systems plan” Computers & Security, Vol 25 No 1, pp. 55-63

Ehn, P. (1992), “Scandinavian Design: On participation and Skill”. In Adler P.S. and Winograd, T.A. (Eds.), Usability – turning technologies into tools. Oxford University Press, New York.

Gordon, L.A. and Loeb, M.P. (2002), “The economics of information security investment”, ACM Transactions on Information and System Security (TISSEC), Vol 5 No 4, pp. 438-457.

Hagen, J.M, (2007), Evaluating applied information security measures. An analysis of the data from the Norwegian Computer Crime Survey 2006, FFI/REPORT-2007/02558, pp 35-48.

Hale, A.R. (2000), “Culture’s confusion”, Safety Science. Vol 34 No 1-3, pp.1-14

Hale, A.R. and Baram, M.S. (Eds.) (1998), Safety management: the challenge of change. Pergamon, Oxford

Hubbard, W. (2002), Methods and Techniques of Implementing a Security Awareness Program, SANS Institute white paper

Hollnagel, E.; Woods, D.D.; and Leveson, N. (2006), Resilience engineering: concepts and precepts Ashgate, Aldershot, UK.

Hovden, J.; Lie, T.; Karlsen, J.E. and Alteren, B. (in press), "A study of occupational health and safety management in the Norwegian oil and gas industry", Available online at Safety Science

Höne K. and. Eloff, J.H.P. (2002), "Information security policy – what do international security standards say?" Computers & Security, Vol 21 No 5, pp. 402–409.

Ilstad, S.; Paasche, T. and Hovden, J. (1977), Survey-metoden. In Norwegian [Survey methods]. Tapir, Trondheim, Norway.

ISO/IEC 27001:2005, Information technology – Security Techniques – information security management systems.

Johnson, E. (2006), "Awareness Training, Security awareness: switch to a better programme", Network Security, Vol 2006 No 2, pp. 15-18

Kemp, M (2005), "Beyond trust: security policies and defence in depth", Network Security, Vol 2005 no 8, pp 14-16.

Karyda, M.; Kiountouzis, E. and Kokolakis, S. (2005), "Information systems security policies: a contextual perspective", Computers & Security, Vol 24 No 3, pp. 246-260.

Keeney, M.; Kowalski, E, Capelli, D., Moore, A., Shimeall, T. and Rogers, S. (2005), Insider Threat study: Computer System Sabotage in Critical Infrastructure Sectors, Carnegie Mellon, Software Engineering Institute

Kotulic, A.G. and Clark, J.G (2004), "Why there aren't more information security research studies", Information & Management, Vol 41 No 5, pp.597-607

Levin, M. and Klev R. (2002), Forandring som praksis. Læring og utvikling i organisasjoner. In Norwegian. [Change as practice. Learning and development in organizations], Fagbokforlaget, Bergen, Norway.

Lobree, B. (2002), "Impact of Legislation on Information Security Management", Security Management Practices, November/December 2002, pp. 41-48

Mitropoulos, S., Patsos, D. and Douligeris, C. (2006, "On incident Handling and Response: A State-of-the-art approach", Computers & Security Vol 25, No 5, pp. 351-370

Morgan, G. (1998), Images of organizations, Sage Publications, London

Netsec (2004) Using metrics to improve security, Security brief, Using metrics to improve security, available at: http://www1.netsec.net/content/securitybrief/archive/2004-09_Metrics.pdf

OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

Randazzo, M.R, Keeney, M.; Kowalski, E, Capelli, D. and Moore, A. (2004), Insider Threat Study: Illicit Cyber Activity in the Banking and Finance sector, Carnegie Mellon, Software Engineering Institute

Rasmussen, J. (1997), “Risk Management in a Dynamic Society”, Safety Science, Vol 27 No 2/3, pp. 183-213.

Reznec, L. (2003), “Which Models Should be Applied to Measure Computer Security and Information Assurance” in the proceedings of the IEEE International Conference on Fuzzy.

Ringdal, K. (2001), Enhet og mangfold: samfunnsvitenskaplig forskning og kvantitativ metode. In Norwegian [Unity and diversity: social science and quantitative methods], Fagbokforlaget, Bergen, Norway.

Schneier, B. (2000), Secrets & lies. Digital security in a Networked World, Wiley Publishing Inc, Indianapolis, Indiana.

Siponen, M.T (2000), “A conceptual foundation for organizational information security awareness”, Information Management and Computer security, Vol 8 No 1, pp. 31-41.

Siponen, M.T. and Oinas-Kukkonen, H. (2007), “A review of Information Security Issues and Respective Research Contributions”, The Data base for Advances in Information Systems, Vol 38 No. 1, pp.60-81.

Sundt, C. (2006),, “Information security and the law”, Information Security Technical Report, Vol 11 No 1, pp. 2-9.

Thomson, K-L. and von Solms R. (2006) “Towards an Information Security Competence Maturity Model”, Computer Fraud & Security, Vol 2006 No 5, pp 11-15.

Von Solms, B. (2000), “Information Security – The Third Wave?”, Computers & Security, Vol 19 No 7, pp. 615–620.

Von Solms, B. (2001), “Information security – A multidimensional Discipline”, Computers & Security, Vol 20 No 6, pp. 501-508.

Von Solms, B. (2006), “Information Security – The Fourth Wave”, Computers & Security, Vol 25 No 3, pp. 165-168.

Voss, B.D. (2001), “The Ultimate Defense of Depth: Security Awareness in Your Company” SANS Institute white paper.

Ward, P. and Smith, C.L. (2002), “The Development of Access Control Policies for Information Technology Systems”, Computer & Security, Vol 21 No 4, pp. 365-371

Wiant, T.L. (2005), “Information security policy’s impact on reporting security incidents”, Computers & Security, Vol 24 No 6, pp. 448-459.

Wiencke, H. S., Aven T. and Hagen J. (2006), “A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT” In the proceedings of ESREL2006.

PAPER V:

Albrechtsen, E. and Hovden, J. (2007).

“User participation in information security”.

In Aven, T and Vinnem, J.E. (eds.) *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007 (Esrel 2007)*. London, UK: Taylor & Francis, 2551-58

PAPER VI:

Albrechtsen, E. and Hovden, J. (2007).

"Industrial safety management and information security management: risk characteristics and management approaches".

In Aven, T and Vinnem, J.E. (eds.) *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference 2007 (Esrel 2007)*. London, UK: Taylor & Francis, 2333-40