Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security

T.O. Nævestad & S. Frislid Meyer
Institute of Transport Economics, Oslo, Norway

J. Hovland Honerud
University College of Southeast Norway, Norway

ABSTRACT: The aims of the present study are to 1) develop and test a scale measuring organizational information security culture, and 2) examine its relationships to other aspects of information security. The study focuses on an organization providing critical infrastructure. We developed the scale by conducting qualitative interviews (N = 22) and three focus groups (N = 15) in an organization providing critical infrastructure, and by reviewing previous research on culture in organisations. Based on our literature review and the interviews, we chose to measure organizational information security culture by reformulating one of the few existing general organizational safety culture questionnaires. We first tested the questionnaire in a small pilot survey, and then conducted a questionnaire survey (N = 323) including all departments in the organization. Our examination of the factor structure of the scale indicated two factors. Regression analyses indicate that our adapted GAIN-scale, measuring organizational information security culture is the most important variable influencing information security behavior in the model.

1 INTRODUCTION

1.1 *Background*

Information security is often defined as protection against breaches of confidentiality, integrity and accessibility. This applies to information that is oral, written or electronic. Confidentiality refers to ensuring that only those who are authorised to access information, accesses it. Integrity refers to protecting the accuracy and entirety of information and processing methods. Accessibility refers to ensuring that authorised users have access to the information and associated equipments when necessary (Report to the Storting 29. 2011–2012).

Ruighaver et al (2007) assert that it was not until the start of the century that scholars began to recognise the importance of organizational information security culture for information systems security in organisations. The importance of culture for security and safety has also gained recognition in the Norwegian society in recent years. One of the most important conclusions of the report of the investigation commission following the terrorist attack in Oslo and Utøya, July 22. 2011 was that future efforts to secure sensitive objects (e.g. people and critical infrastructure) and information should focus on culture, focusing especially on the acknowledgement of risk and leadership.

The study organization is a provider of critical infrastructure in Norway. As a provider of critical infrastructure, the study organization is obliged to follow the requirements of the Security Act ("Sikkerhetsloven") when it comes to preventive safety work, which includes safety analyses, securing objects, information security and safety drill. Based on these requirements, the study organization decided to map and analyse their own organizational security culture. Critical infrastructure means the facilities and systems that are completely necessary to maintain society's critical functions, which in turn meet society's basic needs and respond to the population's need for a perception of safety (NOU 2006).

1.2 *Aims*

The aims of the present study are to 1) develop and test a scale measuring organizational information security culture and 2) examine its relationships to other aspects of information security.

1.3 *Research on culture in organisations*

1.3.1 *Organisational information security culture*

Although Ruighaver et al. (2007) note that the organisational security culture concept has gained recognition, they also underline that there is

lacking consensus when it comes to how the concept should be defined and conceptualized (cf. Chia et al., 2002). Additionally, they also assert that in spite a large amount of research on organisational security and how it should be improved, this research only focus on certain aspects of security and not how these aspects can be analysed as part of a larger organisational culture.

Based on this understanding, Ruighaver et al. (2007) choose to draw on organisational culture research in their analysis of security culture. This approach is similar to that applied by scholars studying organisational safety culture, who analyse safety culture as a focused and safety relevant aspect of the larger organisational culture (e.g. Hale, 2000, Haukelid, 2008, Antonsen, 2009). Based on this, we may also analyse security culture as "security relevant" aspects of the larger organisational culture, define and conceptualising using models of organisational culture (e.g. Schein, 2004). In this paper, we suggest that the research on information security culture could learn from the research on safety culture. Nosworthy (2000) asserts for instance that one of the key challenges of information security culture implementation is how to educate the people of the organization to successfully implement the requirements of the information security policy. A lot of effort has been put in to understand this in safety culture research, discerning between formal (structure; safety management system; procedures, training, routines etc.) aspects of safety and informal aspects (culture) (Antonsen, 2009). Additionally, Knapp et al. (2006), depict the top management support as a significant predictor of an organization's security culture and level of policy enforcement. This also reflects a key finding in organizational safety culture and safety culture research, and thus it is relevant to also draw on the knowledge gained in these research fields.

1.3.2 *Organisational culture*

The influential scholar Schein defines organizational culture as: "(...) a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems." (Schein 1992: 12). According to Guldenmund (2000: 222–225), organizational culture has the following characteristics: 1. It is a construct in the sense that it is an abstract, not a concrete concept, 2. It is relatively stable, 3. It has multiple dimensionality, in the sense that it can be described in many different ways, 4. It is shared by groups of people, 5. It consists of various aspects, which means that several different cultures can be identified within organizations, depending on the issue at hand, 6. It constitutes practices, 7. It is functional. Guldenmund describes organizational culture in the following manner: "Overall, organisational culture is a relatively stable, multidimensional, holistic construct shared by (groups of) organisational members that supplies a frame of reference and which gives meaning to and/or is typically revealed in certain practices." (Guldenmund 2000: 225).

As the research on organizational safety culture seems to have been through many of the challenges that the organizational security culture research now is facing, we draw on the experiences of the former, e.g. when it comes to analyzing security culture as a focused aspect of organizational culture.

1.3.3 *Organizational safety culture*

Even though the concept of safety culture has become popular since it first was introduced in the wake of the Chernobyl accident in 1986, it is not well understood (Reason, 1997). Safety culture scholars may disagree on a range of different issues, but they seem to agree that the research on safety culture and its relationship with safety is fragmented and unsystematic (e.g., Cox & Flin, 199, Pidgeon, 1998, Hopkins, 2006, Guldenmund, 2007; Choudry et al., 2007; Glendon, 2008). In spite of this disagreement, most scholars seem to agree that safety culture refers to shared and safety relevant ways of thinking or acting that are (re) created through the joint negotiation of people in social settings (Nævestad, 2010a), and as noted as safety-relevant aspects of organisational culture (Hale 2000). The element of safety culture that can be measured is often referred to as safety climate. Thus, safety climate can be conceived of as "snapshots", or manifestations of safety culture (Cox & Flin, 1998). Quantitative measurements of safety culture can provide leading indicators of safety and consequently offer predictive assessments that enable safety improvements without having to wait for accidents or incidents to happen (Antonsen, 2009). Senior management commitment to safety is the most studied and best-documented characteristic of a good safety culture, independent of sector (Flin et al. 2000; Guldenmund 2000).

2 METHOD

Our methodological approach is based on a literature review conducted in 2012, interviews (N = 22) and focus groups (N = 15) in 2014 and survey in 2014 (N = 323).

2.1 *Interviews and focus groups*

We started with the qualitative part of the study before conducting the quantitative survey, so that

we could form a picture of key issues concerning safety and security work at the study organisation. This is important because we had to adapt the security culture questionnaire, and because it gave us the opportunity to add questions that are central to safety and security work at the study organisation to the questionnaire. We have conducted 22 in-depth interviews, primarily managers, and one group interview with 3 respondents. Focus groups, primarily employees: 2 focus groups with a total of 12 persons. This makes a total of 37 in-depth interviews.

We used a semi-structured and relatively open interview guide based on the safety and security culture topics from the safety culture index. Our point of departure was topics related to information security and the protection of critical infrastructure. The interview guide had to be open so that we could depend on the interviewees' understanding of how different features of the organisation culture in the study organisation have had and can have consequences for safety and security.

The interviews were built up around the following main topics: 1) In general about the department's and respondent's responsibility and roles, 2) Security focus, and relation to safety in the information security, HSE safety, deliverance reliability, 3) Organizational framework, management lines and communication, 4) Safety culture issues; safety, training, expertise, procedures, etc.

2.2 *Literature review*

The literature review was originally conducted as part of another project (cf. Nævestad & Bjørnskau 2012), but we nevertheless draw on it in the present study, as it also was relevant to the present study, and as our choice of safety culture scale for the present study was based on it. This is based on our mentioned ambition to learn from the safety culture literature when measuring and understanding organisational information security culture.

In this review, we conducted literature searches for articles and reports that document experiences with different safety culture measurement tools. We conducted searches through two key scientific databases, "Science direct" and the ISI web of science. A search for "Safety climate" in "abstract/title/key words", "safety climate scale" and "safety climate questionnaire" in scientific publications (primarily referenced journal articles, but also some books) for all years, gave everything in all 249 results. The next search we made from the scientific database "ISI-Web of Knowledge". Here we searched for articles with "safety climate" in title or subject, for all years, and received 458 hits.

The scales were reviewed according to the following criteria, whether: 1) they are based on a solid scientific approach (e.g. based on previous research and existing theory, have been validated in several studies), 2) they are universal, 3) they are) user-friendly; do not include too many themes and questions, which are understandable for people who are not researchers and 4) A key criterion has been that the themes and the items in the scales are in accordance with the key results of the interviews and focus groups. Our review resulted in 11 scales that we perceived as relevant enough to be evaluated systematically against these criteria.

In the present study, we choose to reformulate one of the few existing universal organizational safety culture scales, the GAIN-scale for safety culture, into an organizational security culture scale. The GAIN scale was chosen first, as our previous literature review, conclude that this is one of very few universal safety culture surveys (Nævestad & Bjørnskau, 2012). Thus, the wording of each item can be adapted to different sectors (and presumably also to security) without obviously altering the particular aspect which that item measures. Thus, the scale has the potential to be developed as a generic measure.

Second, the scale was chosen, as it is founded on a relatively solid scientific foundation. It must be noted that we ended up recommending another scale in the above mentioned 2012 review. In this review, we chose the NOSAQ-50 scale (Kines et al., 2011), over the GAIN-scales (GAIN, 2001), as this had been subjected to a more systematic literature review. We have however conducted several studies using the GAIN scale since 2012 (e.g. Nævestad & Bjørnskau, 2014, Nævestad et al., 2017, Nævestad, 2017), subjecting it to exploratory and confirmatory factor analyses, and we have also analyzed the relationship between the scale and safety outcomes (e.g. Nævestad, 2017). The scale has also been used to study and compare safety culture in different transport sectors like road, rail, helicopter and aviation (Bjørnskau & Longva, 2009).

Third, the scale was chosen, as it is relatively easy to use. The GAIN-scale has for instance considerably shorter than the NOSAQ 50; it has only half the items. Additionally, the questions are relatively short, and it is relatively easy to change and adapt the wording to information security culture.

2.3 *Survey*

2.3.1 *Sample characteristics*

A total of 323 individuals responded to the survey, from 11 different departments, giving a response rate of 56%. More than 90 per cent of the respondents are permanent employees and seven per cent are hired consultants. We also see that seven per cent are section or department managers. It should also be mentioned that more than 50% those who responded to the survey had been employed by the

study organisation for five years or less. This is a relatively high percentage. It explains that more than 40 per cent of the respondents have been employed by 3–5 other business in their working life before the study organisation. Almost a quarter of those who responded have however been employed for more than 20 years. This is an approximate reflection of the actual distribution in the study organisation, but respondents with the shortest seniority are overrepresented. 56 per cent of the respondents are above the age of 46. This is interesting, considering that around half have seniority of five years or less. 61 per cent of the respondents are men and 66 per cent have graduated from university/university college.

2.3.2 *Pilot survey*

As we developed several new questions in the survey which had never been tested before, we conducted a small pilot study (N = 12) directed at personnel in the study organisation to obtain feedback and assess how the questions worked. In the pilot study we received some useful feedback, including that we should use the term "my immediate supervisor" rather than "my department manager" in the survey on safety culture and information security culture

2.3.3 *Survey topics*

The survey contains mainly questions about ten topics. It first contains a set of background questions (e.g. gender, age, education, experience, level) that were sent to all respondents. In addition, three short indexes follow with questions about three different types of security related to information security, HSE safety and deliverance reliability. The questions are identical and have the same scale so that we can directly compare the meanings of the three forms of safety and security in the study organisation. Furthermore, the questionnaire 13 contains questions about attitudes and behaviour regarding information security culture.

2.3.3.1 Background variables

The survey also includes questions on demographic background variables and various performance targets related to safety. The background variables include information on: 1) gender, 2) age, 3) education, 4) seniority, 5) employment in other businesses, 6) level in the organization and 7) employment status in the organization (permanent, hired). These background variables are only presented at the enterprise level.

2.3.3.2 The GAIN scale

Global Aviation Information Network (GAIN) is a voluntary association of airlines, manufacturers, trade unions, governments and other organisations in aviation. The GAIN questionnaire contains 24 questions concerning (we excluded one of the original questions, because of the wording):

1. Management's attitude to and focus on safety:

Man 1: My immediate supervisor discovers employees who fail to take sufficient considerations to information security in their work
Man 2: My immediate supervisor often praises employees for maintaining information security
Man 3: My immediate supervisor is aware of the most important information security issues in the company
Man 4: My immediate supervisor often discusses information security issues with the employees
Man 5: My immediate supervisor is personally involved in activities to improve information security
Man 6: My immediate supervisor postpones tasks/activities if information security is not sufficiently ensured
Man 7: My immediate supervisor considers information security to be very important in all tasks and activities
Man 8: My immediate supervisor does everything he/she can do to avoid breaches of information security

2. Employees' attitudes to and focus on safety:

Emp 1; My colleagues do everything they can to avoid breaches of information security
Emp 2: Employees encourage one another to safeguard information security
Emp 3: Employees usually report all breaches and irregularities related to information security that they experience at work

3. Reporting culture and reactions to incident reporting:

Rep 1: Those who pursue breaches of information security in the business attempt to find the real causes rather than just blaming the employees
Rep 2: There are routines and procedures at my workplace so that I may report information security-related breaches or irregularities
Rep 3: After a breach of information security, measures are implemented to prevent this from happening again
Rep 4: All irregularities and information security issues that are reported are remedied in a short time
Rep 5: Everyone has plenty of opportunities to forward suggestions related to information security

4. Safety training and education:

Tra 1: Employees in my company are provided with adequate training in the secure use of ICT systems (e.g. e-mail, storage, encryption)
Tra 2: All new employees are provided with adequate training for tasks and the secure use of ICT systems (e.g. e-mail, storage, encryption)
Tra 3: Everyone is provided with sufficient feedback on how the enterprise is performing with regard to information security

Tra 4: Everyone is informed of any changes that may impact information security

5. General questions concerning safety in the organization in question:

Gen 1: There are procedures that must be followed in the event of an emergency situation in my workplace
Gen 2: Information security in my business is better that in other businesses
Gen 3: Regular security audits are carried out
Gen 4:_Information security is generally well taken care of at my workplace

Respondents can rate the questions from 1 (totally disagree) to 5 (totally agree). Thus, a safety culture index with a minimum value of 24 (1 × 24) and a maximum value of 120 (5 × 24) can be compared across companies and sectors. According to GAIN (2001), organizations with a score of 93–125 points on the safety culture index have a positive safety culture, 59–92 indicates a bureaucratic safety culture and 25–58 indicates a poor safety culture.

2.3.3.3 Questions about information security
Based on the interviews (and literature review of organizational security culture scales, e.g. SjekkIT developed by NTNU and Sintef for the Norwegian National Security Authority (NSM), we also included 22 additional questions about information security in the organisation. These were themes representing special information security challenges in the organization.

3 RESULTS FROM INTERVIEWS AND FOCUS GROUPS

In the interviews, we discussed organisational security management with the key managers, and based on the interviews, we found that they perceived the five GAIN themes as important and relevant. Management and employee commitment for safety was perceived as key. The organisation had also developed a reporting system covering information security, and they were also engaged in several initiatives to educate employees in information security issues.

Based on the interviews and focus groups, we also developed 22 survey questions, reflecting the most important information security challenges in the organisaion. We included several untested questions among the 22, and we experienced that nine of these did not work because some of them had relatively large shares of "neither/nor" responses. The 13 questions on information security we ended up with after removing the 9 that did not work (of 22 questions in total) may be divided into the following topics. We unfortunately don't have the opportunity to present all here due to space considerations, but will nevertheless reproduce the topics and questions, as they are an important result of our qualitative surveys:

1. Knowledge/attitudes—information security:

We constructed an index for knowledge of and attitudes to information security with five questions. All of the questions have five values, such that the minimum value for the index is 5 and the maximum value is 25 (Cronbach's Alpha = 0.740).

In my work, I have a clear understanding of what the term information security means.
I have a clear understanding of what entails a breach of information security in my business.
I feel that I have adequate knowledge on the secure use of ICT systems (e.g. e-mail, storage, encryption)
All unfamiliar persons at the workplace are noticed, and one investigates what they are doing there.
When I am asked for information, I always think carefully about whether the information can be used for other purposes than originally intended.

2. Security assessment—PC and cell phone:

My cell phone contains sensitive information.
If I'm working on a PC from home, information security is just as high as it is at work

3. Classified information and accessibility.

We created an index of the following three questions on classified information (Cronbach's Alpha was 0.721):

I am well aware of which type of information that is sensitive and classified
I am well aware of who has access to various types of classified information
I take precautions when I come into contact with sensitive and classified information

The respondents were also asked to consider the following statement: "Considerations to information security (for example passwords to log on) impede my work".

4 RESULTS FROM THE QUANTITATIVE SURVEY

4.1 *Clear understanding of information security?*

The questionnaire that measures information security culture is based on the GAIN safety culture index, where the word "safety" is replaced by "information security." The questionnaire opened with definitions of information security and related sub-concepts.

4.2 *Organisational information security culture index*

We have combined the 24 statements with five response options on the five different aspects of information security in an information security culture index. The indexes for the departments correspond to the average scores for the respondents. Since we have removed a statement from the GAIN index, the minimum score will be 24 (24 × 1) and the maximum score will be 120 (24 × 5). Cronbach's Alpha for the 24 questions in the index is 0.913, which means very good agreement between the questions and that the index is very good.

Factor 1: Information security management and commitment	**Factor loadings**
Man 4: My immediate supervisor often discusses information security issues with the employees	0.774
Tra 4: Information security is generally well taken care of at my workplace	0.745
Man 7: My immediate supervisor considers information security to be very important in all tasks and activities	0.743
Man 6: My immediate supervisor postpones tasks/activities if information security is not sufficiently ensured	0.735
Man 8: My immediate supervisor does everything he/she can do to avoid breaches of information security	0.733
Rep 3: After a breach of information security, measures are implemented to prevent this from happening again	0.729
Man 3: My immediate supervisor is aware of the most important information security issues in the company	0.691
Man 5: My immediate supervisor is personally involved in activities to improve information security	0.678
Rep 4: All irregularities and information security issues that are reported are remedied in a short time	0.654
Emp 2: Employees encourage one another to safeguard information security	0.644
Man 2: My immediate supervisor often praises employees for maintaining information security	0.639
Emp 3: Employees usually report all breaches and irregularities related to information security that they experience at work	0.634
Gen 3: Regular security audits are carried out	0.615
Rep1: Those who pursue breaches of information security in the business attempt to find the real causes rather than just blaming the employees	0.598
Man 1: My immediate supervisor discovers employees who fail to take sufficient considerations to information security in their work	0.593
Emp 1: My colleagues do everything they can to avoid breaches of information security	0.591
Rep 5: Everyone has plenty of opportunities to forward suggestions related to information security	0.572
Gen 2: Information security in my business is better that in other businesses	0.548
Rep 2: There are routines and procedures at my workplace so that I may report information security-related breaches or irregularities	0.534
Tra 1: There are procedures that must be followed in the event of an emergency situation in my workplace	0.508

Factor 2: Information security training	**Loadings**
Tra 2: All new employees are provided with adequate training for tasks and the secure use of ICT systems (e.g. e-mail, storage, encryption)	0.691
Tra 1: Employees in my company are provided with adequate training in the secure use of ICT systems (e.g. e-mail, storage, encryption)	0.629
Tra 3: Everyone is provided with sufficient feedback on how the enterprise is performing with regard to information security	0.562
Tra 4: Everyone is informed of any changes that may impact information security	0.550

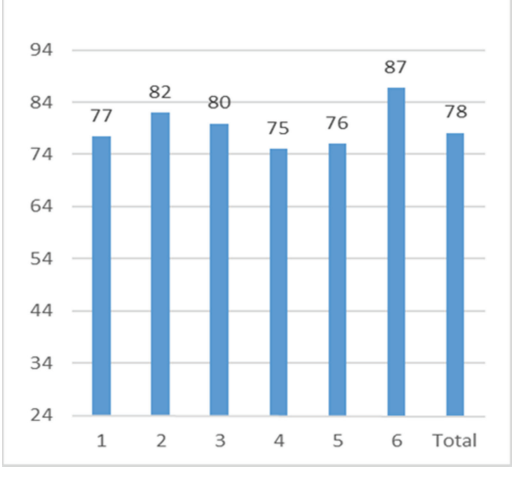

Figure 1. Mean scores on the GAIN index applied to organsiational information security culture. Departments in the study organisation. Minimum 24, maximum 120. (N = 249).

The figure shows that DEP 6 has the highest score and that DEP 4 has the lowest score. The difference between the highest and lowest score is more than 11 points. The differences between the departments are significant at the 1% level. We are careful of comparing the departments and in relation to the information security culture questions. The number of "neither/nor" responses indicate that the respondents are unwilling or incapable of considering the statements on the area, which may make it difficult to interpret the numbers. It also entails that respondents who have actually had an opinion are a minority for some of the questions. All in all, we therefore consider this index to be less robust than the others. This applies to all departments, except DEP 6.

The first topic in the index was "Immediate supervisor's attitude to and focus on information security." Here DEP 6 had the highest score, DEP 4 the lowest.

The second topic in the index is "Employees' attitude to and focus on information security." Once again DEP 6 had the highest score while DEP 1 had the lowest. The differences are significant at the 5% level. This should be interpreted in the light of DEP 1 having responsibility for following up such work, and is probably more critical in its assessment.

The third topic in the index is "Reporting culture and reactions to incident reporting." DEP 6 and DEP 2 had the highest scores, while DEP 4 and DEP 5 had the lowest. Differences were significant, of more than two points.

The fourth topic in the index is "Training in information security thinking." DEP 2 and DEP 6 had the highest scores, while DEP 1 had the lowest. The fifth topic in the index is "General information security issues." DEP 6 had the highest score, while DEP 1 had the lowest. The differences are significant at the 1% level.

4.2.1 *Exploratory factor analysis*

An Exploratory Factor Analysis (EFA) was conducted to examine the underlying factor structure of the 24 items in the sample. Although the original GAIN-scale for safety culture is comprised of five themes, we chose EFA as we apply it to a new topic; information security culture. Tests indicated that the items and the data were suitable for factor analysis. Bartlett's test of sphericity (approx. Chi-square) was 3380,834 ($p < 0.001$). The Kaiser–Meyer–Olkin's measure of sampling adequacy showed a value of 0.909. An unrotated principal component analysis (PCA) was used. We sat the cut off value of factor loadings equal to or above 0.40, as Matsunaga (2010) suggests that this perhaps is the lowest acceptable threshold on a conventional liberal-to-conservative continuum. Results showed five components with initial Eigenvalues higher than 1, which explained a total of 64.9% of the variance. The choice of the number of factors to retain was based on a combination of a) Eigenvalues, b) inspecting the scree plot for a bending point, c) inspecting the factor loadings in the component matrix, and d) conceptual and theoretical consideration. By inspecting the scree plot, a bend was relatively clearly identified between factor 5 and 6, indicating a five-factor solution. This is in line with the Eigenvalues. However, when looking at the factor loadings, we saw that all items loaded on the first component, while there were seven cross-loading. Four of these had lower factor loadings on the other factors than the first factor, and they were distributed on different factors. They were therefore kept in the first factor, with one exception. Three of the cross-loading items were all in the second factor, they had higher factor loadings in the second factor and they all concern security training. They were therefore attributed to a second factor. Additionally, one of the first mentioned cross-loading items had quite similar loadings in both factors (0.567 vs. 0.562), but as it matched the second conceptually, we attributed it to this factor.

Thus, based on our analysis of the factor loadings and a conceptual and theoretical consideration (the four latter items all concern information security training), we chose a two-factor solution, which explained a total of 50% of the variance, i.e. about 15% less than the three-factor solution.

4.2.2 *Regression analysis: What influences organisational information security scores?*

The information security culture scores vary according to conditions such as age, education and seniority, but we do not know which conditions that are most important to explain the variation in information security culture, or whether the effect we see from education is actually due to age or vice versa. We have conducted regression analyses to assess which conditions explain variation in the information security culture index.

We have used linear regression as the dependent variable is continuous. We add various independent variables in steps, so that we can assess their isolated effect on the dependent variables, i.e. when the values of the other variables remain unchanged. In this manner we can examine the effect of education controlled for age, for example.

We add the gender, age, education and seniority variables in the study organisation and department. We have converted the department variable to a dichotomous variable, i.e. with two values. The reason is that in regression analyses one cannot have independent variables that are at the nominal level, i.e. with values that are mutually exclusive, but which can't be ranked. The two values of the department

variable are 1) all other departments, 2) DEP 6. We have done this because DEP 6 had the highest score on the information security culture index.

We see that age contributes significantly and positively in 2; the older the respondents are, the better their information security culture score. In model 3 however, the age variable stops being significant, and that indicates that the age effect is actually due to it correlating with education. This means that younger respondents have higher education and a lower information security culture score and vice versa. Seniority does not make a significant contribution in any of the models.

Finally, we see that the department variable makes the strongest contribution in the regression analysis in Table 1. Belonging to DEP 6 predicts a positive score on the information security culture index. We already knew this, but in the regression analyses in Table 1 also show that this also applies when controlling for gender, age, education and seniority. We may therefore conclude that DEP 6's high score on the information security culture index is not due to underlying variables such as gender, age, education and seniority.

We see that the adjusted R^2 value, which indicates which proportion of the variation in the dependent variable that is explained by the independent variables significantly increasing in model 3 when education is included in the analyses, and that it increases by more than twice as much when department is included in model 5. The independent variables education and department explain 9.7% of the variation in the information security culture index.

4.3 *Regression analysis: What influences information security behaviour?*

We have conducted regression analyses to assess which conditions explain variation in the variable "I have never caused a breach of information security." This is a variable with five options from 1 (strongly disagree) to 5 (strongly agree). The overall "neither/nor" share is 26.3% for this question. What one answers here is probably to a certain extent dependent on whether one has a clear understanding of what information security is, or what it means for day to day work. The answer will also depend on how many opportunities one has to breach information security in one's work. We have used linear regression as the dependent variable is continuous. We add four independent variables in steps, so that we can assess their isolated effect on the dependent variables, i.e. when the values of the other variables remain unchanged. We add the gender, age and seniority variables in the study organisation and information security culture.

The table shows that seniority and information security culture contribute significantly to explain the variation in the variable "I have never caused a breach of information security." Both effects are positive. The positive effect of seniority means that

Table 1. Linear regression. Dependent variable: Organisational information security culture standardised beta coefficients.

Variable	1	2	3	4	5
Gender	–0,003	0,028	0,021	0,020	0,003
Age		**0,158****	0,105	0,076	0,034
Edu (Uni = 2)			**–0,185*****	**–0,157****	**–0,138****
Seniority				0,078	0,059
Department (DEP 6 = 2)					**0,244*****
Adj. R^2	–0.004	0.016	0.044	0.045	0,097

*p < 0,1; **p < 0,05; ***p < 0,01.

Table 2. Linear regression. Dependent variable: "I have never caused a breach of information security." Standardised beta coefficients.

Variable	Mod. 1	Mod. 2	Mod. 3	Mod. 4
Gender	–0,043	–0,042	–0,046	–0,051
Age		0,005	–0,070	–0,087
Seniority			0,159**	0,132*
Information security culture				0,192***
Adjusted R^2	–0.002	–0.006	0.010	0.041

*p < 0,1; **p < 0,05; ***p < 0,01.

the longer one has been employed by the study organisation, the higher the likelihood that one has not caused a breach of information security. This is perhaps somewhat unexpected, as one would assume that the longer one has been employed, the more opportunities (in terms of time) there have been to breach information security. It further means that there is reason to assume that the study organisation had scored somewhat higher on security culture if the distribution of respondents had corresponded to that in the organization: In the survey, 51 per cent of respondents had 0–5 years seniority, while in reality there are 38 per cent who have 0–5 years seniority in the study organisation. There is nevertheless no reason to believe that this possible skewness alters fundamental conclusions, as the difference is too small.

The effect of information security culture is however strongest, and this is the most important variable to explain variations in breaches of information security in the analyses. The higher the information security culture score is, the higher the likelihood that one has not caused a breach of information security.

We see that the adjusted R2 value, which indicates which proportion of the variation in the dependent variable that is explained by the independent variables, is negative in the two first models, but that it is at 1 and 4.1% in the last two. This happened when we included seniority and information security culture. These variables explain 4.1% of the variation in the variable "I have never caused a breach of information security".

5 CONCLUDING DISCUSSION

Learning from research on organizational culture and safety culture, we have adapted an organizational safety culture scale to measure organizational information security culture. Our examination of the factor structure of the scale indicated two factors. Regression analyses indicate that our adapted GAIN-scale, measuring organizational information security culture is the most important variable influencing information security behavior in the model.

REFERENCES

Antonsen, S. 2009. "The relationship between culture and safety on offshore supply vessels", *Safety Science*, Vol. 47. Issue 8, pp. 1118–1128.

Bjørnskau, Torkel og Frode Longva 2009. Sikkerhetskultur i transport. TØI rapport 1012/2009 Oslo: Transportøkonomisk institutt.

Chia P, Maynard S, Ruighaver AB. Understanding organizational security culture. In: *Sixth pacific Asia conference on information systems,* Tokyo, Japan; 2–3 September 2002.

Cox, S.J. & R. Flin (1998): "Safety Culture: Philopher's Stone or a Man of Straw?", *Work & Stress,* Vol 12, No 3 189.

Flin, R., K. Mearns, P. O'Connor & R. Bryden (2000): "Measuring safety climate: identifying the common features", *Safety Science,* Vol.34, 177–192.

GAIN (Global Aviation Network) 2001. Operator's Flight Safety Handbook, http://flightsafety.org/files/OFSH_english.pdf.

Guldenmund, F.W. (2000): "The Nature of Safety Culture: a Review of Theory and Research", *Safety Science*, vol. 34, 1–14.

Hale, A.(2000): "Editorial: Culture's Confusions", *Safety Science,* vol. 34, 1–14.

Haukelid, K. (2008): "Theories of (safety) culture revisited—An anthropological approach", *Safety Science*, Vol. 46/3, 413–426.

Kines, P.J. Lappalainen, K. Lyngby Mikkelsen, E. Olsen, A. Pousette, J. Tharaldsen, K. Tómasson & M. Törner (2011): Nordic safety climate questionnaire (NOSACQ-50): A new tool for diagnosing occupational safety climate, *International Journal of Industrial Ergonomics,* Vol. 41, pp. 634–646.

Knapp KJ, Marshall TE, Rainer RK, Ford FN. (2006) Information security: management's effect on culture and policy. *Information Management & Computer Security* 2006;14(1):24–36.

Nosworthy J. (2000) Implementing information security in the 21st Century—do you have the balancing factors? *Computers and Security;*19(4):337–47.

NOU (2006). Når sikkerhet er viktigst, Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.

Nævestad, T.-O. (2010a): *"Cultures, crises and campaigns: examining the role of safety culture in the management of hazards in a high-risk industry"*, Ph.D. dissertation, Centre for Technology, Innovation and Culture, Faculty of Social Sciences, University of Oslo.

Reason, J. (1997): *Managing the Risk of Organisational accidents,* Aldershot: Ashgate.

Ruighaver, A.B.S.B. Maynard, S. Chang (2007) Organisational security culture: Extending the end-user perspective, computers & security 26 (2007) 56–62.

Schein, E.H. (2004): *Organizational Culture and Leadership,* Third Edition, San Francisco: Jossey-Bass.

SjekkIT. Verktøy for å måle informasjonssikkerhetskultur utviklet av NTNU og Sintef for NSM.