Information & Computer Security

Management commitment and awareness creation - ICT safety and security in electric power supply network companies

Ruth Østgaard Skotnes

Management commitment and awareness creation – ICT safety and security in electric power supply network companies

Ruth Østgaard Skotnes
Center for Risk Management and Societal Safety, Department of Media, Culture and Social Sciences, University of Stavanger, Stavanger, Norway

Received 28 February 2014
Revised 30 June 2014
8 September 2014
30 October 2014
Accepted 3 November 2014

Abstract

Purpose – This paper aims to follow-up on previous research by studying the degree of management commitment to information and communication technology (ICT) safety and security within network companies in the electric power supply sector, implementation of awareness creation and training measures for ICT safety and security within these companies and the relationship between these two variables.

Design/methodology/approach – Data were mainly collected through a survey among users of ICT systems in network companies within the Norwegian electric power supply sector. In addition, qualitative data were gathered through interviews with representatives from the regulatory authorities, and observation studies were conducted at ICT safety and security conferences.

Findings – In accordance with previous research, our survey data showed a statistically significant correlation between management commitment to ICT safety and security and implementation of awareness creation and training measures. The majority of survey respondents viewed the degree of management commitment to ICT safety and security within their own organization as high, even though qualitative studies showed contradictory results. The network companies had implemented awareness creation and training measures to a varying degree. However, interactive awareness measures were used to a lesser extent than formal one-way communication methods.

Originality/value – The paper provides insight into management commitment to and implementation of awareness creation and training measures for ICT safety and security within network companies.

Keywords Training, Management commitment, Security, Safety, Awareness creation, ICT

Paper type Research paper

1. Introduction

Previous research has advocated the need for more training, awareness creation and management commitment regarding ICT safety and security[1] (Johnson, 2006; Hagen *et al.*, 2008; Hagen, 2009; Hagen and Albrechtsen, 2009a). Studies of safety have suggested that management involvement is important for the safety work within companies. If the management is engaged, it will be aware of the need for information security measures to comply with the laws and assure that safety and security measures are implemented. The success of safety and security management systems is often said to be dependent on the commitment of all staff, and all members must be aware of their responsibility for safety and security. Otherwise, the safety and security mechanisms can be bypassed or diminished by employees.

Information & Computer Security
Vol. 23 No. 3, 2015
pp. 302-316
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-02-2014-0017

This article follows up on previous research which has shown a positive relationship between management commitment to ICT safety and security and implementation of awareness creation and training measures. The following research questions are addressed:

RQ1. To what degree is the management of network companies in the electric power supply sector committed to the safety and security of their organizations' ICT systems?

RQ2. To what extent are awareness creation and training measures for ICT safety and security implemented within network companies in the electric power supply sector, and what type of measures are implemented?

ICT has increasingly become a part of all critical infrastructures[2] (Line and Tøndel, 2012), and is used to monitor, control and operate power generation plants and power distribution within electric power supply systems. A breakdown in these ICT systems (process control systems) can seriously compromise the physical grid, which can result in major financial disasters and damage to public safety and health (Patel and Sanyal, 2008). The electric power supply is the most critical infrastructure in modern society (Hagen and Albrechtsen, 2009a), and a prolonged interruption of the electric power supply may have consequences for many critical societal functions caused by the interdependencies between infrastructures.

Process control systems, for example supervisory control and data acquisition systems (SCADA systems)[3], and other ICT systems used within the electric power supply system, are vulnerable to a multitude of threats, both natural and man-made (Rodal, 2001). Connecting the ICT systems to the Internet has increased the risk for system breakdowns and serious failures (Hagen and Albrechtsen, 2009a), and has made the formerly isolated ICT systems vulnerable to a set of threats and risks that they have not been exposed to before (Line and Tøndel, 2012). Vulnerability of ICT systems in the electric power supply system is also expected to increase during the next years. Advanced Metering Infrastructure (AMI) and, later on the Smart Grid, are now being introduced in the electric power systems of the Western countries. The electric Smart Grid promises increased capacity, reliability and efficiency through the marriage of cyber technology and the existing electricity network. However, the scale and complexity of the smart grid, along with its increased connectivity and automation, make the task of cyber protection particularly challenging (Kundur *et al.*, 2010).

The research questions are answered by presenting results from a survey sent to 137 network companies in Norway, supplemented by results from interviews with representatives from the Norwegian Water Resources and Energy Directorate (NVE) and observation studies. The next section introduces the theoretical foundations for the study. Section 3 presents the data material and methods used in the study, and data analysis and results of the survey are presented in Section 4. In Section 5, results from the survey, interviews and observation studies are interwoven in the discussion, and finally, Section 6 contains the conclusion.

2. Theory

2.1 ICT safety and security measures

ICT safety and security measures include both technological and organizational measures. Technological measures can consist of personal passwords, redundancy of critical systems, intruder detection systems, anti-virus software and firewalls. Hagen *et al.* (2008) have categorized organizational measures into four main groups: security policy, procedures and control, administrative tools and methods (e.g. risk analysis, audits, incident reporting systems) and organizational and individual awareness creation and maintenance. The first three groups of organizational safety and security measures can also be described as technical–administrative measures. The fourth group of organizational measures consists of training/education, awareness campaigns, user participation, top management's engagement and involvement of all parts of the organization in learning processes from incidents. In this study, we have chosen to focus on management's engagement/commitment (both top management and middle management), and training/education and awareness campaigns.

According to Hagen *et al.*'s (2008) survey among information security professionals in Norway, awareness-creation measures were assessed to be very effective compared to the basic, formal security systems; however, awareness-creation measures were also the least implemented. Information security management has traditionally emphasized formal management approaches, and formal measures are also less resource-demanding than awareness-creation measures. When formal management systems (i.e. policies, procedures and tools) are in place, these measures may be taken for granted and accepted as contributors to an adequate security level.

2.2 Management commitment

According to Rasmussen (1997), management's commitment to safety and security has appeared to be a major problem, and has led to the relating efforts of society to control management incentives by safety and security regulation. Research on safety climate has also indicated that the safety levels of organizations are influenced by managers' attitudes toward safety and the perceived priority given to safety training (Antonsen, 2009). Hagen (2009) defines information security as essentially a management responsibility. Information security should be embedded in all management processes, and include incident reporting and organizational learning. According to Johnson (2006), organizational policies and user guidelines require the commitment of top-level managers, and should be directly linked to the company's business strategies. The top management must be committed to ICT safety and security through its activities and through a dedicated budget. In addition, an organization's safety and security policy should contain a letter of commitment from the top management showing commitment to ICT safety and security within the organization, and assign responsibilities of each member of the organization, particularly line management, top management and safety and security professionals.

2.3 Awareness creation and training

Formal technical–administrative measures and documented systems, for example safety and security policies, guidelines and instructions, can be taken for granted, and often few users[4] have actually read the documents. Nevertheless, documents are often seen as important because they form the basis for other measures (Albrechtsen and Hovden, 2009). But when technological and administrative measures are in place, "softer" resources can be used to modify performance. Influencing individuals' knowledge, attitudes and behavior must be regarded as important means that are complementary to formal technical–administrative measures (Hagen, 2009). As Siponen (2000, p. 36) puts it:

> […] security people want end-users to internalize and follow given guidelines […] rather than to be aware of them but for some reason or other fail to apply them in reality.

ICT safety and security awareness can be seen as the extent to which organizational members understand the importance of information safety and security, the level of safety and security required by the organization and their individual safety and security responsibilities, and act accordingly (ISF, 2005, referred to in Albrechtsen, 2006). Members of an organization can have inadequate ICT safety and security awareness if they are unfamiliar with possible threats to the systems and how to mitigate them, if they are unaware of the possible consequences of safety and security breaches and if they see their own work in isolation and are unaware of the implications of their use of ICT systems (Albrechtsen and Hovden, 2009). A lack of safety and security awareness by users has been cited as the top obstacle for effective ICT safety and security. If people (management and employees) do not handle and protect ICT systems in a safe and secure manner, even the best technologies will be ineffective. Previous research has suggested that the impact of ICT safety and security breaches coming from people inside an organization is bigger than all other sources combined (Johnson, 2006; Hagen, 2009).

According to Albrechtsen and Hovden (2009), users often assume that the responsibility for ICT safety and security rests with the technology and with the ICT safety and security managers and they do not realize the benefits of ICT safety and security measures. In addition, users often trade-off ICT safety and security against efficiency and functionality, which can be caused by efficiency demands, emphasis on minimum-effort work and poor quality of ICT safety and security training and education resulting in insufficient skills and knowledge. For employees, the responsibility for acting in a manner that is safe and secure for the organization comes on top of other demands that they are faced with in their everyday work.

3. Material and methods

The research methodology in this study was mainly based on a survey; statistical data were collected from users of ICT systems (managers and employees) in network companies within the Norwegian electric power supply sector. In addition, qualitative data were gathered through in-depth qualitative interviews and observation studies. A combined approach can strengthen the validity of the study, as some of the findings can complement and validate each other (Silverman, 2006). However, as in this study, a combined approach can also show discrepancies between analysis results of data collected using different methods, and may thus open for new possibilities of interpretation.

3.1 Survey

A Web-based questionnaire was developed using QuestBack Survey and distributed to the respondents by e-mail[5]. The survey was sent to managers and employees in the 137 network companies that are part of the PSPO[6], 334 individuals in total[7]. The questionnaire contained ten sections – background information, knowledge of safety and security, perception of compliance, attitude toward safety and security, attitude toward regulation, experience of incidents, risk perception, safety and security management, awareness creation and training and overall rating of the safety and security levels of the organizations' ICT systems. In this article, we have chosen to focus on the results of the items in the safety and security management scale (management commitment) and the awareness creation and training scale. Items on the scales were measured on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

The safety and security management scale contained five items measuring the management's commitment to ICT safety and security in the network organizations. The items in this scale were:

- "My immediate manager intervenes immediately if the ICT safety and security rules are not followed";
- "My immediate manager checks from time to time whether we are actually working safely and securely";
- "My immediate manager is involved in the organization's ICT safety and security work";
- "My immediate manager appreciates my pointing out matters of importance to ICT safety and security"; and
- "I would rather not discuss ICT safety and security with my immediate manager".

Managers (ICT safety and security managers/coordinators and contingency planning managers) and employees (operators in system control centers and ICT staff) responded to the same items, hence we received information about the commitment of both top management and middle management in the network organization. The awareness creation and training scale contained six items related to the use of different awareness-creating and training measures in the network organizations (the individual items are shown in Section 4.1).

One hundred and three respondents returned the survey questionnaire, for a response rate of 31 per cent. NVE provided the names and e-mail addresses of ICT safety and security managers/coordinators and contingency planning managers in the network companies, and the managers were asked to provide names and e-mail addresses for employees in the organizations' system control centers and ICT staff. A survey sample of 103 respondents can be considered a relatively small sample, and may limit the potential for generalizing. According to Fricker and Schonlau (2002), response rates for Web surveys where no other survey mode is given have tended to range from moderate to poor. Other researchers have also experienced the same response rate problem in studies of information security management. The main reasons for non-responses have been related to a policy of not sharing information regarding their information security performance, the volume of survey requests received by the organizations and a desire not to spend valuable time on the particular research project (Albrechtsen and Hovden, 2009). In an attempt to raise the response rate, hidden identity for respondents was activated in our electronic survey, and all e-mail addresses were deleted after the survey was closed.

On the other hand, according to Pallant (2010, p. 135), a sample of 100+ respondents can be regarded as a large sample, and the sample size can be seen as adequate for the types of data analyses done in our study. In addition, qualitative research data were gathered to support the quantitative results from the survey, which might increase the potential for generalizing.

3.2 Interviews and observation studies

To explore our research theme, research questions were produced that could be tested by the quantitative survey, and to complement the data gathered through the survey, qualitative data were gathered through two group interviews with representatives from NVE. To complement the data from the survey and inform our study, observation studies were also carried out at two conferences on ICT safety and security within the electric power supply industry.

Semi-structured interviews with open-ended questions were used. The interviewees were representatives from the contingency planning department in NVE, who are responsible for safety, contingency planning and supervision in the Norwegian electric power supply sector. The first interview was done with three interviewees, and the questions mainly focused on the interviewees' opinion of the Norwegian network companies' risk perception and awareness regarding the risk of electric network failure caused by malfunctions in or attacks on their ICT systems. The second interview was done with two interviewees, and the questions mainly focused on the interviewees' opinion regarding the use of functional internal control regulations for ICT safety and security, and their impression of the network companies' attitudes toward these regulations.

The two conferences on ICT safety and security within the electric power supply industry were held in Norway in 2011. The participants at both conferences were mainly managers and employees working with ICT safety and security within network companies in Norway, in addition to suppliers of industrial control systems (e.g. SCADA-systems) and ICT safety and security solutions for these systems. The speakers at the conferences included representatives from NVE, NorCERT (the Norwegian Computer Emergency Response Team), Mnemonic AS (one of the largest providers of IT information security services in the Nordic region), NorSIS (Norwegian Centre for Information Security) and ICT safety and security researchers from universities and research institutes. During the observation studies, we observed the types of ICT safety and security issues raised at the conferences, the types of issues participants focused on and the types of questions and discussions that came up during the conferences.

4. Data analysis and results of survey

The Statistical Package for the Social Sciences (SPSS) v. 18 was used to perform the analyses, which included descriptive statistics and correlation. Negatively worded items were reversed, and total scale scores were calculated to give an overall score for the two scales used in the survey. A reliability test of the total scale scores indicated that the scales used in this study had good internal consistency; Cronbach's alpha was 0.85 for the safety and security management scale and 0.84 for the awareness creation and training scale.

4.1 Descriptive statistics

Table I shows the demographical distribution of the respondents. Out of all the respondents, 66 were managers and 32 were employees (5 respondents did not specify their job category). Only three of the respondents were female and the rest male. Sixty-three respondents worked in small network companies with less than 100

	Company size		
Job categories	More than 100 employees	Fewer than 100 employees	Total
Manager			
Gender			
Male	19	44	63
Female	1	1	2
Total	20	45	65[a]
Employee			
Gender			
Male	14	15	29
Female	1	0	1
Total	15	15	30[a]
Other			
Gender			
Male	2	3	5
Total	2	3	5
Total			
Gender			
Male	35	62	97
Female	2	1	3
Total	37	63	100

Note: [a] Three respondents (one manager and two employees) did not answer the item regarding company size; thus, the numbers in Table I are not completely consistent with the numbers in Section 4.1

Table I.
Demographic profiles of respondents

employees, and 37 respondents worked in large network companies with more than 100 employees (three respondents did not answer the item regarding company size). Based on the use of hidden identity in the electronic survey, we lack information regarding how many of the 137 network companies the respondents actually represented. However, 29 respondents were ICT safety and security managers (information security managers), 11 from large companies and 18 from smaller companies. Due to the fact that each company only has one ICT safety and security manager, at least 29 companies are represented in the data material and most likely more.

The mean value on the total scale score for the safety and security management scale was 18.83, the minimum possible value was 5 and the maximum possible value was 25. This means that the respondents agreed to most statements, and the majority of respondents viewed management commitment to ICT safety and security in their organization as high. The results are shown in Figure 1.

Table II presents the distribution of the respondents' scores on the individual items of the awareness creation and training scale.

The distribution of the respondents' scores on the individual items of the awareness creation and training scale suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had implemented training sessions in ICT safety and security whenever their ICT systems were updated and altered; however, a large percentage of the respondents answered "Neither disagree nor agree" (43.1 per cent)

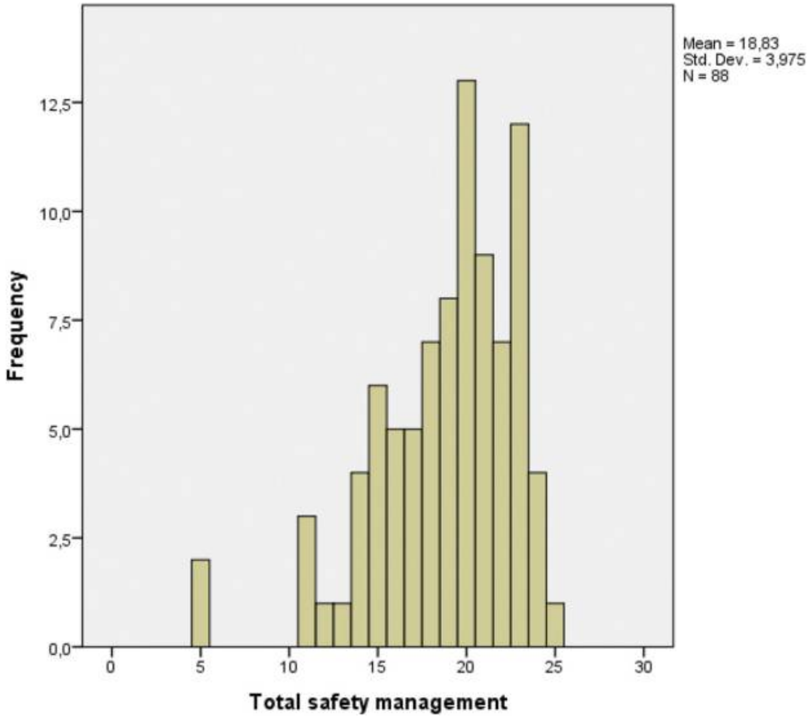

Figure 1.
Total scores on the safety and security management scale (calculated by adding up the scores from the five items that make up the scale)

on this item. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary a lot between the companies. In all, 54.9 per cent answered negatively[8] on the item regarding use of face-to-face presentations of information about ICT safety and security, and 76.7 per cent answered negatively on the item regarding use of informational videos on ICT safety and security.

4.2 Correlation

The relationship between management commitment to ICT safety and security (as measured by the total safety and security management scale) and implementation of awareness creation and training measures (as measured by the total awareness creation and training scale) in the network companies was investigated using Pearson product-moment correlation coefficient. Before this statistical analysis could be performed on the data set, the total scale scores for the two scales needed to be calculated by adding up the scores from the items that made up each scale (Pallant, 2010). The correlation analysis revealed a large positive correlation between the two variables "management commitment" and "awareness creation and training", $r = 0.641$, $n = 81$[9]. There was a strong, positive relationship[10] between the variables, and high levels of management commitment were associated with high levels of awareness creation and training.

Table II.
Distribution of scores on item 1-6 within the awareness creation and training scale

	Distribution of scores on items (in percentage)					
	Item 1: *"New employees receive thorough training in the organization's ICT safety and security rules (included in the organization's ICT safety and security policy and safety and security instructions)"*	Item 2: *"Training sessions in ICT safety and security for managers and employees are conducted whenever the ICT systems are updated or altered"*	Item 3: *"Awareness campaigns about ICT safety and security are often*[a] *held in my organization"*	Item 4: *"In my organization e-mails containing information about ICT safety and security are often distributed to raise employee awareness"*	Item 5: *"In my organization formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness"*	Item 6: *"In my organization informational videos on ICT safety and security are often showed to raise employee awareness"*
Strongly disagree	3.9 ($N = 4$)	4.9 ($N = 5$)	4.9 ($N = 5$)	7.8 ($N = 8$)	12.7 ($N = 13$)	23.3 ($N = 24$)
Disagree	9.7 ($N = 10$)	16.7 ($N = 17$)	27.2 ($N = 28$)	23.5 ($N = 24$)	42.2 ($N = 43$)	53.4 ($N = 55$)
Neither disagree nor agree	26.2 ($N = 27$)	43.1 ($N = 44$)	35.0 ($N = 36$)	35.3 ($N = 36$)	33.3 ($N = 34$)	18.4 ($N = 19$)
Agree	46.6 ($N = 48$)	28.4 ($N = 29$)	27.2 ($N = 28$)	25.5 ($N = 26$)	9.8 ($N = 10$)	3.9 ($N = 4$)
Strongly agree	10.7 ($N = 11$)	3.9 ($N = 4$)	4.9 ($N = 5$)	6.9 ($N = 7$)	1.0 ($N = 1$)	0.0 ($N = 0$)
Not relevant	0 ($N = 0$)	1.0 ($N = 1$)	0.0 ($N = 0$)	1.0 ($N = 1$)	1.0 ($N = 1$)	1.0 ($N = 1$)
Don't know	2.9 ($N = 3$)	2.0 ($N = 2$)	1.0 ($N = 1$)	0.0 ($N = 0$)	0.0 ($N = 0$)	0.0 ($N = 0$)
Total	103	102	103	102	102	103

Note: [a] In the awareness creation and training scale, the word "often" was defined as "at least once a year"; the respondents were informed of this in the scale's text information

5. Discussion

The "Cyber Security Strategy for Norway" (Regjeringen, 2012) from 2012 concluded that the lack of awareness concerning ICT safety and security constitutes a high and increasing risk. In many cases, the owners of critical infrastructure have limited knowledge and awareness about vulnerabilities, the interdependencies of critical infrastructures and what the individual enterprise must do to protect the infrastructure. The complexity of the process control systems, together with an increase in the number of attacks on ICT systems, demands a large effort to create awareness of the threats, to provide information about safety and security measures and to influence positive attitudes.

Studies of safety have suggested that management involvement is important for the safety work within companies. ICT safety and security law in Norway places responsibility for ICT safety and security on the management and the boards. The contingency planning regulations for the Norwegian electric power supply sector also emphasize that contingency planning (which includes ICT safety and security) is the responsibility of the top managers in the organizations, and the authorities expect the top management to convey the importance of and follow-up on safety and security within their organization. If the management is engaged, it will be aware of the need for information security measures to comply with the laws and assure that security measures are implemented (Hagen and Albrechtsen, 2009a).

The results from our survey showed a strong relationship between management commitment to ICT safety and security and the implementation of awareness creation and training measures for ICT safety and security in the network companies. High levels of management commitment were associated with high levels of awareness creation and training. These findings correspond well with results from former studies (Johnson, 2006; Hagen *et al.*, 2008; Hagen and Albrechtsen, 2009a).

According to Hagen and Albrechtsen's (2009a) comparative study of regulation of information security and the impact on top management commitment in the electric power supply sector versus the finance sector in Norway, a larger number of electric power supply companies reported incidents typically caused by insiders (e.g. abuse of ICT systems, unintentional use violating security, etc.) compared with financial companies. The researchers found that higher organizational security awareness corresponded with less exposure to insider threats. The results of the study also showed that high management engagement corresponded with a high degree of adopted security measures and a lower degree of insider incidents. According to our interviews with representatives from NVE, a high threshold for acknowledging the risk of insider incidents exists in the network companies. The companies might take for granted that "this does not happen in our company", which can affect their awareness.

During our observation studies at an ICT safety and security conference for companies within the Norwegian electric power supply sector in 2011, we observed a representative from one of the network companies asking the representative from NorCERT if the ICT systems in the Norwegian electric power supply sector were considered a high target for cyber attacks. The representative from NorCERT answered that the Norwegian Police Security Service (PST) did not assign a high threat level to the possibility of cyber attacks on Norwegian ICT systems, but they had observed an increasing amount of Internet espionage. According to several of the participants at the conference, it was hard to get money for ICT safety and security measures from the top management when the authorities did not consider the threat level as high.

On the other hand, our observation studies were carried out in 2011, and according to PST's annual threat assessment for 2012, there *is* a danger that foreign intelligence services' computer and Internet-based intelligence activity could more severely affect Norwegian intelligence targets. A report from 2012 on terror toward the US electrical grid concluded that a few, well-informed persons may be able to blackout large areas over a long period, with devastating and life-threatening consequences. According to NVE, this threat is just as great for Norway as for the USA (Teknisk Ukeblad, 2012). And according to The Norwegian Intelligence Service's (Etterretningstjenesten) open security threat assessment from February 2013 (FOCUS, 2013), cyber terror is now one of the main threats to national security. As previously mentioned, there are also large ICT safety and security challenges related to the implementation of AMI.

According to our interviewees from NVE, they had the impression that it was easier to get the network companies to implement technological and technical–administrative measures than to achieve management commitment to and create awareness about ICT safety and security within the companies. As previously mentioned, a possible explanation for this may be that when formal management systems (i.e. policies, procedures and tools) are in place, these measures may be taken for granted and accepted as contributors to an adequate security level. However, contrary to the results from our interviews and observation studies, the majority of respondents in our survey viewed management commitment to ICT safety and security in their organization as high. One possible explanation for this discrepancy may be that on subjective assessments regarding their own company's performance, respondents are often inclined to assess themselves positively. Sometimes it may also be difficult to answer negatively on questions concerning one's immediate manager (Hagen *et al.*, 2008).

Of the awareness creation and training measures listed in our survey, the most implemented was training in ICT safety and security for new employees. Some network companies had also implemented training sessions in ICT safety and security whenever their ICT systems were updated and altered; however, a large percentage of the respondents answered "Neither disagree nor agree" on this item, which might indicate that these types of training sessions were not conducted on a regular basis.

According to Albrechtsen and Hovden (2009), both the ICT safety and security managers and end-users of ICT systems who were interviewed in their study agreed that end-users often do not have the knowledge and skills needed for safe and secure behavior. Both groups believed this shortcoming to be the result of insufficient training. Users of ICT systems often do not realize the benefits of information security, and consider practicality and efficiency as far more important for their work. Both the interviewed managers and end-users also agreed that the best measures to raise awareness about ICT safety and security were interactive, face-to-face measures, for example personal meetings or presentations. However, this type of measure was also among the least frequently used approaches by the companies in the study. Formal one-way communication methods, such as information material and electronic information (e.g. screen savers, e-mail messages and leaflets), were extensively used because these measures are simple and cheap. The problem with these types of measures was that users often lacked the motivation and awareness to obtain the knowledge in this information, in addition to being bombarded with other types of information.

Similar results were found in our survey. In all, 54.9 per cent of the respondents answered negatively ("Strongly disagree" or "Disagree") on the statement: "In my organization formal face-to-face presentations of information about ICT safety and security are often held to raise employee awareness", only 10.8 per cent of the respondents answered positively ("Strongly agree" or "Agree") and 33.3 per cent answered "Neither disagree nor agree"[11].

According to Albrechtsen and Hagen (2009), employee participation is valuable for measures influencing user performance as well as for other parts of information security management. Practical learning (through interaction), rather than formal education, is likely to be the most effective way to improve knowledge on how to act safely and securely. Thomson and von Solms (1998) argued that social psychological principles needed to be introduced to improve the effectiveness of security awareness programs. The use of role-playing exercises and the use of examples related to the employee's own work situation were suggested as good techniques to achieve information security awareness among users of ICT systems. Use of e-learning can be another way to strengthen individual security awareness and behavior. A study by Hagen and Albrechtsen (2009b) discusses the effects of a computer-based security training program (using e-learning software) which was introduced in a multinational commercial organization in 2008. The study documented significant improvements in information security knowledge, awareness and behavior of the employees who participated in the training program.

However, these types of awareness creating and training measures are often resource-demanding because they must be repeated to be effective. Removing employees from their work during presentations, meetings and training sessions can also reduce the production capacity of the company. This may be a reason for why these types of measures are used to a lesser extent than formal one-way measures, even though studies have shown that they are considered better and more effective for raising awareness about ICT safety and security (Hagen *et al.*, 2008; Albrechtsen and Hovden, 2009).

6. Conclusion

The results from our survey among managers and employees in Norwegian electric power supply network companies showed a strong relationship between management commitment to and the implementation of awareness creation and training measures for ICT safety and security in the companies. High levels of management commitment were associated with high levels of awareness creation and training. These findings correspond well with results from former studies (Johnson, 2006; Hagen *et al.*, 2008; Hagen and Albrechtsen, 2009a).

The survey data showed that the majority of respondents viewed management commitment to ICT safety and security in their organization as high. However, contrary to this, results from our interviews with representatives from the authorities and observation studies at ICT safety and security conferences indicated that it is easier to get the network companies to implement technological and technical–administrative measures than to achieve management commitment to and create awareness about ICT safety and security within the companies.

Furthermore, the results from our survey suggested that the majority of the network companies had implemented training in ICT safety and security for new employees. Some network companies had also implemented training sessions whenever their ICT systems were updated and altered; however, our results indicated that these types of training sessions were not conducted on a regular basis. The use of awareness campaigns and distribution of e-mails containing information about ICT safety and security seemed to vary a lot between the companies. Interactive face-to-face presentations of information about ICT safety and security did not seem to be used as a measure to raise employee awareness within most of the network companies, even though former research has found that interactive measures are often viewed as the best measures to raise awareness about ICT safety and security (Hagen *et al.*, 2008; Albrechtsen and Hovden, 2009). Other measures involving employee participation and practical learning through interaction, for example e-learning or role-playing exercises, have also been shown to improve knowledge and awareness about how to act safely and securely. Our current survey did not include items regarding the use of these types of measures within the Norwegian network companies; however, this would be an interesting topic for further research.

Notes

1. A number of different terms are commonly used when discussing ICT safety and security and threats to ICT systems: information security, IT safety and security, computer safety, computer crime, data safety, cyber safety, cyber threats, cyber crime, cyber terror, logical threats, etc. In this article, we mainly use the term ICT safety and security, but different terms will be used when referencing to other research studies. In the area of risk research, it is traditional to distinguish between the terms safety and security, and the meaning of the terms can vary considerably from one context to another. According to Piètre-Cambacédès and Chaudet (2010), two relevant and representative distinctions can be identified (the SEMA referential framework). The first is the system versus environment distinction, where security is concerned with the risks originating from the environment and potentially affecting the system, whereas safety deals with the risks arising from the system and potentially affecting the environment. The second is the malicious versus accidental distinction, where security typically addresses malicious (intentional) risks, while safety addresses purely accidental (unintentional) risks (p. 59).
2. An infrastructure is critical if its failure would lead to unacceptable human or economic consequences, and would impact societies' capabilities of rescue, response and recovery. This links the notion of critical infrastructures closely to the concept of societal safety. Societal safety can be defined as "society's ability to maintain critical social functions, to protect the life and health of the citizens and to meet the citizens' basic requirements in a variety of stress situations" (Olsen *et al.*, 2007, p. 71).
3. SCADA systems help control and monitor utilities by gathering field data from sensors and instruments located at remote sites, transmitting and displaying these data at a central site and enabling engineers to send control commands to the field instruments (Patel and Sanyal, 2008, p. 398).
4. A user can be characterized as a person with legitimate access to the organization's information (and communication) systems (Albrechtsen, 2006), for example end-users, security officers, managers, designers (Besnard and Arief, 2004).
5. Before distributing the survey, we performed a pilot-test of the questionnaire to ensure that the instructions and scale items were clear. We sent the pilot to three respondents; one contingency planning manager, one ICT safety and security manager and one system control centre operator, and the questionnaire was adjusted according to feedback.
6. The Power Supply Preparedness Organisation (PSPO) prepares, establishes and maintains a structure to efficiently handle extraordinary situations in the power supply system. In 2012,

the PSPO included 197 organizations, and 137 of these can be classified as network companies (numbers were provided by NVE).

7. The survey was distributed to respondents in June 2012, and closed in September 2012.
8. "Strongly disagree" and "Disagree".
9. Correlation was significant at the 0.01 level (two-tailed).
10. The strength of the correlation is interpreted according to Cohen's guidelines from 1988: small correlation – $r = 0.10$ to 0.29, medium correlation – $r = 0.30$ to 0.49, large correlation – $r = 0.50$ to 1.0 (Pallant, 2010, p. 134).
11. $N = 102$.

References

Albrechtsen, E. (2006), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26 No. 4, pp. 276-289.

Albrechtsen, E. and Hagen, J.M. (2009), "Information security measures influencing user performance", in Martorell, S., Guedes Soares, C. and Barnett, J. (Eds), *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Taylor & Francis Group, London, pp. 2649-2656.

Albrechtsen, E. and Hovden, J. (2009), "The information security digital divide between information security managers and users", *Computers & Security*, Vol. 28 No. 4, pp. 76-490.

Antonsen, S. (2009), *Safety Culture: Theory, Method and Improvement*, Ashgate Publishing Limited, London.

Besnard, D. and Arief, B. (2004), "Computer security impaired by legitimate users", *Computers & Security*, Vol. 23 No. 3, pp. 253-264.

FOCUS (2013), "Annual assessment by the Norwegian intelligence service", available at: http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/0886-FOCUS-english-2013.pdf (accessed 15 August 2013).

Fricker, R.D. and Schonlau, M. (2002), "Advantages and disadvantages of internet research surveys: evidence from literature", *Field Methods*, Vol. 14 No. 4, pp. 347-367.

Hagen, J.M. (2009), "The human factor behind the security perimeter – evaluating the effectiveness of organizational information security measures and employees' contributions to security", PhD thesis no. 2009:874, Series of dissertations submitted to the Faculty of Mathematics and Natural Sciences, University of Oslo.

Hagen, J.M. and Albrechtsen, E. (2009a), "Regulation of information security and the impact on top management commitment: a comparative study of the energy supply sector and the finance sector", in Martorell, S., Guedes Soares, C. and Barnett, J. (Eds), *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Taylor & Francis Group, London, pp. 407-413.

Hagen, J.M. and Albrechtsen, E. (2009b), "Effects on employees' information security abilities by e-learning", *Information Management & Computer Security*, Vol. 17 No. 5, pp. 388-407.

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397.

Johnson, E.C. (2006), "Awareness training, security awareness: switch to a better programme", *Network Security*, Vol. 2, pp. 15-18.

Kundur, D., Feng, X., Liu, S., Zountos, T. and Butler-Purry, K.L. (2010), "Towards a framework for cyber attack impact analysis of the electric smart grid", Texas A&M University, Department of Electrical and Engineering.

Line, M.B. and Tøndel, I.A. (2012), "Information and communication technology: enabling and challenging critical infrastructure", in Hokstad, P., Utne, I.B. and Vatn, J. (Eds), *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis*, Springer-Verlag, London, pp. 147-225.

Olsen, O.E., Kruke, B.I. and Hovden, J. (2007), "Societal safety: concept, borders and dilemmas", *Journal of Contingencies and Crisis Management*, Vol. 15 No. 2, pp. 69-79.

Pallant, J. (2010), *SPSS Survival Manual – A Step by Step Guide to Data Analysis Using SPSS*, 4th ed., Open University Press, Berkshire, NY.

Patel, S.C. and Sanyal, P. (2008), "Securing SCADA systems", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 398-414.

Piètre-Cambacédès, L. and Chaudet, C. (2010), "The SEMA referential framework: avoiding ambiguities in the terms 'security' and 'safety'", *International Journal of Critical Infrastructure Protection*, Vol. 3, pp. 55-66.

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

Regjeringen (2012), "Cyber security strategy for Norway [Nasjonal strategi for informasjonssikkerhet]", available at: www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf (accessed 10 January 2013).

Rodal, S.K. (2001), "Sårbarhet i kraftforsyningens drifts- og styringssystemer [Vulnerabilities in the information systems of the electric power supply]", *FFI Report No*. 04278, available at: http://rapporter.ffi.no/rapporter/2001/04278.pdf (accessed 20 November 2012).

Silverman, D. (2006), *Interpreting Qualitative Data: Methods for Analyzing Talk, Text and Interaction*, Sage, London.

Siponen, M. (2000), "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8 No. 1, pp. 31-41.

Teknisk Ukeblad (2012), "Sikkerhet i kraftnettet– Kraftsystemet må ikke bli lavterskeltilbud for terrorister [Safety and security in the power grid – The electric power supply system must not become a low threshold service for terrorists]", available at: www.tu.no/energi/2012/12/14/-kraftsystemet-ma-ikke-bli-lavterskel-tilbud-for-terrorister (accessed 17 December 2012).

Thomson, M.E. and von Solms, R. (1998), "Information security awareness: educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

About the author

Ruth Østgaard Skotnes is a PhD candidate in Risk Management and Societal Safety at the University of Stavanger in Norway. Her current research focuses on challenges for safety and security management of network companies due to increased use of information and communication technology (ICT) in the electric power supply sector. She received her MSc degree in administration and organization theory from the University of Bergen in Norway. Ruth Østgaard Skotnes can be contacted at: ruth.skotnes@uis.no