available at www.sciencedirect.com

ScienceDirect

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

ELSEVIER

Computers & Security

The information security digital divide between information security managers and users

Eirik Albrechtsen[a,b,*], Jan Hovden[a]

[a]Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, N-7491 Trondheim, Norway
[b]Department of Safety Research, SINTEF Technology and Society, N-7465 Trondheim, Norway

ARTICLE INFO

Article history:
Received 3 May 2007
Received in revised form
1 December 2008
Accepted 5 January 2009

Keywords:
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 indicate that a digital divide exists between these groups in terms of their views on and experience of information security practices. Information security professionals mainly regard users as an information security threat, whereas users believe themselves that they are an untapped resource for security work. The limited interaction between users and information security managers results in a lack of understanding for the other's point of view. These divergent views on and interpretations of information security mean that managers tend to base their practical method on unrealistic assumptions, resulting in management approaches that are poorly aligned with the dynamics of the users' working day.

© 2009 Elsevier Ltd. All rights reserved.

1. Introduction

Traditionally, ‘‘digital divide’’ has been understood as a socio-economic perspective, dealing with access to information communication technology, particularly the Internet, and the ability to use this technology to participate fully 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, all of which contribute to a gap in the use of information systems.

From a socio-technical perspective, a digital divide in information security can be viewed as consisting of the existing differences with regard to information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance between individuals. A digital divide in information security within organisations is thus not only a question of access to information systems that have implemented adequate

[*] *Corresponding author*. Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, SINTEF Teknologi og Samfunn, N-7491 Trondheim, Norway.

E-mail address: eirik.albrechtsen@iot.ntnu.no (E. Albrechtsen).

0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.01.003

information security technology; it is also a question of considerable differences in skills, knowledge, responsibilities, perceptions and interpersonal relationships between the various members of the organisation. From this perspective, several digital divides may exist within information security, related to, for example, age, gender, IT experience, education and occupation. In this article we will discuss the digital divide in information security in terms of any existing differences in information security views and expectations between information security professionals and users.

An organisation consists of its members and their interactions. Each member has his own role to play, and his own sphere of responsibility, which contribute towards realising the organisation's goals. Preserving information security is among the goals of any organisation, and every member has a responsibility for ensuring such security in practice. Whereas information security managers have a particular responsibility because of their expert knowledge, for other users at all levels of the organisation the responsibility for acting in a manner that is safe and secure for the organisation comes on top of the other demands they are faced with in their everyday work. An information security digital divide between users and information security managers with regard to skills, knowledge and responsibilities is therefore to be expected.

This article aims at discussing an information security digital divide between information security managers and users by exploring *similarities and differences between their views on and experience of information security practices in organisations*. This purpose is approached by looking at how managers and users view their own role compared to how they experience the role of the other, and at how they experience administrative security measures. Furthermore, given that there are differences, how are these differences reflected in the actors' judgement of risk? A two-fold approach is adopted. First, 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 performed by the authors (Albrechtsen, 2007) and other relevant research results on the human aspects of information security. Second, quantitative data from two different surveys of, respectively, users' and information security managers' judgement of IT-related risks are compared.

Although some studies have addressed information security user performance and information security management (for an overview, see Stanton et al., 2005), few attempts have been made at research which seeks to combine and compare the role and views of users and information security managers. A study in the health domain by Adams and Blandford (2005) showed contrasting perspectives among security professionals and users on the role of users and on security practices. Kuttschreuter and Gutteling (2004) showed that experts and lay people had different perceptions of the risk associated with the Y2K problem.

Our study mainly considers the administrative information security system and the role of users and managers. Technological issues are dealt with only in a brief manner. Focusing on non-technological issues of information security makes comparisons easier as well as richer, as it is likely that many users have no specific insight into the technological aspects of information security.

The next section presents the data sources and the analytical approach used to study possible information security divides. The results, as well as a discussion of each of the aims of the article described above, are presented in the subsequent sections. On the basis of qualitative data, Sections 3–5 present and compare the ways in which security managers and users experience the role of security managers, the user aspect of information security, and user-directed measures. Subsequently, survey data are used to show how users and security managers assess IT-related risks, and some interpretations of these results are discussed. In Section 7, these results and discussions are summarised, and the indication is indeed that a digital divide in information security exists between users and managers. The article concludes with a statement that the social digital divide between users and managers creates unrealistic assumptions about sharp-end activities among information security managers, who base their practical management approach upon these assumptions.

2. Data and analysis

2.1. *Analytical approach*

Data from four independent empirical sources form the basis for this article:

- *An interview study of managers:* a qualitative interview study of information security managers in large Norwegian organisations.
- *An interview study of users:* a qualitative interview study of users in a Norwegian bank and a Norwegian IT-company.
- *A survey of managers:* a survey among information security managers in several Norwegian organisations.
- *A survey of users:* a survey among users working in a Norwegian public agency

These sets of data were collected for purposes that differed slightly from the objective of this study. In this respect, the present approach is a secondary analysis of available data. With exception of the manager interview study, the studies are all published elsewhere: Albrechtsen (2007, 2018) and Hagen et al. (2008). However, the research designs of the four studies were all created in a way that made the present comparative study possible, since the two interview studies covered the same topics, and the two surveys included a set of questions relevant to the present comparative study.

Fig. 1 shows the analytical design of the article. The views held by users and information security managers with regard to different information security activities and characteristics are subjected to a comparative study in order to explore whether indications may be found of a digital divide in relation to information security in organisations. The figure also shows how the different sets of data described in the bulleted list above are used in comparative analyses of different information security topics.

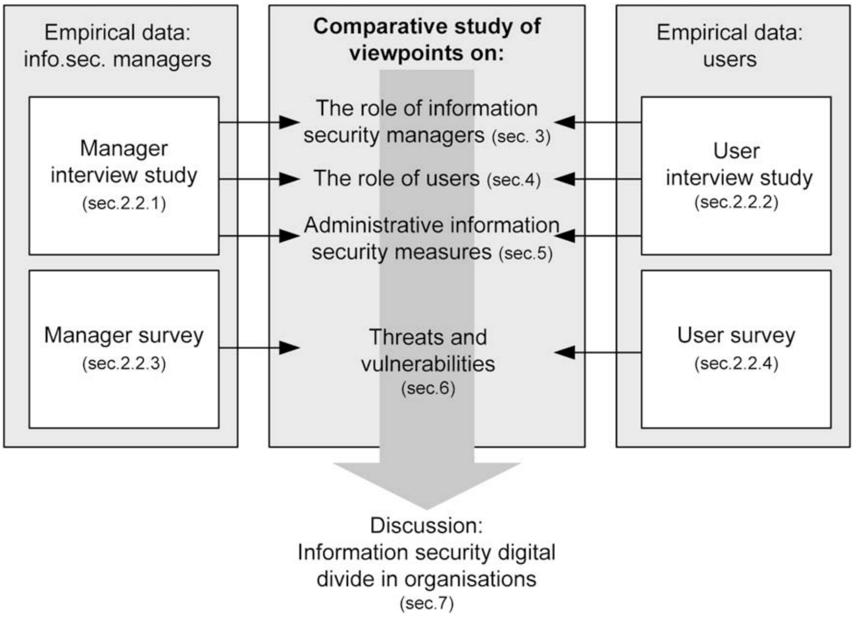
Empirical data: info.sec. managers
Manager interview study (sec.2.2.1)
Manager survey (sec.2.2.3)
Comparative study of viewpoints on:
The role of information security managers (sec. 3)
The role of users (sec.4)
Administrative information security measures (sec.5)
Threats and vulnerabilities (sec.6)
Empirical data: users
User interview study (sec.2.2.2)
User survey (sec.2.2.4)
Discussion: Information security digital divide in organisations (sec.7)

Fig. 1 – Analytical approach. Comparative study based on four sets of empirical data.

Our analytical approach is an explorative study of different empirical sources. As indicated in the introduction, the relationship between users and information security managers is a largely unexplored topic in the existing research. Furthermore, few studies have focused on how users and information security managers experience information security management practices. Thus, our approach aims at theory building rather than at testing the validity of existing information security theory. Such an exploratory approach requires that different issues related to the research questions be examined by means of close study of various sources of empirical data on the views held by both information managers and users.

2.1.1. *Qualitative analyses*

The interview studies of the managers and the users were both analysed in similar ways according to principles of qualitative research. Qualitative data analysis implies data reduction, data display and drawing of conclusions in an interwoven manner before, during and after data collection (Miles and Huberman, 1994). Transcribed interviews were coded in HyperRESEARCH (a software tool for analysis of qualitative data). The codes were then categorised according to the aims of the interview studies and analysed by switching between the whole picture and the details (Leiulfrud and Hvinden, 1996) by 1) testing ideas registered 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. This qualitative research approach does not aim at generalised findings, but at providing insight into social processes (Strauss and Corbin, 1998; Thagaard, 2003). The interview is a useful method for this purpose as it makes possible for the informants to describe and explain both broadly and in an in-depth manner processes experienced daily (Kvale, 1996).

In Sections 3–5 of this article we compare the findings of the manager interview study with findings from the user interview study and other studies on users' views on information security (e.g. Adams and Sasse, 1999; Besnard and Arief, 2004). Both interview studies were designed to cover the same topics, that is the role and function of users, the role and function of information security managers, daily information security practices, and information security measures.

2.1.2. *Quantitative analyses*

Data from two different surveys were used to reveal how users and information security professionals assess risks. The two surveys were developed in order to provide answers to questions other than those in this study but since they also included questions on risk judgement, they could be utilized in the present study. The quantitative data analysed in the present article were not included in the other publications based on the two surveys. Both survey questionnaires contained the same set of questions regarding judgement of information security threats and vulnerabilities. The respondents were asked to rate 14 information security threats and vulnerabilities applying to the day-to-day operation of their organisation on a 5-point scale from 1 = no risk to 5 = very high risk. The set was created on the basis of monthly reports on threats and vulnerabilities published by the Norwegian Centre of Information Security (NorSIS). The listed 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.

The aim of the quantitative analysis was to reveal any existing significant differences between users and information security managers in their assessment of risks. For this purpose, we used independent-samples *t*-tests to test the null hypothesis ''there is no difference in risk judgement between the two groups''. The objective of *t*-tests is to determine whether two samples have significantly different mean scores on a given variable (Ringdal, 2001).

2.1.3. Strengths and weaknesses of the analytical approach

The four sets of empirical data come from different organisations and sectors. The interview study of managers covers informants from large Norwegian organisations, both in the public and in the private sectors. The interview study of users was performed at a bank and at an IT-company, both of which were similar in size to the organisations employing the interviewed managers. Respondents to the survey of managers work for different Norwegian organisations in different sectors, while the user survey was performed at a public agency. Consequently, the findings discussed in the present article are derived from different organisational contexts, implying that our analysis contains certain weaknesses: survey material on users represents only public services, whereas the managers were found in both the public and the private sectors. Moreover, there are differences in age, gender, knowledge and skills between the two groups (users and managers).

Obviously, the asymmetry between the survey respondents and the interviewees used in the comparative analysis in terms of organisational contexts and individual attributes will influence the way each individual experiences information security practices, thus potentially impacting on our results. This might make it difficult to draw strict conclusions from the comparisons. The problem of organisational asymmetry could have been solved by using only the responses from managers employed in the public sector. Similarly, the interviews with security managers could have been carried out in banks and IT-companies. However, this would not have solved the problem of different organisational contexts, as actors in the public sector, banks and IT-companies also operate in different organisational contexts (e.g. size, tasks, traditions, public expectations): The within variance of the business domains may be as high as the between variances. A better research design is hence needed for hypothesis testing and generalisations; for the explorative purpose of this study, however, the data sets are sufficient.

The four studies were combined in two ways, as described by Hammersley (1996): complementarity (each method produces different, complementary data about the same phenomenon) and triangulation (using data produced by different methods to validate each other). These combined approaches strengthen the validity of the study, as some of the findings complement and validate each other (Silverman, 2006). The role of users in information security and information security management of employees represents an unexplored area of research (Dhillon and Backhouse, 2001; Schultz, 2005; Siponen and Oinas-Kukkonen, 2007; Albrechtsen, 2008). The explorative research design with an inductive strategy used in this article is well suited to the initial phases of this research, as it generates understandings of information security processes at individual and organisational levels as well as providing descriptions of information security management in several organisations.

2.2. Empirical sources

2.2.1. Interview study of information security managers

The qualitative study of information security managers (for the sake of simplicity called the manager interview study in the rest of this article) consisted of 11 in-depth interviews with information security managers in large Norwegian organisations. The objective was to discover how these managers interpreted the management of the human aspect of information security. Topics such as their views on how different measures were evaluated by users as well as by themselves, and on the functioning of the day-to-day information security work, were discussed during interviews lasting from 60 to 90 min. The manager informants worked in four different fields of business: five of them were employed by public agencies, two of them worked in oil and gas operators, two in manufacturing organisations and two in logistics firms. These were all distributed organisations with 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, such as developing documented systems, arranging awareness campaigns and supporting decision-makers at the line management level.

2.2.2. Interview study of users

The interview study of employees, which is fully described and discussed in Albrechtsen (2007), was performed among the staff of the costumer counselling department of a bank and of the service centre of an IT-company. For both of these organisations, information security is essential for business. 18 interviews were conducted – nine at each of the studied organisations – each with a duration of about 1 h each. The main objective of the service centre is to support different computer-based business systems and other business areas in the organisation. A typical task procedure is to receive an error notification about a customer's address, find the reason for this error, and fix the problem in a database. The operators at the service centre have access only to data, not to the database designs. There were 15 employees in the department; only two of them were men. 9 female users were interviewed. They were between 30 and 60 years old. All of them had been employed by the organisation for a long time, and few of them had any education above college level. None of them had any management responsibility. The interviewed users at the bank do consultation work in relation to private and corporate costumers of the bank. This service includes all types of bank consultations by phone or e-mail, as well as face-to-face meetings regarding, e.g. insurance and loans. At the bank, 8 men and 1 woman were interviewed. They were between 30 and 60 years old, and most of them had worked within the financial sector 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 these systems being in place.

The study (Albrechtsen, 2007) indicated inadequate information security awareness among the interviewees in both organisations: each individual performed very few information security actions; they were unfamiliar with possible threats; they were unaware of the possible consequences of security breaches; they were largely unable to identify problems or potentials for improvement of their own working conditions; and some of the users failed to recognise the value of their information security role in the total security work of the organisation.

2.2.3. *Information security manager survey*

The manager survey used in the present article was distributed to information security managers in Norwegian organisations for the purpose of studying the effectiveness of organisational information security measures; see Hagen et al. (2008). In addition to questions concerning the use and evaluation of the effectiveness of organisational security measures, the questionnaire contained 14 questions addressing the respondents' perception of the risk posed by different threats and vulnerabilities, which are used in the present article. Table 1 shows the organisations to which the managers belonged, and Table 2 shows the demographic characteristics of the respondents.

A web-based questionnaire was distributed by e-mail to 658 individuals who were either members of three national information security interest groups or security managers in organisations subject to two regulatory authorities. As a consequence, the respondents either had a personal motivation for information security through their membership of an interest group, and/or their organisation was subject to specific information security regulations because it operated critical information infrastructure. It can thus be assumed that the respondents were well-informed about and interested in information security, and that their organisations represented businesses where information security is essential. Only 87 respondents returned the survey questionnaire, which is a small sample with limited potential for generalizing. Kotulic and Clark (2004) experienced the same response rate problem in a US study of information security management effectiveness, as they received only 67 completed questionnaires out of a total of 1474 possible respondents. They followed up the small response rate with a study which uncovered that the main reasons for the non-responses were related to the volume of survey requests received by the organisations 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.

Although the manager survey forms a poor basis for a generalisation of the findings, the study provides good understanding of information security manager's interpretation of the risk of threats and vulnerabilities, which suits the explorative strategy of the present article. Furthermore, nearly all the respondents assessed their organisation's security performance as high or average (Hagen et al., 2008). Hence, the respondents believe that they are ''top of the class''. It can thus be claimed that only those who have knowledge about and take an interest in information security responded to the survey. As a result, we may assume that the manager respondents had expert knowledge on information security threats and vulnerabilities, thus strengthening the quality of their risk evaluation.

Table 1 – Manager survey, demographic data for the managers' organisations (*N* = 87).

Organisations	
Public agencies	32.2%
Power suppliers and 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%

Table 2 – Demographic data for the respondents of the user survey and the manager survey.

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

2.2.4. *User survey*

The objective of the user survey was mainly to evaluate the effects of a participative training programme on users' awareness and behaviour, as presented in Albrechtsen and Hovden (submitted for publication). The data used in the present article are the results of the last questionnaire in a time-series analysis. The user survey study covered an intervention group participating in the training programme and a control group not included in this programme. In addition to questions concerning individual attitudes and behaviour, the questionnaire contained 14 questions addressing the respondent's perception of the risk posed by different threats and vulnerabilities. The answers to these questions are used in the present article. The questions were similar to the questions related to risk perception in the manager survey.

Table 2 shows demographic data on the users responding to the survey. The users belonged to a Norwegian public agency which has 500 employees and is responsible for several national computerised registers used for support and services to businesses and public administration. Independent-sample *t*-tests revealed no significant differences in risk perception between the intervention and control groups. The user group is therefore treated as a homogeneous population ($N = 157$) in the present study.

3. 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 do not 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.

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
Gatherings (large plenary sessions, small information meetings)	●	●	●		●				●		●	6
Education and competitions (interactive training, training new employees, interactive competitions)	●	●			●	●			●			5
Personal presence (informal conversations, observation)	●	●									●	3
User participation (active involvement of employees in info. sec. activities)			●									1

> 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 from that 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 (see Section 5, 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 indicates a discrepancy between the reasoning behind the most commonly used measures and the way in which information security managers perceived themselves.

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. The latter was also the technical-operative unit for information security. According to the interviewed managers, 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 intelligible manner to all members of the organisation.

The visibility of managers was also considered an important factor by the interviewed users. Some of the users said during their interview 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 they considered it important to know who worked with information security since this made it easier to report problems and ask questions. Claims were also made among the users that seeing a manager is important for raising awareness:

> "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. Having information meetings is much better than receiving documents and e-mail messages." *User, IT-company.*

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 how they experienced user performance. They provided two main reasons for this superficial interpretation of users. First, the managers were employed by large organisations with a large number of users. This meant that there were great variations among the users in terms of information security knowledge and skills, personal characteristics, and tasks, which made it difficult to give specific details. Second, several of the interviewed managers felt that they lacked the resources to systematically review the activities of different groups of users or to meet 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 of 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 ought to know something about them – but I have to admit that I don't.'' *Information security manager, public agency IV*.

The managers' claim that it was difficult to be specific about the security performance of users might have weakened the validity of our qualitative study, but the interviews corrected the picture: it transpired a good way into the interview with each of the managers that the manager did after all have 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 are able to express in words. Using interviews as a research tool makes it possible to enter more deeply into the informants' everyday work (Kvale, 1996), and thus to bring out their tacit knowledge.

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

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 with the managers, during which they tended to emphasise negative assessments 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. The negative side of the Janus face of users was above all related to day-to-day operation, i.e. users caused problems because they lacked the motivation, knowledge and skills necessary for safe and secure behaviour.

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

> ''For one thing users do not want to have passwords. Moreover, 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 may have considerable consequences. According to some of the managers, however, users do not realise this: they often see their own work in isolation and are unaware of the implications of their use of IT systems. Users are often familiar with what security measures they should be taking, but they often fail to take them, and they generally

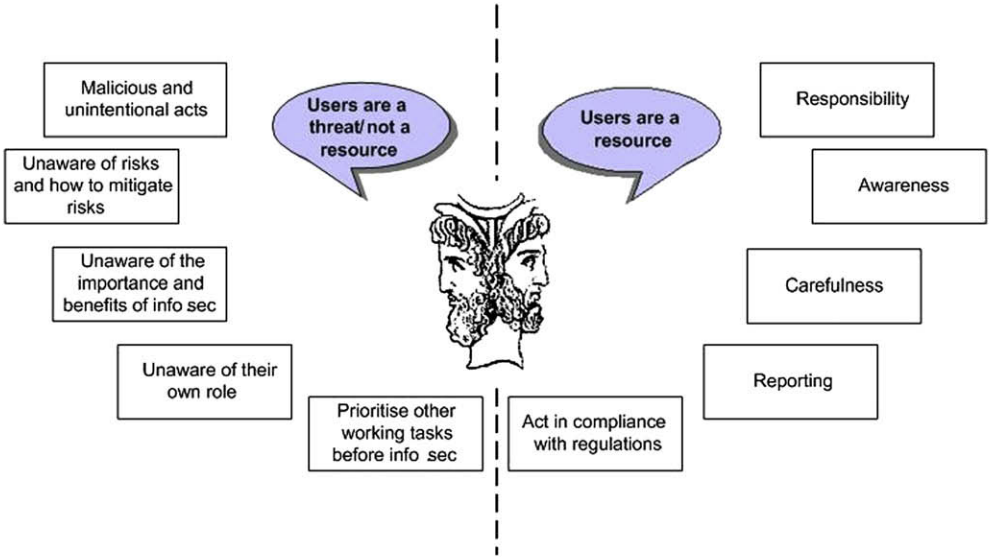
Malicious and unintentional acts
Unaware of risks and how to mitigate risks
Unaware of the importance and benefits of info sec
Unaware of their own role
Prioritise other working tasks before info sec
Users are a threat/not a resource
Users are a resource
Responsibility
Awareness
Carefulness
Reporting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

Fig. 2 – The Janus face of the users' role in information security.

tend to give lower priority to or to be indifferent to security work. Thus 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 they tend to prioritise other work tasks over information security. The managers also claimed that the users were unaware of the risks and of how to mitigate them. Some interviewed managers stated that users often assume that responsibility for information security rests with the technology and the information security managers.

Most of the interviewed managers said that users give information security only second or third priority in their everyday work, and they explained this by referring to users as being unfamiliar with thinking beyond their designated tasks. Some of the managers claimed that the financial situation of the organisation prevented users from performing any tasks outside their main area of work.

4.2. *The managers' experience compared to the users' own views on their role in information security*

The interview study of users showed that users believe that they have an important role to play in information security; but it also showed that they do not have the knowledge to act in a safe and secure manner (Albrechtsen, 2007). The interviewed managers in the present study shared this view of users as an important resource, but they nonetheless emphasised the negative sides of the users' role. Both of the interviewed groups agreed that users in general do not have the knowledge or skills needed for safe and secure behaviour, a shortcoming that both groups believed to be 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 concentrated mainly on the non-resource side of the Janus face of users. The users, on the other hand, focused on how they might be 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 interview study of users uncovered that most users agree that information security is important to the organisation, especially with regard to the organisation's public image.

However, one problem experienced by interviewed users and managers alike was that users trade off information security against efficiency and functionality. This finding is supported by information security research (Adams and Sasse, 1999; Besnard and Arief, 2004; Post and Kagan, 2007). According to the insight provided by the interview studies of users and managers this trade-off is caused by the following factors: efficiency demands; emphasis on minimum-effort work; and poor quality of information security training and education resulting in insufficient skills and knowledge. The challenge of loss prevention trade-off is also well known from the safety research domain. Reason (1997) and Rasmussen (1997) describe safety trade-offs at an organisational level, where safety margins are eroded due to an emphasis on efficiency and a desire for minimum-effort work-loads rather than safety. At an individual level, Battmann and Klumb (1993) argue that a major share of the violations of safety regulations can be attributed to individuals who optimize their behaviour by minimizing the spending and maximising the gaining of resources. Their argument is based on behavioural economics, which explains that individual behaviour is created within a frame of internal (e.g. skills and knowledge) and external factors (e.g. administrative systems, colleagues, technology) (Navon and Gopher, 1979). The information security trade-offs identified in the interview studies of managers and users are also explained by internal factors (low information security awareness among users; lack of information security skills and knowledge), and external factors (inadequate training programmes; efficiency demands).

5. Managing the human aspect 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' organisations.

Technological tools that seek to control and monitor user behaviour were used by all of the interviewed managers' organisations. Technology is used mainly because it prevents many of the users' intentional as well as unintentional actions, since it limits what users are and are not allowed to do, e.g. through access control. Technology 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 fail sometimes, but not the way that humans do. You don't have to keep the technology informed, which is a clear advantage. Technology definitely reduces risk more than the training of any user can achieve." *Information security manager, Public agency I*

All the interviewed managers said that they operated by the security policy, the non-disclosure agreement, the guidelines and/or instructions. These documented systems were intended to describe what users were expected to do or not to do. In the managers' experience it was important to notify users of the existence of a system of requirements regarding user behaviour. However, they believed that few users actually 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 that four reasons account 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 of these documents because it is poorly presented; 3) the documentation is not readily available or it is 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 of the involved organisations. The intranet was particularly widely used for spreading information, but several of the organisations also used other means, such as screen savers, e-mail messages and leaflets. Information on security was thus made available to users, but this still meant that users had to read the information and make an effort in order to obtain the knowledge it contained. According to the interviewed managers users often lacked the motivation and awareness to make this effort. Furthermore, users are also bombarded with information from other parts of the organisation, making it even harder for information security messages to reach the targeted group. As users tend to be uninterested and unmotivated in information security, this kind of information is filtered out in the total information overload. However, although the interviewed managers had no confidence in the effect of these formal one-way information measures, they develop and implement them extensively. This paradox was explained by the fact that the measures are simple and thus do not require many resources. Moreover, some of the managers believed that even if the information reached only 10 per cent of the users, this was still better than it reaching none at all.

According to the interviewed managers, the most efficient method for influencing user awareness and behaviour is interaction in some form or other between users and security managers, e.g. in small face-to-face information meetings. Table 3 shows, however, that this type of measure is among the least frequently used approaches, mainly because of the cost it involves. Some of the managers found that simply being visibly present, e.g. by spending time in public spaces in the organisation and conducting informal conversations, was very effective.

> “Meeting people is different from sending electronic information. This approach is an important one, not least in terms of making myself and my role visible… There are always a lot of questions about information security when I meet people. This indicates that they are interested and see the benefits of information security when they are approached in this manner. I have found both formal and informal contact with employees to be 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 of the interviewed security managers. Only one of these managers had actually made users 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:

> “The users, the top management and I have all had several aha experiences 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. No one knows these conditions better than the users … Creating discussion is the most important aspect. If I participate in the processes myself, I get a valuable impression of the information security reality of the organisation.” *Information security manager, Public agency III*

There was an inverse relation between the managers' evaluation of the effectiveness of measures and their actual choice of measures: The measures in Table 3 considered to be most effective were the least commonly used ones, while the most widely used measures were regarded as the least effective approaches. The degree of user involvement was related to the degree of effect on individual security awareness. The managers seemed to go through a number of stages with regard to what measures they employed, from documents at one end of the scale, over formal information and human interaction, to user participation at the other. The experienced security manager who had used a participative approach had thus not always approached users in this way, and described the development of his information security approach to users in the following way:

> “When I started my job as a security manager I looked upon 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 was a matter of top-down information, and wasn't followed up over time. I arranged information meetings with one-way communication, where I told people how they should act. I experienced 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*

The following patterns for how users experienced administrative information security measures emerged from the interview study of users (Albrechtsen, 2007):

- 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 contents or availability of their organisation's documentation on expected behaviour.
- The IT-company had organised several formal awareness campaigns using one-way communication for several years before the study. Almost all the interviewed employees at this organisation 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 organisations 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 distribution of written rules and guidelines. Adams and Blandford (2005) have shown through qualitative studies in hospitals that all parties involved gain from this interactive approach in terms of involvement and openness.

The users' views on information security measures were similar to those held by the information security managers. The explanation 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 level of information security 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. Users were not aware, however, of the resources required by a participatory approach.

6. Risk judgement

This section presents the results of the judgements of risk posed by a set of information security threats/vulnerabilities presented to 151 users and 87 information security managers. Table 2 in Section 2 shows the demographic characteristics of the respondents to the manager and user survey, respectively. Chi-square tests revealed significant gender and age differences between users and managers. These differences may have influenced the results of the risk perception comparisons, but no definite conclusion can be drawn about this since the groups also differed with regard to other characteristics such as occupation and knowledge about information security. Since it is outside the scope of the research questions, multivariate analyses with risk judgement as the dependent variable and demographic data as independent variables were not performed.

6.1. Results

The respondents assessed 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*. Fig. 3 shows the mean value for each threat/vulnerability for each group. Independent-sample t-tests were performed in order to identify significant differences in the mean values of the respondents' assessment of risks.

There were no significant differences between users and managers in their perception of half of the threats/vulnerabilities listed. These included technical items such as software vulnerabilities and virus infections, as well as treatment of sensitive information.

Seven mean values were significantly different: The security managers evaluated the risk level for four threats/vulnerabilities to be lower than did the users. These four were incautious use of the Internet ($p < 0.10$), spam mail ($p < 0.05$), use of the organisation's IT resources for illegal purposes ($p < 0.025$), and hacking ($p < 0.05$). 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. On the other hand, security managers ranked the risk level for three of the listed threats as significantly higher than did users. These were IT-related human error ($p < 0.05$); user carelessness, e.g. leaving the computer unlocked ($p < 0.025$); and social engineering attempts, i.e. attempts to manipulate or deceive employees into committing security breaches ($p < 0.025$). A common feature of these three vulnerabilities is that they are all related to users' lack of skills and knowledge.

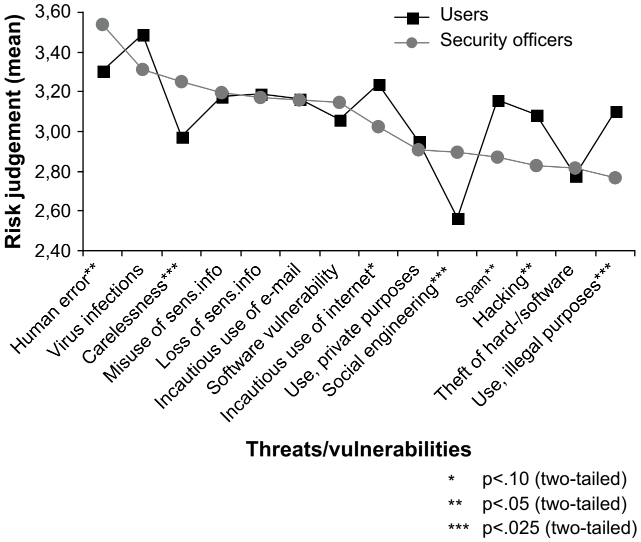

Fig. 3 – Mean values for judgements of IT-related risks by users (*n* = 151) and information security professionals (*n* = 87). Range from 1 = no risk to 5 = very high risk.

The security managers considered users to be a greater problem, i.e. a threat, to information security than did the users themselves. With regard to the highest and lowest ranked risks in both groups, security managers ranked IT-related human error as the highest risk factor, whereas users ranked social engineering attempts as by far the lowest risk factor.

The data on risk judgements presented in Fig. 3 are measured at a single point in time. As a result, the findings of our study do not consider the possible variation of risk judgement. Rather than studying the volatility of risk judgement in a time-series analysis, we made a temperature measurement at a single point in time. There is an inherent variability in human, social and technological performance (Hollnagel, 2006). One explanation of individual variability is that perception of risk has a strong impact on people's attitudes and behaviour (Wilde, 1982; Howarth, 1987). Wilde's (1982) theory of risk homeostasis proves this by explaining that people adjust their behaviour in order to balance individually perceived risk with individual target level of risk (acceptance criteria). Both the target level of risk and the perceived risk will vary according to dynamic stressors such as technological development; public opinion; events triggering attention; and changes in political and organisational contexts. Measuring risk judgement at a single point of time thus only provides a snapshot of a dynamic picture. A longitudinal study could thus make possible a more reliable comparison of experts and users. However, despite the fact that the data are taken from a single point in time we consider the results and their interpretations as valid for the purpose of the study and not particularly vulnerable to the volatility of risk perception: First, because the study does not focus on the exact scores on the questions but on comparison between the two groups. Relative scores are more reliable than absolute scores on the items. Second, because the questions asked were so generic and fundamental in their character that it is not reasonable to believe that they are significantly influenced by any short term volatility of risk perception. Furthermore, the theory of risk homeostasis is particularly interesting for explaining individual behaviour and in relation to the choice of countermeasures. Studying the dynamics of information security risk judgement is thus an interesting topic for future research.

6.2. *Discussion of risk judgements*

There is a shortage of risk perception and risk judgement studies in the field of information security. One exception is a study by Kuttschreuter and Gutteling (2004) on the Year 2000 bug problem. The study showed that users perceived the likelihood that the millennium problem would have negative consequences as greater, and worried more about it, than did experts. The opposing interpretations of risk between lay people and experts are, however, a much debated topics in general risk research (e.g. Shrader-Frechette, 1991; Slovic, 2000; Jaeger et al., 2001; Sjöberg, 2002), albeit 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 such 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) identify 18 characteristics of risk that influence people's risk perception, which they classify into three main groups: dread, familiarity and number of people exposed.

There has been a debate about which of these three components is ranked highest by different groups (Rundmo and Moen, 2006), and there are different theories in the literature concerning the factors behind the differing risk perception among experts and lay people. Slovic (2000) argues that experts differ from non-experts in terms of 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 perception between users and experts diverge in both directions, but also that some risks are perceived in a similar way. This seems to support Sjöberg's (2002) argument that the factors explaining experts' risk perception 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 demonstrated differences in risk evaluation.

Information security managers evaluate risks relating to user behaviour as being significantly higher than do users. 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 the largest number of incidents experienced by most of the respondents by far. This could mean that security managers tend to emphasise the probability dimension when evaluating risk. Drottz Sjöberg (1991) has also shown that experts tend to stress probability when asked about risk evaluation, while lay people tend to stress consequences. The risk judgement material and the qualitative data presented in prior sections in the article confirm that security managers consider users a major threat to security, while users do not; they evaluate the consequences of their behaviour as less serious than do the experts, 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 under assessment, thus creating an inverse relationship between risk and benefit evaluations. The managers' judgement of risk concerning user behaviour can be related to Slovic's argument. Elsewhere in the article we have shown that managers tend to focus on users as a problem in relation to information security. Hence, the managers have a low level of confidence in the security benefits to be gained from user behaviour, which according to Slovic creates an inverse relationship of low benefit and high risk evaluation.

The significant differences in risk evaluation presented in Fig. 3 show that users evaluate situations that disturb their work, such as spam mail and incautious use of the Internet and equipment, as posing a higher risk than do the experts. This may indicate that users are more self-centred in their evaluations and associate risk with the immediate consequences for themselves if something goes wrong.

Users also evaluate hacking as a significantly higher risk than do the experts. This is probably due to the facts that security managers are aware that defences against hacking are in place in the organisation's technological configurations, and that they have access to the statistics on avoided attacks. Users, on the other hand, do not possess this information and may be influenced for example by media reports of successful hacking attacks on Internet banks and such. This argument is supported by our risk evaluation figures for virus infections, which is another topic receiving extensive media coverage. Again, information security managers have access to statistics showing the number of prevented virus infections in the organisation, whereas users do not possess such information. In addition, most anti-virus organisations post up-to-date statistics on virus threats on their web pages, which may also influence the experts' risk evaluations, since it helps make managers aware of the large number of prevented virus attempts. Again, this shows that experts tend to use probability rather than consequences as a basis for evaluating risk, given their knowledge that most organisations today have up-to-date anti-virus software that will seldom allow virus infections to take place. Although users do not possess this knowledge, they still evaluate risk from viruses as the highest of the 14 listed threats and vulnerabilities. Again, the explanation may be found in the extensive media coverage of the virus threat.

7. Information security digital divide within organisations

The empirical findings reveal differences between security managers and users with respect to their experiences and views on information security, indicating the existence of an information security digital divide within the studied organisations:

- Both the interviews and the risk evaluations showed that managers tend to focus 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. Thus, information security managers concentrate mainly on the threat side of the Janus face of users, while users themselves focus on the other, resource side of their role.
- Security professionals and users have different opinions on the human part of information security given that users experience information security as important to the organisation and its reputation, while professionals feel that users are unaware of the importance of information security.
- Paradoxically, while 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. This indicates that there is a gap between their professional knowledge and their real-world practice.
- The studies revealed that there was little interaction between users and information security managers. As a result of the relative lack of contact, the users regarded the security managers as remote, invisible and secretive. In spite of this, however, they continued to leave the responsibility for information security up to the managers. Both groups considered interaction the most efficient tool for influencing user behaviour and awareness.
- Users and information security managers had different priorities regarding information security. The managers were under the impression that the users gave lower priority to information security than to other work tasks, which is supported by the user interview study and literature (Reason, 1997; Adams and Sasse, 1999; Besnard and Arief, 2004). In contrast, information security was the main work responsibility of the security managers.
- There is no mutual trust between users and information security managers. Whereas 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, however. They agree on the effectiveness of certain information security activities aimed at users, and neither group had much confidence on the impact 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 rationalities*

Fig. 4 shows the levels of authority of information security professionals and users in relation to information security tasks. These 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 might 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.

The information security professionals have a high degree of specialisation, and they have access to expert knowledge, time and resources for collecting and processing information, as well as sophisticated tools and methods for information processing. Consequently, they have the time and space to optimize planned information security activities. On the other hand, given they are at the blunt end of operations 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 very little about the users' situation and that they had only limited 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, such as instructions for safe and secure behaviour; and through formal one-way communication, such as e-mail messages.

In addition to showing the roles of users and information security professionals, Fig. 4 also shows the role of line managers and IT managers in this context. IT and line managers have been given very little attention in the present article, although these managers play 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 decisions are made by line and IT managers, often on the basis of the expert evaluations made by the professionals. The decision-making situations of these 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 do not necessarily represent the best option. Kørte et al. (2002) have shown that decisions made at the management level based on results from risk analyses

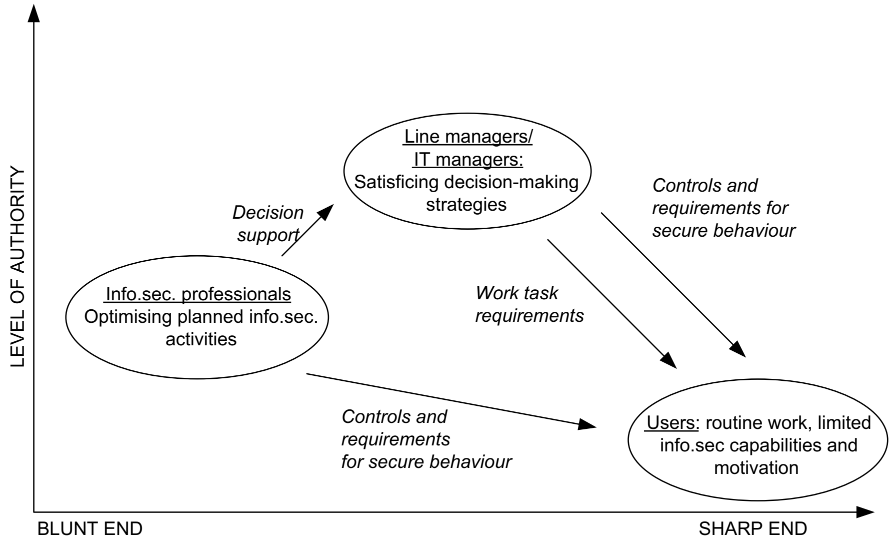
LEVEL OF AUTHORITY
Line managers/ IT managers: Satisficing decision-making strategies
Decision support
Controls and requirements for secure behaviour
Info.sec. professionals Optimising planned info.sec. activities
Work task requirements
Controls and requirements for secure behaviour
Users: routine work,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

Fig. 4 – Work situations in operative information security work. Based on Rosness (2001).

made by experts at the blunt end tend to be satisficing decisions.

The low priority given to information security by users is the result of a range of different management decisions influencing the users' total work situation. Users at the sharp end are the recipients of outputs from decisions concerning information security and other work tasks made by both security professionals and other managers. One output of management decisions takes the form of information security measures that directly influence the working day of users at the sharp end, such as 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 (2007), and Post and Kagan (2007) have shown that users consider other work demands as more important than information security tasks in the day-to-day operation of the organisation.

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. In the interviews, users and managers alike stated that documents and formal information had little effect on security awareness and behaviour. This can be explained partly by the unrealistic expectations of those developing the measures and by 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 for formal information to have any effect, it must actually be read by the users. Users at the sharp end, however, are likely to have most of their working time occupied by other work-related tasks. Security information is only one of many different types of information users have to process. Users at the sharp end thus have limited motivation and capability for information security processing.

Technological measures frame and control what users may and may not do, whereas 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 taking it 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 conflicts both with the normal working day of users and with the characteristics of modern organisations. Schön (1991) has argued that a technical rationality cannot provide an adequate description of 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 take into account human resources and values, unlike the information security measures considered effective by our managers, such as face-to-face information and user participation.

As shown by the vertical axis of Fig. 4, information security activities are also closely related to power and authority. 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 the passive recipients of information on already decided measures. There are no discourse-based power mechanisms that might form identity and allow change at an individual and organisational level. This interpretation is supported by Bachrach and Baratz' second face of power argument (Clegg, 1989), which claims that latent conflicts over information security remain invisible 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 access to instruments, techniques and procedures which attempt 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 described in Dahl's (1963) view of power: A has power over B to the extent that 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 hold 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 different rationalities. 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 geared towards achieving the organisation's goals of profit and productivity. However, users do have a responsibility for maintaining information security since this is also one of the organisation's goals.

The information security digital divide within organisations discussed in this article is not in itself a threat to the functionality of information security management. However, the differences in approach, experience, understandings 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 wish to thank all those who participated in the empirical studies for sharing their experience of information security. Eirik Albrechtsen's PhD project has been financed by TrygVesta insurance company.

REFERENCES

Adams A, Blandford 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):41–6.

Albrechtsen E. A qualitative study of users' view on information security. Computers & Security 2007;26(4):276–89.

Albrechtsen E. Friend or foe? Information security management of employees. PhD Thesis no. 2008:101, Norwegian University of Science and Technology; 2008. p. 101.

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

Battmann W, Klumb P. Behavioural economics and compliance with safety regulations. Safety Science 1993;16(1):35–46.

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

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. In: Neckerman Kathryn, editor. Digital inequality: from unequal access to differentiated use in social inequality. New York: Russell Sage Foundation; 2004. p. 355–400.

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

Drottz Sjöberg BM. Non-experts definitions of risk and risk perception, RHIZIKON: risk research reports no.3. Stockholm: Centre for Risk Research; 1991.

Hagen J, Albrechtsen E, Hovden J. Use and effectiveness of organizational information security practices. Information Management & Computer Security 2008;16(4):377–97.

Hammersley M. The relationship between qualitative and quantitative research: paradigm loyalty versus methodological eclecticism. In: Richardson JTE, editor. Handbook of qualitative research methods for psychology and the social sciences. Leicester: The British Psychological Society; 1996.

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.

Hollnagel E. Resillience – the challenge of the unstable. In: Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering. Concepts and precepts. Aldershot: Ashgate; 2006.

Howarth CI. Perceived risk and behavioural feedback: strategies for reducing accidents and increasing efficiency. Work & Stress 1987;1(1):61–5.

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):507–35.

Kotulic AG, Clark JG. Why there aren't more information security research studies. Information and Management 2004;41(5):597–607.

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.

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

Leiulfrud H, Hvinden B. Analyse av kvalitative data: Fikserbilde eller puslespill?. [Qualitative data analysis: puzzle picture or jigsaw puzzle?]. In Norwegian. In: Holter H, Kalleberg R, editors. 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.

Navon D, Gopher D. On the economy of the human-processing system. Psychological Review 1979;86(3):214–55.

Partridge H. Establishing the human dimension of the digital divide. In: Quigley E, editor. Information security and ethics: social and organizational issues. Hersey, US: RM Press; 2005. p. 23–47.

Post GV, Kagan A. Evaluating information security tradeoffs: restricting access can interfere with user tasks. Computers & Security 2007;26(3):229–37.

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

Reason J. Managing the risks of organizational accidents. Aldershot: Ashgate; 1997.

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

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. SINTEF report no. STF38 A04403; 2004.

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):623–40.

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

Schön DA. The reflective practitioner: how professionals think in action. New York: Basic Books; 1991.

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

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

Siponen MT, Oinas-Kukkonen H. A review of information security issues and respective research contributions. Database for Advances in Information Systems 2007;38(1):60–81.

Sjöberg L. The allegedly simple structure of experts' risk perception: an urban legend in risk research. Science, Technology & Human Values 2002;27(4):443–59.

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, editor. The perception of risk. London: Earthscan Publications Ltd; 2000. p. 137–53.

Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. Computers & 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. [Introduction to qualitative methods]. In Norwegian. Bergen, Norway: Fagbokforlaget; 2003.

Warschauer M. Reconceptualizing the digital divide. First Monday 2002;7(7).

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

Eirik Albrechtsen obtained his PhD at the Department of Industrial Economics and Technology Management at the Norwegian University of Science and Technology in 2008. His current research interests include human and organisational aspects of information security and strategies for safety and security management. He is currently a researcher at SINTEF Technology and Society and is also employed as an assistant professor at the Norwegian University of Science and Technology.

Jan Hovden is a professor in safety management at the Department of Industrial Economics and Technology Management at the Norwegian University of Science and Technology. His fields of interest are: safety and security management in industrial organisations; vulnerabilities of infrastructures and dynamic complex socio-technical systems; and social safety. He has produced several publications within different types of loss prevention disciplines and sectors. He has been a member of editorial boards of international journals and a great number of scientific committees. He also was a member of the Government's commission on the vulnerability and emergency preparedness of the Norwegian society.