COMPUTERS & SECURITY 29 (2010) 432–445

available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study

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 19 June 2009
Received in revised form
19 November 2009
Accepted 10 December 2009

Keywords:
Information security
Awareness
Behaviour
Participation
Intervention study
Training

ABSTRACT

The paper discusses and evaluates the effects of an information security awareness programme. The programme emphasised employee participation, dialogue and collective reflection in groups. The intervention consisted of small-sized workshops aimed at improving information security awareness and behaviour. An experimental research design consisting of one survey before and two after the intervention was used to evaluate whether the intended changes occurred. Statistical analyses revealed that the intervention was powerful enough to significantly change a broad range of awareness and behaviour indicators among the intervention participants. In the control group, awareness and behaviour remained by and large unchanged during the period of the study. Unlike the approach taken by the intervention studied in this paper, mainstream information security awareness measures are typically top-down, and seek to bring about changes at the individual level by means of an expert-based approach directed at a large population, e.g. through formal presentations, e-mail messages, leaflets and posters. This study demonstrates that local employee participation, collective reflection and group processes produce changes in short-term information security awareness and behaviour.

1. Introduction

Awareness and behaviour among all kinds of users are important parts of the information security performance of an organisation. Adequate information security training is thus required in order to create and improve user awareness and behaviour. This paper discusses and evaluates the effects of a training programme aimed at improving users' information security awareness and behaviour by involving them directly.

Several single or combined measures might be taken in order to improve users' information security performance (Hubbard, 2002; Voss, 2001), ranging from the distribution of messages via, e.g. pamphlets, e-mails, intranet pages, screen savers, posters, mouse pads, and pens to games, formal presentations, lunch meetings, and training courses. Common for most of these measures is one-way communication directed at a large population from authorities to single individuals by use of expert knowledge. On the other hand, several organisational researchers argue that bringing in local

* *Corresponding author*. Department of Industrial Economics and Technology Management, Norwegian University of Science and Technology, N-7491 Trondheim, Norway.
E-mail address: eirik.albrechtsen@sintef.no (E. Albrechtsen).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.12.005

knowledge through processes that involve employees is both necessary and efficient in order to attain all kinds of organisational change (Ehn, 1992; Greenberg, 1975; Greenwood and Levin, 1998; Levin and Klev, 2002). This argument is also the theoretical foundation for the intervention study presented in this paper, which emphasises the importance of employee participation, plenary reflections and group for improving employees' information security awareness and behaviour.

Fig. 1 shows a simple conceptual model of the intervention study, adapted from Kristensen (2005) and adjusted for the current study. To the left is the theoretical model of the intervention, which shows that the intervention is expected to improve information security awareness and behaviour among the intervention participants (indicated by the vertical arrow). The main part of the intended intervention was a small-sized 2-h workshop. The workshop participants conducted most of the discussions among themselves, which created the possibility for each participant to reflect over their working situation and information security on their own terms. Inviting employees to actively share their experiences and thoughts on information security as well as listen to colleagues' and security officers' knowledge in plenary reflections and in small groups was expected to result in changes of both awareness and behaviour.

The two boxes to the right represent the actual course of events, which should hypothetically reflect the theoretical model. The vertical and horizontal relationships in the model indicate two research questions:

- Was the intervention carried out as intended?
- Did the intervention lead to the intended changes in information security awareness and behaviour?

These research questions are followed by a question addressing the causes of the modifications – or lack of such – of information security abilities:

- Why did the intervention lead to changes – or lack of such – of awareness and behaviour?

The two boxes in the middle of the model represent the empirical research aimed at measuring the intervention and its effects in valid ways, thus answering the research questions formulated in the above. Two approaches were utilized for this purpose: statistical analysis three surveys – one before and two after the intervention; and qualitative analysis of the data from the intervention processes.

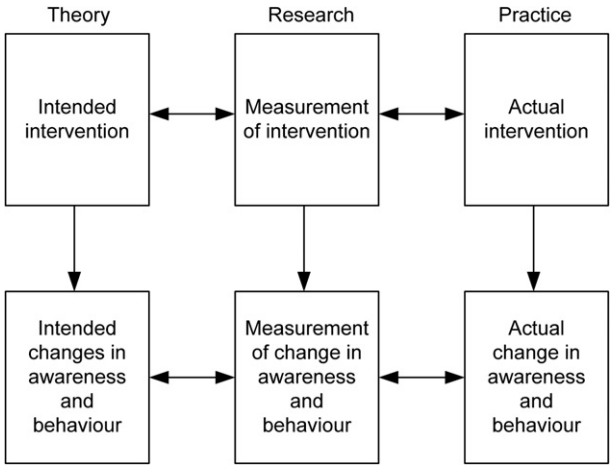

Fig. 1 – Conceptual model of the intervention study.

2. The intervention project: information security workshops

The intervention programme took place at a Norwegian public administration agency, the Brønnøysund Register Centre. The Brønnøysund Register Centre is responsible for several different national computerised registers providing support and services for businesses and public administrations. It is thus vital that stored information is easily available and correct when needed, and presented in proper form. Consequently, information security is essential to the core operations of the register centre.

For the Brønnøysund Register Centre the objective of the intervention was to improve information security attitudes among the employees, and change work behaviour relevant to information security for the better. Workshops with some 15 participants each constituted the main part of the intervention. In addition, certain measures directed at all the members of the organisation were also implemented. A news message regarding the planned information security workshops was published on the company's intranet, together with a message emphasising that everyone must keep their ID-card visible. Additionally, an information security handbook was published on the intranet.

2.1. *Theoretical framework*

Two fixed frames were established for the workshops in the development of the intervention: a set of information security subjects to be covered, and a theoretical framework regarding the processes in the meetings. Through worker participation, collective reflections, group-work, and experience transfer at an organisational level the intervention project aimed at changing individual security performance. Individual change is important since it is individuals who perform organisational activities. However, an organisation is a collective institution of interaction and coordination (Weick, 1996). Consequently, common insight into information security structures and procedures is fundamentally important for coordinated information security interaction in an organisation. Group-based sharing of experiences and knowledge between employees and information security professionals is important for the information security work, since it is likely to created common insight among employees. For this intervention project, sharing experiences and knowledge between members of the organisation is facilitated by participation, collective dialogues and considerations, and group-work processes.

The effects of employee participation on organisational development and change are known within several research traditions, but this knowledge is not reflected in mainstream standards and guidelines for information security (Albrechtsen and Hovden, 2007). Participation is likely to create

advantageous information security conditions, such as improved ownership and motivation among workers (Greenberg, 1975); improved quality of technological solutions (Adler and Winograd, 1992; Ehn, 1992); and reduced levels of risk (Elden, 1983; Shrader-Frechette, 1991). Moreover, it will satisfy the democratic rights of workers to influence their own working conditions (Elden, 1983; Greenberg, 1975). Worker participation and collective reflection are claimed to be the two foundation pillars for the success of all kinds of organisational learning, change and development (Levin and Klev, 2002). Collective reflection can be made possible for example by having plenary discussions and avoiding one-way communication and lecturing during training sessions, thus aiming at dialogue rather than instructions. The collective reflections produce a mutual understanding of routines in organisational work, which is fundamentally important for the interaction in an organisation. Interaction in groups facilitates participation and collective thinking. Furthermore, groups represent a good tool for experience and knowledge transferral among both employees and managers (Levin and Rolfsen, 2004).

2.2. *The contents and processes of a workshop*

The intervention study includes six workshops, involving a total of some 100 employees (15–20 participants per workshop). These workshops took place in April 2006. Later, the rest of the organisation participated in 33 additional workshops, but these are not included in the current evaluation. Fig. 2 illustrates the contents and processes of a single workshop.

The session started with a clear statement that there would be no one-way communication from the security officers. Rather, it was emphasised that the meeting was a forum for discussion, and that the participants were supposed to do most of the talking. The participants were encouraged to contribute with their thoughts about information security and to talk among each other in order to create reflection. After the brief introduction, a short animated cartoon was shown, functioning as a simple introduction to the field of information security and the role of individuals in security work.

Next, the first plenary discussion was launched. The security officers presented a simple question: 'Why do we need information security? The discussions related to this question led to the statement that information security is important for the Brønnøysund Register Centre as it is supposed to supply information to the public in a stable manner 24 h a day, 7 days a week. Additionally, the discussions emphasised that each user has an important role to play in the information security work.

After this, the group-work was introduced. The participants were divided into seven groups or pairs of 2–3 persons sitting next to each other. Seven different scenarios were used for igniting discussions, i.e. one scenario per group. The scenarios were as follows:

- You've been out for lunch. A stranger says he has forgotten his entrance card, and asks you to let him in. What do you do?
- You work in a landscaped office and must leave your desk for a short while. What do you do?
- You're having a day off. Someone at work phones you and asks for your password in order to access an important e-mail you have received. What do you do?
- You're about to log on to a computer when you observe that someone else is already logged on to that computer. What do you do?
- On the company's public file folder, you get access to a document containing sensitive personal information about colleagues. What do you do?

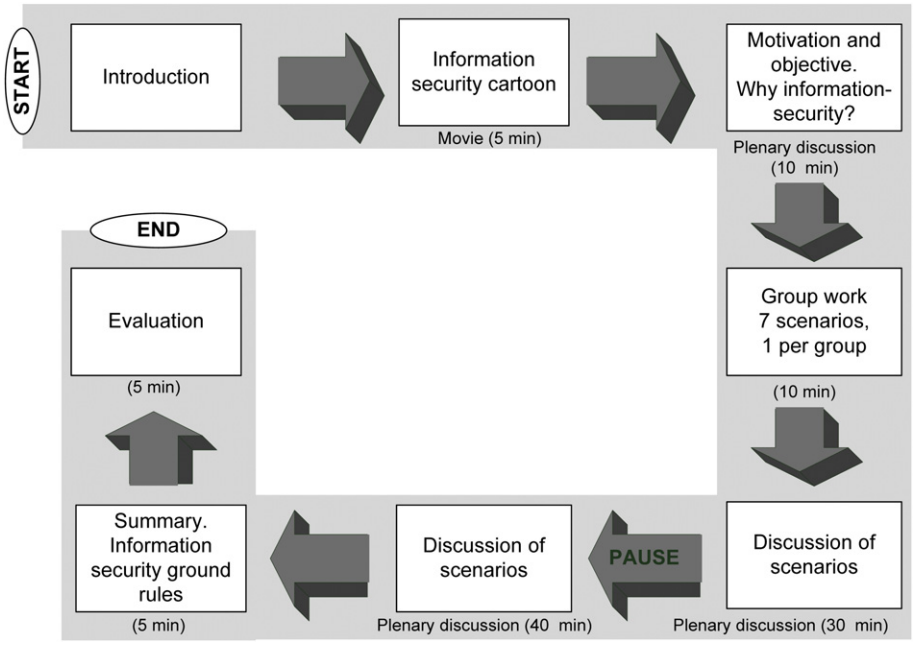

Fig. 2 – Content and processes of an information security workshop.

- You're checking your private hotmail and find that you have received an e-mail from an unknown sender. What do you do?
- There is a fire outside your office. What do you do?

After the group discussions were finished, each scenario was discussed in plenary. Each scenario was discussed following the same interwoven steps. The discussion started by a group presenting their response to the scenario they had worked with. Then the rest of the participants were invited to comment on the group's answer. The security officers did not get involved in the ensuing plenary discussion unless necessary, i.e. unless questions were addressed to the officers; the focus had strayed too far from the defined topic; or the discussion was about to end. As the discussion seemed to be coming to a close, the security officers briefly presented their view on the scenario. This presentation was often followed up by questions or comments from the participants.

This approach ensured that individual experiences were shared among the participants. For example, one participant would say: ''I would never lock my computer when leaving my desk. I can't see any reason for doing that''. This statement was then followed up by a colleague agreeing. Then a third colleague would question this, wondering why they do not lock their computers given that they have lots of sensitive information stored in their systems. In this way individual tacit knowledge was shared among a group of employees.

As the penultimate point on the agenda, the security officers summarized the workshop by presenting a set of 10 information security rules. The participants were given a laminated, pocket-format leaflet containing these rules, along with the suggestion that they put this up beside their computer screen. Finally, the last 5 min were used for evaluation of the workshop.

3. Method

In our own evaluation, we used two main approaches: a quantitative survey; and a qualitative approach which combined interviews, group conversations and observation of the intervention. The quantitative approach uncovers whether the intervention had any effect on awareness and behaviour, whereas the qualitative approach provides us with an understanding of how that effect was brought about by the intervention. The design and analysis of the current intervention study draws on methodological experiences from occupational health and safety intervention studies [e.g. (Goldenhar and Schulte, 1994; Kristensen, 2005; Robson et al., 2001)], i.e. ''studies in which the effects of planned activities at the worksites with the aim of improving the working conditions and/or the health of the workers are being evaluated with research methods'' (Kristensen, 2005:205). Occupational health and safety intervention can in a broad sense be considered as prevention-oriented interventions (Goldenhar and Schulte, 1994); consequently, evaluation strategies utilized in these intervention studies are useful for designing and performing the evaluation of the effects of the current information security study as well.

3.1. *Quantitative evaluation*

3.1.1. *Design and data collection procedure*

An experimental design was used for measuring individual awareness and behaviour before and after the intervention. Fig. 3 shows the design of the study. The study population of 197 employees was randomized into an intervention group participating in the workshops, and a control group not participating in the workshops.

An initial survey (t_1) was performed 1 month before the intervention took place. An invitation to fill in a web-based questionnaire containing questions on information security awareness and behaviour was sent by e-mail to the study population. The questionnaire consisted of different statements on information security topics, which the respondent had to agree or disagree on based on a 5-point Likert scale. Regarding behaviour, there were questions on how often the respondents performed different information security actions, e.g. 'how often do you lock your computer when absent from it'. The participants responded to the behaviour questions on a 5-point Likert scale ranging from never to always.

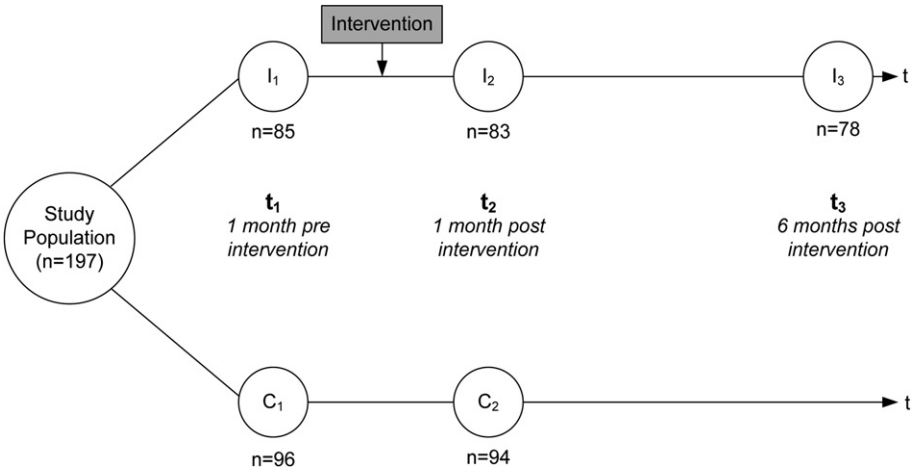

Fig. 3 – Model of multiple time-series research design with an intervention group and a control group.

The second survey (t_2) took place one month after the workshops were arranged. In order to evaluate the stability of the awareness and behaviour produced by the intervention, a third survey (t_3) was performed half a year after the intervention. For each survey, both groups received the same questionnaires. The questions used in the first survey were also used in the second and third surveys. In addition, the second and third surveys included questions about changes in behaviour and attitudes during the last months. In the second survey, the members of the intervention group were asked to assess the intervention and the impact of the intervention on their attitudes and behaviour. For these additional questions, closed questions was used, plus some open-ended questions regarding how participants had experienced the workshops and how the workshops could improve.

The third survey was also sent out to the control group. However, during the months which had passed since the second survey, an unknown number of the members of the control group had participated in workshops. Hence, some of the members of the control group were influenced by the intervention at t_3. Since it was not possible to divide the control group between those who had participated in workshops and those who had not participated, the data for the control group at t_3 had to be discarded.

3.1.2. Indexes

Based on factor analyses and on theoretical comprehension of which variables belong together, the following indexes were constructed for the analysis of the intervention outcomes. The indexes cover a broad range of aspects of information security awareness and behaviour.

The variables/items included in the awareness indexes were statements in the questionnaire, which the respondents had to agree or disagree on based on a 5-point Likert scale, ranging from 'strongly disagree' to 'strongly agree'. Each item used in the indexes is thus a statement. The following indexes on attitudes towards different information security topics were constructed for the study:

1. *Responsibility:* Perceived responsibility for information security compared with other work responsibilities. Consists of five items (I have a responsibility to create and maintain a satisfactory level of information security at the company; I have a personal responsibility to prevent that my use of IT-systems create virus infections; I believe that user friendly systems are more important than secure systems; Maintaining information security is equally important to efficient work; One must always comply with information security requirements irrespective of the working situation). Cronbach's $\alpha = .760$ (Cronbach's α for the intervention group, data from all three surveys)
2. *Motivation:* Willingness to contribute to the information security work. Consists of three items (Writing passwords down on a note is OK; There is no need to lock my computer when I leave it for a short period of time; It is no wonder that people write down their passwords since they are difficult to remember). Cronbach's $\alpha = .703$.
3. *Information security vs functionality:* Information security perceived as not being an obstacle and not only being a technological challenge. Consists of three items (I think information security is bothersome for my working situation; A lot of information security requirements cannot be met if I'm going to work efficient; Managing information security is first and foremost a technical challenge). Cronbach's $\alpha = .708$.
4. *Importance of specific information security measures*. Consists of six items (Safe use of e-mail is important; Keeping passwords secret is important; Anti-virus tools are important; Locking the computer when absent from it is important; Cautious use of the internet is important; Non-disclosure agreement is important). Cronbach's $\alpha = .770$.
5. *Importance of generic security and safety measures*. Consists of five items (Reporting incidents is important; Keeping ID-cards visible is important; Following ethical guidelines is important; Occupational accident prevention is important; Fire protection is important). Cronbach's $\alpha = .749$.

Due to poor correlation with other items, the following single items are also used as indexes, as they are interesting subjects with regard to the objective of the intervention.

6. *Reporting:* Willingness to report observed or suspected information security incidents (If I observe or suspect an information security incident, I will report this to the management)
7. *Perceived skills and knowledge:* Perceived information security skills and knowledge with regard to the individual working situation. (I have the necessary information skills and knowledge to handle information security in my working situation)

The questionnaire included eight questions about the frequency with which the respondent performed different information security tasks, such as keeping her password secret. The items invited responses on a 5-point scale (from always to seldom). Some of the items had a skewed distribution. Since it would be difficult to get significant changes for these items, they were left out of the analysis. It was only possible to perform useful pre-post analysis of four of the behaviour items. These four items produced poor reliability in all possible combinations of four, three and two. Consequently, the analysis of behaviour items consists of four single items:

8. *Locking the computer*
9. *Carrying ID-cards*
10. *Checking unfamiliar persons without ID-cards*
11. *Manual virus-check*

All indexes for the intervention group were satisfactory, i.e. Cronbach's $\alpha > .70$. For the control group, the reliability was less stable, as the indexes 'Responsibility', 'Importance of generic security and safety means', and 'Information security as technological annoyance for work functionality' gave $0.60 < \alpha < .70$.

3.1.3. Statistical analysis

Fig. 3 indicates the following null hypotheses that are to be statically tested in order to assess whether a change of awareness and behaviour has occurred or not:

- $H_0$1: There is no improvement of awareness and behaviour at t_2 compared to t_1 among members of the intervention group
- $H_0$2: There is no change in awareness and behaviour at t_3 compared to t_2 among members of the intervention group
- $H_0$3: There is no change in awareness and behaviour at t_2 compared to t_1 among members of the control group

The first hypothesis is directional, so the test of significance is one-tailed. For the other two hypotheses the test of significance is two-tailed. Testing of these hypotheses answers the research question of whether the intended changes have occurred in the awareness and behaviour of the test subjects.

All respondents were given an anonymous respondent number, which was automatically generated by the web-based questionnaire software, and used in each of the three surveys. As a consequence, individual respondent data was matched for each survey. The experimental design of the intervention study thus made it possible to test the hypothesis of no difference from one point in time to another by using paired-sample *t*-tests, which were performed in SPSS.

An experimental design strengthens the internal validity of the study, i.e. whether it actually is the intervention that modifies awareness and behaviour in the current study. Randomization strengthens the experimental design, 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 best way to ensure external validity for experimental designs is to randomize groups (Ringdal, 2001).

3.2. *Qualitative evaluation*

The quantitative analysis of an intervention should be supported by qualitative evaluation techniques (Kristensen, 2005; Robson et al., 2001). This triangulating approach offers better interpretation of the intervention and its effects, as qualitative methods provide a breadth and depth to the evaluation that cannot be achieved by using quantitative approaches only. The use of qualitative methods is important not least for studying the dynamics of the intervention process itself, as qualitative research provides understanding of social processes (Strauss and Corbin, 1998; Thagaard, 2002).

The aim of the qualitative evaluation of the intervention is thus to get indications of why the workshops functioned as they did, and of how the workshops influenced awareness and behaviour. Four qualitative research approaches were used to collect data:

- *Group-based discussions* during the last part of each workshop. These gave input as to how the participants experienced the workshop and its effect on their knowledge and skills.
- *Observation study*. The observation study aimed at mapping how the workshop participants and the security officers acted and reacted to different elements in the meeting.
- *An in-depth interview* with each of the two security officers was conducted about a month after the workshops, mapping their impressions of the workshop and why it functioned as it did.
- *Free-text data* from the second questionnaire regarding the structure and function of the workshop.

The qualitative data collected by the methods listed above was analyzed by looking for patterns in the data (Leiulfrud and Hvinden, 1996) that described how the intervention was interpreted and why the intervention modified or failed to modify awareness and skills. Furthermore, the data was also searched for reasons for these patterns.

4. Results

This section presents the results of the quantitative and qualitative evaluation of the intervention study. First, quantitative results are presented, indicating whether the intended modifications of behaviour and awareness occurred among the intervention group and whether or not there were any changes within the control group. Second, qualitative results of the intervention study are presented, providing a basis for interpreting what caused the quantitative results.

4.1. *Quantitative evaluation*

4.1.1. *Participants*

Table 1 shows the demographic characteristics of the participants of the study at t_1. Chi-square tests show no significant differences between the two groups. Independent sample *t*-tests for the awareness and behaviour indexes revealed that there were no significant differences between the intervention and the control group at t_1.

196 respondents of the total study population of 197 replied to one or more of the surveys at a response rate of 92% for the pre survey, 89% for the post survey and 84% for the post–post

Table 1 – Comparison demographic characteristics of participants in the intervention group and the control group at t_1.

	Intervention group	Control group
Age (years)		
18–29	8.0%	7.0%
30–39	36.5%	37.0%
40–49	36.5%	32.5%
50–59	16.5%	16.5%
60-	2.5%	7.0%
Education		
High school	53.0%	46.5%
College/university <3 years	21.0%	21.0%
College/university >3 years	16.5%	22.0%
Other	9.5%	10.5%
Seniority (years)		
0–1	1.0%	7.0%
1–5	22.5%	22.5%
6–10	32.0%	24.0%
11–25	44.5%	46.5%
Women (%)	69.5%	71.0%
N at t_1	85	96

survey. 143 employees responded to all three surveys. The number of respondents used in the paired-sample t-tests was given by adding the respondents who replied to either the pre and post surveys or to the post and post–post surveys to the number of respondents who replied to all three surveys. For the pre-post test this gave $N = 79$ respondents in the intervention group and $N = 89$ respondents in the control group. $N = 71$ of the members of the intervention group answered both the post and the post–post survey.

4.1.2. *Pre-post test*

Table 2 gives the results of the paired-sample t-test of the pre and post surveys for both the control group and the intervention group. All indexes range from 1 (poorest) to 5 (best), so the awareness indexes are generally quite high for both the intervention group and the control group. At t_2 most of the indexes have a score around 4, but eve at t_1 the indexes are above the median value of the ordinal scale. This suggests that the awareness of the study population is fairly high. This pattern is not reproduced for the behavioural indexes. However, the purpose of this study is not to evaluate the information security condition, but to identify whether modification of awareness and behaviour has occurred or not.

Generally speaking, the data shows that awareness and behaviour among members of the intervention group had improved a month after the workshop, while the control group had mainly remained stable over the same period of time. Awareness had improved more significantly than behaviour among the intervention group. In particular, this group shows significant improvement of their personal willingness to contribute to the information security work ($p < .001$) and personal responsibility for information security ($p < .001$). It can thus be claimed that the personal involvement and commitment to information security has improved

Table 2 – Results of paired-sample t-test of the pre and post survey for intervention and control group.

	Index	Pre Mean (SD)	Post Mean (SD)	t (df)
Awareness	*Responsibility*			
	Intervention group	3.91 (0.45)	4.12 (0.52)	4.16 (75)****
	Control group	4.05 (0.49)	4.06 (0.51)	0.31 (86)
	Motivation			
	Intervention	3.54 (0.94)	3.89 (0.81)	4.80 (78)****
	Control	3.56 (0.84)	3.75 (0.87)	2.60 (88)^
	Info.sec vs functionality			
	Intervention	3.46 (0.64)	3.59 (0.62)	1.95 (78)*
	Control	3.56 (0.62)	3.52 (0.58)	−0.67 (85)
	Reporting			
	Intervention	4.03 (0.73)	4.27 (0.80)	2.35 (78)*
	Control	4.15 (0.89)	4.09 (0.92)	−0.42 (88)
	Perceived skills and knowledge			
	Intervention	3.29 (0.75)	3.97 (0.66)	7.66 (78)****
	Control	3.60 (0.77)	3.44 (0.75)	−2.06 (88)^
	Importance of specific information security means			
	Intervention	3.89 (0.76)	4.13 (0.75)	3.32 (75)****
	Control	4.10 (0.67)	4.02 (0.74)	−1.34 (84)
	Importance of generic loss prevention means			
	Intervention	3.78 (0.84)	4.07 (0.80)	4.19 (75)****
	Control	4.07 (0.72)	4.06 (0.73)	−0.19 (87)
Behaviour	*Checking unfamiliar persons without ID-cards*			
	Intervention	1.25 (0.71)	1.42 (0.93)	2.18 (78)*
	Control	1.30 (0.85)	1.33 (0.81)	0.23 (88)
	Carrying ID-cards			
	Intervention	3.22 (1.47)	3.59 (1.52)	2.57 (78)**
	Control	3.52 (1.53)	3.62 (1.50)	1.34 (88)
	Locking the computer			
	Intervention	2.39 (1.52)	2.94 (1.43)	3.13 (78)***
	Control	2.64 (1.52)	2.88 (1.51)	2.22 (88)^
	Manual virus-check			
	Intervention	2.66 (1.62)	2.77 (1.73)	0.55 (78)
	Control	3.15 (1.62)	3.26 (1.63)	0.72 (88)

*One-tailed $p < .05$, **one-tailed $p < .01$, ***one-tailed $p < .005$, ****one-tailed $p < .001$.
^Two-tailed $p < .05$.
Indexes range from 1 (poorest) to 5 (best).
SD = standard deviation, t = t-value, df = degrees of freedom.

among the intervention group members. The perceived importance of loss prevention measures has improved significantly for this group. Although the main focus of the workshops was on information security topics, the perceived importance of generic loss prevention measures improved in the same way as the specific information security measures.

There is a significant improvement for the single item of perceived personal knowledge and skills of information security among the intervention group ($p < .001$). A two-tailed test of the same item shows that the control group has a significant (two-tailed $p < .05$) decrease in perceived skills and knowledge. This negative change in the control group may indicate that non-participants in the workshop have noticed the information security initiatives of the organisation and feel that they, too, need more knowledge. The control group displays two significant changes in a positive direction: They show improved willingness to contribute to the information security work and have started locking the computer when away from it. Employees who have not yet participated in the workshops have thus become more motivated for making individual contributions to information security, but simultaneously state that they feel an increased lack of knowledge and skills regarding information security. This should be an excellent point of departure for the planned security training of this group of employees.

The post–post test (see Table 3) shows the result of the paired-sample t-test for the intervention group six months after the workshops were arranged. The hypothesis of no difference of indexes between t_2 and t_3 was tested, and showed that there were no significant changes of awareness among the intervention group. This implies that the improved awareness occurring one month after workshop participation remains stable half a year after the workshops were arranged. Behavioural indexes have on the other hand changed significantly in a positive direction at t_3. This could indicate that it takes more time to modify behaviour than awareness. Three behaviour items have improved significantly from t_2 to t_3. All of these items had also improved significantly from t_1 to t_2.

4.1.3. *Perceived change in awareness and behaviour*

Table 4 shows the distribution of answers to the question 'have you changed your information security behaviour or awareness during the last year?' The paired-sample t-tests in Tables 3 and 4 indicate that there are significant changes in the awareness and behaviour of the intervention group after their participation in the intervention. These findings are validated by the participants' perceived changes of awareness and behaviour, which remained stable six months after the workshops. Even some members of the control group feel that their awareness and behaviour have changed one month after the intervention. Figs. 4 and 5 indicate which areas the perceived changes have occurred in, and what the respondents felt to be the causes for the changes.

Table 3 – Results of paired-sample t-test of the post and post–post survey for the intervention group.

	Index	Post mean (SD)	Post–post Mean (SD)	t (df)
Awareness	*Responsibility*			
	Intervention	4.12 (0.53)	4.08 (0.51)	−0.70 (69)
	Motivation			
	Intervention	3.91 (0.81)	3.93 (0.79)	0.24 (70)
	Info.sec vs functionality			
	Intervention	3.59 (0.67)	3.60 (0.69)	0.17 (70)
	Reporting			
	Intervention	4.23 (0.87)	4.07 (0.93)	1.16 (70)
	Perceived skills and knowledge			
	Intervention	3.97 (0.70)	3.93 (0.68)	0.48 (70)
	Importance of specific information security means			
	Intervention	4.12 (0.77)	4.15 (0.77)	0.36 (69)
	Importance of generic loss prevention means			
	Intervention	4.10 (0.81)	4.15 (0.78)	0.81 (69)
Behaviour	*Checking unfamiliar persons without ID-cards*			
	Intervention	1.48 (1.04)	1.56 (1.04)	2.23 (70)**
	Carrying ID-cards			
	Intervention	3.68 (1.47)	3.90 (1.29)	1.67 (70)*
	Locking the computer			
	Intervention	2.99 (1.45)	3.35 (1.34)	2.23 (70)**
	Manual virus-check			
	Intervention	2.89 (1.76)	3.25 (1.73)	0.76 (70)

* Two-tailed $p < 0.10$, ** Two-tailed.
$p < 0.05$ Indexes range from 1 (poorest) to 5 (best).
SD = standard deviation, t = t-value, df = degrees of freedom.

Table 4 – Perceived change of awareness and behaviour.

		Intervention group t_2	Intervention group t_3	Control group t_2
Have you changed awareness or behaviour during the last year?	Yes	66.3%	67.9%	27.4%
	Total	100% (83)	100% (78)	100% (94)

The findings illustrated in Fig. 4 verify the findings of the *t*-tests, which also showed improved behaviour in terms of carrying ID-cards, locking the computer, and reporting incidents. The *t*-tests showed improvements of behaviour from t_1 to t_2 and even from t_2 to t_3. Fig. 4 shows the same trend.

There was a particular emphasis on keeping ID-cards visible during the intervention period. First, the intranet notice in the beginning of the period emphasised this. ID-cards were also one of the subjects of the scenarios discussed in the groups during the workshop. Between t_2 and t_3 new lanyards for keeping the ID-cards visible were handed out. Emphasis on particular subjects thus seems to be an effective measure.

Locking the computer gave a high significant change at t_1 ($p < .005$) and the values also improved at t_2. During the workshops one of the security officers picked up a keyboard and showed the participants how simple it was to lock the computer by using the Windows-key in combination with the L-key. This may therefore have been experienced by the participants as a non-time-consuming, practical simple action they could easily perform. Chi-square tests show a significant difference regarding e-mail use ($p = .07$), whereas elsewhere the results remain stable over time. It has not been possible to explain this significant change of e-mail use from the data.

Fig. 5 shows the causes cited by the intervention participants for why their awareness and behaviour have changed. The figure shows that several formal and informal activities are perceived as causes for modified individual information security abilities. This illustrates the importance of combining several activities in programmes aimed at changing awareness and behaviour. The main part of the intervention, the workshops, is also the most frequently assumed cause for improved awareness and behaviour. 92% at post (t_2) and 96% at post–post (t_3) say that their awareness and behaviour have been modified due to their participation in the workshops.

The only significant change in the cited causes for modification between t_2 and t_3 was in relation to the intranet-article ($p = .02$). About 40% say that they have changed as a result of reading the intranet-article at t_2, while only about 20% say that the intranet-article had any effect at t_3. This may indicate that this type of information security measure has a short-term effect.

Table 4 shows that one quarter of the members of the control group perceive that their security abilities have been modified at t_2. Since these did not participate in the workshops, it is interesting to look into the causes for their perceived changes. About 80% of the members of the control group that claim to have changed their awareness/behaviour state that the intranet-article has influenced their awareness and behaviour, and about 80% state that filling out the questionnaire is a cause of their modifications. The *t*-tests also show some significant changes in the control group regarding increased attention to information security, but still a perceived lack of information security knowledge and skills. The measures influencing the control group, i.e. all the activities in Fig. 5 except the workshop and leaflet, thus seem to create interest but to lack the dimension of creating knowledge and skills.

4.2. *Qualitative evaluation of the workshops*

Both the participants and the security officers expressed that they were very pleased with the way the workshops were arranged, and some of the participants even declared that this was the best educational approach they had ever encountered. This is verified by questions in the second survey regarding how the participants experienced the content and processes of the workshops. Several of the participants declared that they perceived an instant improvement of awareness and knowledge, and some announced that they would immediately change their behaviour, e.g. start to lock their computer before leaving it. In the following, we describe

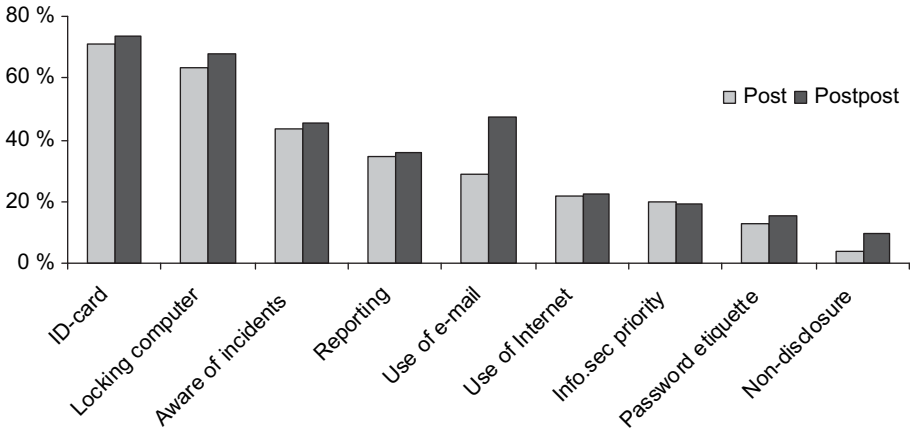

Fig. 4 – Areas in which members of the intervention group report changed awareness or behaviour for post and post–post study (fixed alternatives, several answers possible pr respondent).

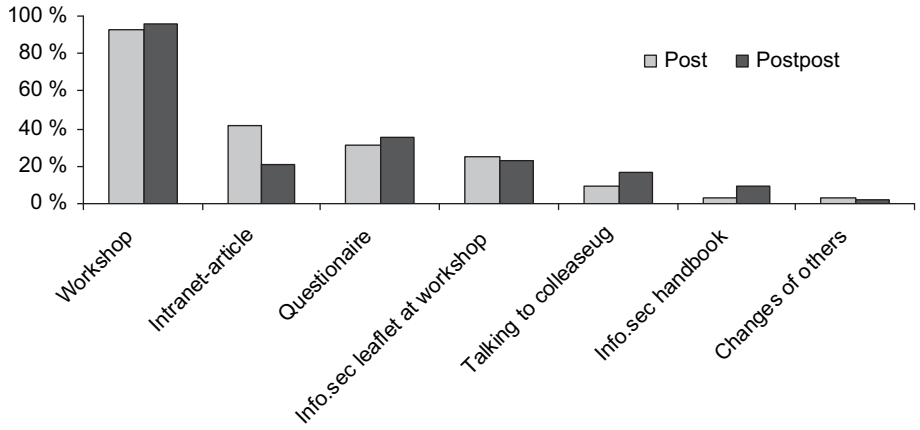

Fig. 5 – Causes of changed awareness and behaviour among members of the intervention group who have perceived a change in behaviour or awareness (several answers possible pr respondent).

patterns which explain why the workshop was highly valued. Common for these patterns is that the actual processes taking place in the workshop are more important than the topics of discussion.

The overall strategy behind the workshop was informed by the theoretical framework presented earlier in the paper. This framework was materialized into action by aiming at involving employees in group conversations in order to make them reflect over information security and their own working situation. There was no one-way communication from the officers to instruct the participants in terms of what they were supposed to think. Instead, the security officers functioned as facilitators for the meetings. The expert knowledge of the information security officers was only used as a tool to suggest alternative courses of action for the participants if their thoughts were heading in the wrong direction. The officers seldom interrupted discussions; rather, they let the participants do the talking. Many of the participants had expected one-way communication from the security officers in the meetings, and were thus pleasantly surprised by the extensive use of plenary discussions and involvement. One of the participants illustrated this neatly by stating: ''I was alarmed by the thought of sitting here for 2 h being bombarded with information. I was thus very surprised by the way the meeting was arranged. This is definitively the way to inform employees'', Participation in discussions was one of the main reasons that the participants experienced the workshops as they did, as exemplified by the following quotation: ''This approach is much better than just sitting there listening. It makes us think. My improved awareness will last longer after this kind of meeting''.

The discussions were lively during the 2 h, and almost all of the participants contributed to the conversations. This is partly explained by the size of the groups, which was suitable for the learning strategy of involving workshop participants in an active way. In each workshop, the participants worked with similar issues, and they already knew each other well. Moreover, the company is located in a small town in northern Norway, which implies that many of the participants knew of each other from home and leisure activities. This created confidence, and may have helped to ease the start of dialogues as well as to maintain them during the workshop.

The lively discussions and the active participation of the employees are also explained by the atmosphere of the workshop. The atmosphere was relaxed, pleasant and informal. The tone was set by the humorous and engaging way in which the workshop procedures and information security issues were explained by the security officers. The entertaining approach taken by the security officers rubbed off on the participants. At the start of the meetings the officers talked some nonsense with each other and the participants. This created roars of laughter, thus setting the scene for the described atmosphere. Although the meetings were funny, there was nonetheless a good balance between jokes and seriousness. The relaxed and humorous atmosphere of the meetings was reflected in the role taken by the security officers, who remained relaxed during the session. They sat by the table, signalizing thus that they were not authoritarian chairmen. The two security officers who facilitated the meeting were praised by the participants for their ability to make information security understandable and humorous, both in the free text sections included in the surveys and in the evaluation at the end of each workshop.

4.2.1. *More insight into the current state of information security*

The quantitative analysis showed improved awareness and behaviour among workshop participants. Another result of the workshop was that the information security officers gained an understanding of how information security is actually performed and interpreted in the organisation. Several inadequate security conditions were discovered during the meetings. According to the security officers, these conditions would never have been recognized by other tools and methods. Consequently, support for better decisions regarding information security was created. Also, the conditions for implementing information security measures are probably improved as a result of the workshop intervention, as the security officers have gained a better understanding of how information security work actually functions in the organisation. At the same time, the members of the organisation have also become familiar with the information

security officers, which may make it easier for users to contact these officers if other problems or questions should arise.

5. Discussion

The conceptual model in Fig. 1 in the introductory part of this article raised some research questions regarding changes in awareness and behaviour, and causes for these possible changes, and regarding whether the intervention was carried out as intended. These questions are jointly discussed in the following.

5.1. *Intended changes in awareness and behaviour*

The pre-post test showed that the intervention was powerful enough to significantly change awareness and behaviour among the participants in the intervention group. The change of awareness is here understood as improved attitudes and knowledge to information security after the intervention, while behavioural changes are related to perceived changes of behaviour among employees. The third survey half a year after the workshops showed that the awareness modifications among the participants remained stable over time, and that there was even a significant improvement for some behavioural attributes from the second to the third survey. The control group mainly remained unchanged in the pre-post test.

Participation in the workshops is the only factor separating the intervention and control groups; it can thus be claimed that the effect of the workshop has created the intended improvements in awareness and behaviour. This is supported by the participants' perceived causes for their changes; see Fig. 5. At both t_2 and t_3, over 90% say that workshop participation has caused changes in their awareness or behaviour.

The control group has a significant increase of their perceived lack of information security knowledge and skills from t_1 to t_2. This indicates that the control group have been affected in the sense that their attention to information security has improved, but that they have not been influenced in a way that makes them feel capable of safe and secure performance in their jobs. This legitimizes the use of future workshops for the rest of the organisation.

The pre-post test showed smaller changes in information security behaviour than in awareness for the intervention group. In contrast, the post–post test shows no changes in awareness but significant improvements in behaviour at t_3. There are several possible explanations for this development. One interpretation is that the intervention participants know how to behave and are capable of behaving that way at t_2, whereas they only actually act this knowledge out at t_3.

Considering behaviour as a direct product of awareness, one may argue that when awareness has matured for some time, modified behaviour follows suit. On the other hand, Lund and Aarø (2004) show that the association between attitudes and behaviour is often weak. Not only attitudes, but several other factors also influence behaviour, e.g. social norms, administrative frameworks, and technology. If we follow this line of thought, the delayed changes of behaviour may be explained by changes occurring in the social norms of the organisation, and by the increased focus on information security in all of its parts. For example, Fig. 5 shows that at t_3, about 20% say that talking to colleagues is one of the causes for their changes of behaviour, whereas in contrast, about 10% cited this as a reason at t_2. The overview in Fig. 5 also shows that administrative factors such as the information security handbook, the intranet-article, and the leaflet influence behaviour and awareness.

5.2. *Why did the workshops lead to intended changes?*

The main part of the intervention was the workshop, although it was combined with other measures. Among the set of intervention measures used, participation in a workshop proved to be by far the most powerful. Respondents who had not participated in workshops show very modest improvements of their information security abilities, whereas the improvements are very significant among the workshop participants. This is verified by the perceived causes for changes cited among the intervention group; see Fig. 5. Over 90% say that one of the causes for their changed information security features was participation in the workshops.

A combination of several measures is often effective in loss prevention work (Lund and Aarø, 2004). Although they may have less effect on awareness and behaviour changes than the workshop, the other measures used in this intervention project should not be rejected. Not least, other measures play an important role in the follow-up activities after the workshop. In this particular study, the data from the control group shows that the intranet notice and filling out the questionnaire (Fig. 5) have caused a perceived change of awareness and behaviour. The pre-post paired-sample *t*-test (Table 2) indicates that members of the control group have improved their attention to the field of information security, although they have not improved their information security knowledge and skills. Hence, the measures other than the workshops used in the intervention have also been shown to have an effect in terms of improved attention to information security. However, since the most powerful intervention measure was workshop participation, the following discussion of the causes for the intervention's intended changes concentrates on the workshops.

From a rationalistic point of view, users are supposed to act in compliance with rules and requirements for expected behaviour and technological inscriptions. On the other hand, research indicates that users tend to have a different type of rationality. Users trade off information security for other work demands, they lack knowledge about information security and associated risks, and they display poor information security behaviour (Adams and Sasse, 1999; Albrechtsen, 2007; Besnard and Arief, 2004; Post and Kagan, 2007; Stanton et al., 2005). These research results indicate that there is a need to improve users' information security abilities. At the same time, these findings question users' motivation for contributing to the information security work of an organisation. Consequently, challenges emerge in terms of how to manage the human part of information security: How should information security management approach the users? The last part of the discussion looks into these challenges by elaborating on why the workshop modified the awareness and

behaviour of its participants although research indicates that users' information security performance cannot easily be modified for the better.

5.2.1. *Participation and dialogue*

The theoretical basis for the intervention study emphasised employee participation, collective reflection, group-work and knowledge sharing at an organisational level. The qualitative data material indicates that the intervention was carried out as intended regarding these preconditions.

Participation proved to be an effective way of influencing employees. The participants state that they had to actively involve themselves in discussions on information security, and most of them report that they enjoyed this way of arranging information meetings. An important premise for involving the employees was that the security officers stayed in the background. They were present, but not in command, thus leaving the meeting open to the contributions of the participants. When these were taken seriously and their involvement was sought through the discussions, they proved to be interested in and motivated for information security after all. Most of the participants expressed opinions, made comments, voiced problems or asked questions. They thus engaged in an active relationship to information security, which created improved motivation, understanding and ownership in relation to information security. The intention of the workshops was not to persuade users, but to convince them, by letting the participants reflect, on their own terms, on why information security is important. The statistical analysis of the effects of the workshop indicates that this intention was fulfilled, as there was significant improvement in the perceived importance of many aspects of information security among the intervention group.

Through collective reflection and participation in groups, individuals get a possibility both to influence their own working conditions and to help shape the organisational community's interpretations and insight into the organisation (Levin and Klev, 2002). This group-based reflection also ensures common insight into information security structures and procedures, which is fundamentally important for coordinated interaction in an organisation (Weick, 1996). This logic indicates that in addition to the changes taking place with respect to individual ideas and practices, collective thoughts and routines also change (Levin and Klev, 2002). Groups are a connecting link between individuals and the different levels and layers in the organisation, and the use of groups makes it possible to integrate individual considerations and initiatives while at the same time dealing with the big picture (Levin and Rolfsen, 2004). Not least, groups are an excellent tool for transferring experience and knowledge among both employees and managers. In this sense knowledge creation happened at an organisational level, as individuals interacted and shared their experiences and thoughts on information security and the security experts added their expert knowledge to the mixture.

5.2.2. *Organisational knowledge creation*

Another important factor contributing to the modified awareness and behaviour of the intervention participants was the use of local experience and knowledge of the workplace, the working conditions, the IT-systems and information security. The plenary dialogues being based on the participants' own terms ensured that the issues were recognisable and accessible to all – an approach which created ownership and familiarity towards the subjects of discussion. Through the participants' sharing of their experience and knowledge with each other, and the security officers' expert contributions, organisational knowledge was according to Nonaka and Takeuchi (1995) created and shared among organisational members (Nonaka and Takeuchi, 1995). This created a common interpretation of information security objectives, responsibilities and means. By sharing knowledge in an understandable way by listening or participating in collective reflections, individuals acquire knowledge themselves. This acquisition of knowledge creates improved information security abilities among workshop participants. The informal atmosphere, the limited role played by the security officers, and the mutual trust among the participants and the security officers were all criteria which contributed to the successful sharing of knowledge in the intervention described in our study.

Argyris and Schön (1996) argue that it is a change in the theory-in-use rather than the espoused theory that creates organisational learning. The paired-sample *t*-tests indicate changes in the theory-in-use, i.e. the behaviour, among individuals who participated at the workshops. However, individual learning does not in itself create changes at an organisational level, because organisations are about people interacting. The most important difference between organisational and individual learning is that organisational learning means a change in common understanding, relations and interactions. We know from our study that individuals have improved information security awareness and behaviour. However we do not know if changes in common understandings and interactions have happened, we can thus not conclude if organisational learning has occurred. To study if organisational learning occurred we need longitudinal research and a research design that studies relations and interactions in the organisation.

5.2.3. *Interest and motivation*

Experiences from occupational safety intervention studies reveal that if behavioural interventions are not interesting or motivating (intensity), and/or the workers do not have enough exposure to the interventions or enough vested in them (frequency and duration), the intervention is unlikely to lead to any changes in behaviour (Goldenhar and Schulte, 1994). Regarding time spent on the intervention, it is interesting to note that although the duration of the intervention was relatively short, the intervention had an effect. In a busy working day, this is in particular of interest for information security managers. The intervention was efficient both regarding success (i.e. improved information security awareness and behaviour) and regarding time spent. As discussed previously, the most powerful factor in the intervention was the workshops. The workshop only lasted for 2 h, so the frequency and duration of the intervention is low. The success of the intervention must thus be explained by other factors than these two factors.

Information security may in the first place seem boring to lay people, so the subject of the intervention may have looked uninteresting to the participants. Nevertheless, qualitative data from the study reveals that employees' motivation for and interest in the intervention has actually been excellent, and that this was one of the main reasons for the successful changes of awareness and behaviour. What made the workshop processes so interesting and motivating to the employees was the dual factors of the relaxed and humorous atmosphere and the active way in which the participants were involved. In this sense, the process itself was more important for the modifications than the actual contents of the meetings. This approach is a useful one, then, not least with respect to future efforts to overcome the lack of motivation and knowledge of information security among users described by several academics (Adams and Sasse, 1999; Albrechtsen, 2007; Besnard and Arief, 2004; Post and Kagan, 2007; Stanton et al., 2005).

6. Conclusion

The approach of the intervention studied in this paper differs from mainstream information security awareness measures, which typically aim at having an impact on the individual level through an expert-based approach directed at a large population, e.g. in the shape of formal presentations, e-mails, leaflets and posters. This study demonstrates that locally based employee participation, collective reflection, group processes, and knowledge creation at an organisational level create changes in information security awareness and behaviour at an individual level. By measuring employees' attitudes and knowledge to information security in addition to perceived individual information security behaviour before and after the intervention, the study successfully shows that information security workshops of short duration and small size produce powerful changes that remain stable for at least half a year.

Some principles applied in the intervention were particularly important for the successful improvement of awareness and behaviour among the intervention participants. These are employee participation, collective dialogue and reflections in a universally comprehensible language register based on the employees' own terms, laid-back expert facilitators, mutual trust in small-sized groups, and sharing of locally-based tacit knowledge. These principles should be emphasised in participation-based approaches to information security management.

The approach used in this intervention 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, or even to other kinds of threats and hazards in risk management, as it was the processes behind the workshop and not its contents and subject matter that above all caused the intended modifications.

Acknowledgements

The authors wish to thank the employees at the Brønnøysund Register Centre who contributed to the study. In particular, we are grateful to the information security officers Olav Melteig and Marius Naaslund Gjerde, whose input made the intervention study possible.

REFERENCES

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 T, editors. Usability – turning technologies into tools. New York: Oxford University Press; 1992.

Albrechtsen E, Hovden J. User participation in information security. In: Aven T, Vinnem JE, editors. Risk, reliability and social safety: proceedings of the European safety and reliability conference 2007 (Esrel 2007). London: Taylor & Francis; 2007. p. 2551–8.

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

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

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

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

Elden M. Democratisation and participative research in developing local theory. Journal of Occupational Behaviour 1983;4(1):21–33.

Goldenhar LM, Schulte PA. Intervention research in occupational health and safety. Journal of Occupational Medicine 1994; 36(7).

Greenberg ES. The consequences of worker participation: a clarification of the theoretical literature. Social Science Quarterly 1975;56(2):191–209.

Greenwood DJ, Levin M. Introduction to action research. Thousand Oaks, CA: SAGE Publications; 1998.

Hubbard W. Methods and techniques of implementing a security awareness program. SANS Institute; 2002. white paper.

Kristensen TS. Intervention studies in occupational epidemiology. Occupational and Environmental Medicine 2005;62(3):205–10.

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.

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

Levin M, Rolfsen M. Arbeid i team [Work in teams] (in Norwegian). Bergen, Norway: Fagbokforlaget; 2004.

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.

Nonaka I, Takeuchi H. The knowledge-creating company. New York: Oxford University Press; 1995.

Post GV, Kagan A. Evaluating information security tradeoffs: restricting access can interfere with user tasks. Computers and Security 2007;26(7):589–99.

Ringdal K. Enhet og mangfold, samfunnsvitenskaplig forskning og kvantitativ metode [Unity and diversity, social research and quantitative methods] (in Norwegian). Bergen, Norway: Fagbokforlaget; 2001.

Robson LS, Shannon HS, Goldenhar LM, Hale AR. 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. Cincinnati, OH: NIOSH; 2001.
Shrader-Frechette KS. Risk and rationality. Oxford: University of California Press; 1991.
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 [Introduction to qualitative methods] (in Norwegian). Bergen, Norway: Fagbokforlaget; 2002.
Voss BD. The ultimate defense of depth: security awareness in your company. SANS Institute; 2001. white paper.
Weick KE. Sensemaking in organizations. Thousand Oaks, CA: SAGE Publications; 1996.

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 senior research scientist at SINTEF Technology and Society and is also employed as an adjunct assistant professor at the Department of Industrial Economics and Technology Management 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 Norwegian Government's commission on the vulnerability and emergency preparedness of the Norwegian society.