Information & Computer Security

An empirical test of the perceived relationship between risk and the constituents severity and probability

Teodor Sommestad Henrik Karlzén Peter Nilsson Jonas Hallberg

Received 18 January 2016
Revised 18 January 2016
Accepted 9 March 2016

An empirical test of the perceived relationship between risk and the constituents severity and probability

Teodor Sommestad, Henrik Karlzén, Peter Nilsson and Jonas Hallberg
Swedish Defence Research Agency (FOI), Linköping, Sweden

Abstract

Purpose – In methods and manuals, the product of an information security incident's probability and severity is seen as a risk to manage. The purpose of the test described in this paper is to investigate if information security risk is perceived in this way, if decision-making style influences the perceived relationship between the three variables and if the level of information security expertise influences the relationship between the three variables.

Design/methodology/approach – Ten respondents assessed 105 potential information security incidents. Ratings of the associated risks were obtained independently from ratings of the probability and severity of the incidents. Decision-making style was measured using a scale inspired from the Cognitive Style Index; information security expertise was self-reported. Regression analysis was used to test the relationship between variables.

Findings – The ten respondents did not assess risk as the product of probability and severity, regardless of experience, expertise and decision-making style. The mean variance explained in risk ratings using an additive term is 54.0 or 38.4 per cent, depending on how risk is measured. When a multiplicative term was added, the mean variance only increased by 1.5 or 2.4 per cent. For most of the respondents, the contribution of the multiplicative term is statistically insignificant.

Practical Implications – The inability or unwillingness to see risk as a product of probability and severity suggests that procedural support (e.g. risk matrices) has a role to play in the risk assessment processes.

Originality/value – This study is the first to test if information security risk is assessed as an interaction between probability and severity using suitable scales and a within-subject design.

Keywords Risk perception, Information security risk assessment, Perceived probability, Perceived severity

Paper type Research paper

1. Introduction

It is widely accepted and uncontroversial to view information security in terms of risks. Information security risks are, in many of the most widely accepted definitions, assessed in terms of the *probability* that a threat will be realized and the *severity* of the consequences of a realized threat. For instance, a number of authorities and textbooks prescribe that information security risk is a combination of probability (in some contexts called likelihood or frequency) and severity (in some contexts called consequence, impact or magnitude) (NIST, 2012; ; Club de la Sécurité de l'Information Français, 2011; Karabacak and Sogukpinar, 2005; Lund *et al.*, 2011). The

Information & Computer Security
Vol. 24 No. 2, 2016
pp. 194-204

2056-4961
DOI 10.1108/ICS-01-2016-0004

decision-making literature agrees - risk is calculated as the product of the severity and the probability (Gordon and Loeb, 2002; Sommestad *et al.*, 2010; Blakley and Mcdermott, 2002). Thus, rational and balanced security decisions require that risk is assessed as the product of probability and severity. The rationale for this is clearest in the extreme cases – with no negative effect (severity zero), the probability should be irrelevant; with no possibility of happening (probability zero), the severity should be irrelevant. But it is also clear in between these extremes – if a bad thing is twice as likely or twice as severe as another bad thing, the expected costs will be twice as large.

The idea that risk is obtained from a multiplication of a bad event's probability and severity is well established. However, results from both information security research and other research areas suggest that people do not multiply in practice. For example, in the original formulation of the Protection Motivation Theory, it was proposed that an interaction of perceived vulnerability and perceived severity influenced behavioral intentions (Maddux and Rogers, 1983; Rogers, 1983). However, this interaction has been abandoned for a simpler additive model on empirical grounds – empirical data do not offer firm support of a multiplicative relationship (Das *et al.*, 2003; Pechmann *et al.*, 2003; Cismaru and Lavack, 2007). One possible explanation for these results is that humans are incapable or unwilling to adhere to established models and mathematical stringency. Another possible explanation is that studies fail to observe the multiplicative relation for one reason or another. There are several reasons to expect the latter.

First, some studies have measured the intentions to engage in protective behavior rather than assess actual risk. Clearly, the effectiveness and costs of the protective behavior are also factors to consider in such protective decisions, and this blend of factors may distort the results. Second, the scales to measure probability and severity used in many of the studies of information security behavior are not suited for multiplication. A multiplicative operation requires that two ratio scales are used, which is seldom the case in the research. For instance, a Likert scale with questions asking the respondent the extent he/she *Strongly Agree* or *Strongly Disagree* does not produce a ratio, and multiplications with such variables are questionable, if not outright invalid. Third, it is possible that people multiply probability and severity to calculate risk, but that they interpret the same scale differently. For example, with a loosely defined scale, one person may assign relative values and set the least probable event as a lowest likelihood, whereas another person may interpret the scale as an absolute scale and leave the lowest likelihood unused. In a between-subject design, which is the most common one in extant research, such differences in how scales should be used will distort the results. Fourth, when a fairly homogenous group of respondents are asked to assess one or a few incidents in a between-subject design, a large portion of the variance may be because of measurement errors. In other words, much of the differences in how respondents assess risks come from unreliable responses rather than actual differences in perceptions. To discover an interaction term when most of the observed variance between the subjects' ratings is due to an error requires considerable sample size. Fifth, the incidents assessed in a study may be so homogenous that respondents only use a portion of the scale presented to them. For example, it may be that all incidents are assessed as events with high probability and low severity. This would decrease the variance between responses, result in a relatively larger measurement error and make analysis more difficult.

Only one study was found that addressed the relationship between probability, severity and risk; isolated risks from remedies; used scales allowing multiplication; and used a within-subject design to avoid differences in scale interpretation. This study, by Weinstein (2000), comprised a convenience sample of 12 individuals who assessed 201 health risks, covering the entire probability–severity spectrum. The respondents first assessed the risk (R) by prioritizing events and valuing hypothetical insurances. After one to two weeks, the respondents assessed the probability (P) and the severity (S) for the same events. A clear multiplicative effect was found in the sample. A function with only a multiplicative term (i.e. $R = P \times S$) explained approximately 90 per cent of the variance explained by a function that also included the additive terms (i.e. $R = P + S + P \times S$). In other words, the additive function did not add much if the multiplicative term was included first. The result of Weinstein's study further suggests that perceived importance of the interaction between probability and severity depends on the value of these variables. For events with high probability and high severity, the severity matters most. For events with low probability and high severity, the multiplicative relationship is highly significant. The respondents were also, on average, insensitive to health risks with moderate to high probability ($p > 40$ per cent). Furthermore, the results suggest that there are considerable individual differences between how people assess health risks. For one respondent, the multiplicative term added 2 per cent explained variance to an additive model. For another respondent, it added 35 per cent explained variance.

This paper describes a study similar to that of Weinstein (2000), but in the information security domain. The primary aim was to test the following hypothesis:

H1. Perceived information security risk of an incident is determined as the product of the perceived probability of occurrence and the perceived severity.

In addition to a test of this hypothesis, an attempt is made to shed light on individual differences in the tendency to see risk as a product of severity and probability. Three variables were identified as potential reasons for why an individual would multiply or not: risk assessments experience, information security expertise and decision-making style. Two hypotheses concerning the tendency to see risk as an interaction between probability and severity are addressed:

H2. The tendency to assess risk as a product of probability and severity is related to the experience and expertise in information security risk assessments.

H3. The tendency to assess risk as a product of probability and severity is related to the decision-making style.

People who are more experienced and knowledgeable (*H2*) in the topic of information security risk assessment are expected to be more inclined to multiply probability and severity to assess the risk, mainly because this behavior is in line with established theories. With respect to *H3*, there are many aspects of the decision-making style that may influence the tendency to see risk as a product of severity and probability. The study described in this paper focuses on how rational and intuitive styles relate to the tendency to carry out multiplication. Individuals who make decisions based on facts and logical analysis (rational style) are believed to have a greater tendency to multiply than those who make decisions based on gut instinct and feelings (intuitive style).

Section 2 of the paper describes the method. Section 3 describes the results and Section 4 discusses these results.

2. Method

The study design was heavily influenced by the design used by Weinstein (2000). The sections below describe the participants, the survey instrument and the data collection procedure.

2.1 Participants

The survey was distributed to a sample of ten researchers active in the areas of information security, IT security, information systems development or human factors. All respondents were from the [ORGANIZATION BLINDED DURING THE REVIEW] (as are the authors of this paper), held university degrees, were in the age range 29-54 years and worked as researchers. To test *H2*, pertaining to security expertise and experience in risk assessments, five of the respondents were drawn from the information security research group and five of the respondents were drawn from the research group specialized in information systems development and human–machine interaction. Thus, whereas the participants were a convenience sample drawn from the authors' own organization, they represent a sample which is suitable to test the hypotheses in question.

2.2 Material and scales

Two paper-based questionnaires were used to conduct the study. The first questionnaire comprised two parts: one part asking questions about the respondent and one part asking the respondent to assess the probability and severity of 105 incidents. The second questionnaire repeated some of the probability and severity questions in the first questionnaire to allow reliability tests, but focused on measuring the perceived risk associated with the 105 incidents.

2.2.1 Incidents and scenarios. The 105 potential incidents (or scenarios) were designed to be meaningful for the target population. For example, they used information objects and threats that are relevant for the organization. Some examples include:

- "A computer virus extracts all documents related to cooperation with foreign states in the office network and shares this with a foreign intelligence service".
- "Spyware is introduced into the organization's office network by an international defense corporation".
- "Employees intentionally violate policies related to the storage of secret documents".
- "A scientist's USB-stick with five years of collected (unclassified) material is stolen at an international conference".

The incidents were constructed to cover the whole range of possible assessments. In other words, they were designed to be assessed as all combinations of low probability, high probability, low severity and high severity. This was not trivial. First, it is difficult to accurately predict how respondents will perceive the severity and probability of different incidents. Second, incidents of both high probability and high severity are (fortunately) difficult to identify. Third, concrete and tangible incidents often require that conditions are introduced that have a considerable impact on their probability. For instance, if an incident can be made more concrete and tangible by describing which documents the attackers obtain. However, the probably that this particular document is

obtained by an attacker may be very small. To handle these three issues and find a good set of incidents, a number of pretest were performed in the target populations. These pretests assessed both the inter-rater reliability and the spread of the responses.

2.2.2 Perceived probability and severity. In the first questionnaire, the respondents were asked to provide the severity and probability of each incident. The perceived *severity* of incidents was indicated by marking a line stretching from 0 (minimal, no harm at all) to 10 (greatest harm). In the questionnaire, it was emphasized that the worst of all 105 incidents should be rated a 10 and that other ratings should be proportional to this (e.g. that 5 means half as harmful as 10). The perceived *probability* of an incident occurring during the next 10 years was provided by marking a line with endpoints 0 per cent (minimal, completely unlikely) to 100 per cent (maximal, guaranteed to happen).

Anchors were present along the lines; however, respondents were free to mark any point on the lines. The corresponding values (e.g. severity 1.6 or probability 16 per cent) were measured using a ruler. To enable tests of reliability, i.e. answers that were stable over time, the second questionnaire asked the respondents to provide probability and severity assessments for 12 randomly selected incidents a second time.

2.2.3 Perceived risk. In the second questionnaire, the respondents were asked to provide the overall perceived risks associated with the incidents using two different methods. This redundancy was introduced to increase the confidence in the results. Both methods were supposed to reflect the perceived risk associated with an incident, without considering how easy or difficult it would be to lower the risk.

One of the methods presented a hypothetical scenario to the respondents. In the scenario, the respondent would have the power to simply eliminate some of the risks corresponding to the 105 incidents at no cost. They were asked to mark the *priority* of eliminating the risks by putting a mark on a line stretching from 0 (not at all prioritized) to 10 (absolutely highest priority). The other method had the respondents indicate the *expected costs* of the incident in monetary terms. More concretely, respondents were asked to write how much they would be prepared to pay to insure the organization against the risk if they were in charge of the budget. As in the study by Weinstein (2000), an upper limit and an anchor were used to simplify the assessment. The respondents were told that no risk was worth an insurance that cost more than SEK 10M (approximately €1M). They were also told that that protection against incidents involving lost or stolen USB-sticks ever happening was worth about 30 per cent of the maximum amount.

2.2.4 Decision-making style. The decision-making style was measured using eight items. These items were direct translations of the items presented by McShane (2006), which in turn was inspired by Scott and Bruce (1995), and the Cognitive Style Index by Allinson and Hayes (1996). Four items measure the tendency to be rational, i.e. to ignore gut instinct when it contradicts objective information and to make decision based on facts and logical analysis. Four items measure the tendency to be intuitive, i.e. to make decisions based on inner feelings or instinct rather than to rely on rational choices conflicting with intuition.

2.2.5 Expertise and experience. Measures of expertise and experiences were obtained from self-ratings by the respondents, which were validated against dichotomous classifications made by the investigators based on organizational department. Self-ratings were provided on the format "Completely agree" to "Completely disagree" for the following statements: "I work with security assessments or risk assessments", "I

work with information security" and "My colleagues think that I am an IT security expert or an information security expert".

2.3 Data collection procedure

Respondents were provided the second questionnaire one to two weeks after they had answered the first questionnaire. One week of time difference was expected to remove the opportunity of simply recollecting their previous responses and multiply them to obtain responses for the second questionnaire. To make sure that they did not have any of their previous responses in writing, the respondents were asked to remove all copies or notes related to their responses after completing the first questionnaire. Furthermore, to avoid influencing the respondents' risk assessment procedure, they were not told what the test actually was about. They were only told that the aim was to investigate how risk perceptions vary between individuals and why they vary. Follow-ups with respondents confirmed that they had not identified the actual purpose of the survey.

2.4 Validity and reliability measurement

In the study, the items on decision-making style had a Cronbach's alpha value of 0.810 and the items on security expertise had a Cronbach's alpha value of 0.962, i.e. they were highly internally consistent. As expected, the five participants who belonged to the information security research group considered themselves to have high security expertise, while the other five participants evaluated themselves much lower (means 4.533 compared to 1.733 on the scale of 1-5).

The repeated questions of the second questionnaire showed eight participants to be highly reliable, with Pearson correlations larger than 0.767 ($p < 0.001$). The responses from two of the respondents had non-significant correlations. Thus, the tests and retests suggest that all but two respondents reasoned about incidents in a similar way when answering questions on both occasions. Furthermore, the two measures for risk used in the second questionnaire were highly internally consistent with an average standardized Cronbach's alpha of 0.776.

3. Results

The risk equation used by the respondents is analyzed within-subjects and presented in Section 3.1. This risk equation allows us to test *H1*. As will be seen, the results of this test made it difficult to test *H2* and *H3*. Section 3.2 describes this further.

3.1 The risk equation

As in Weinstein's (2000) test, *H1* is tested by modeling the relationship between answers in the first questionnaire (on probability and severity) as predictor variables for answers in the second questionnaire (on priority and insurance premium) in a linear regression model. Table I provides the figures of the regression models for risk as priority (the upper half of the table) and risk as insurance premium (the lower half of the table). R^2(S, P) is the coefficient of determination for the linear (non-interaction) model, indicating the fit of that model. ΔR^2(S × P) describes how much the fit improves when considering an interaction model (multiplicative term). Four rows (p) indicate the significance (*) or non-significance (ns) of R^2, the severity (S), the probability (P) and ΔR^2, respectively.

As the table shows, few of the respondents show a tendency to multiply probability and severity to obtain the remediation priority or the insurance fee. Thus, there is little

Participant	1	2	3	4	5	6	7	8	9	10	Mean
Risk as priority											
R^2(S, P)	0.381	0.683	0.493	0.545	0.352	0.724	0.544	0.540	0.434	0.544	0.540
pR^2	*	*	*	*	*	*	*	*	*	*	
pS	*	*	*	*	*	*	*	*	*	*	
pP	ns	ns	*	*	ns	ns	*	ns	ns	*	
ΔR^2(S × P)	0.003	0.018	0.008	0.015	0.000	0.014	0.009	0.072	0.000	0.008	0.015
pΔR^2	ns	*	ns	ns	ns	*	ns	*	ns	ns	
Risk as insurance premium											
R^2(S, P)	0.108	0.464	0.505	0.357	0.193	0.657	0.406	0.453	0.281	0.415	0.384
pR^2	*	*	*	*	*	*	*	*	*	*	
pS	ns	*	*	*	*	*	*	*	*	*	
pP	ns	ns	ns	ns	ns	ns	*	*	*	*	
ΔR^2(S × P)	0.000	0.013	0.007	0.014	0.096	0.003	0.004	0.082	0.024	0.001	0.024
pΔR^2	ns	ns	ns	ns	ns	*	ns	*	ns	ns	

Table I.
Regression analyses with linear and interaction models (* = significant, ns = non-significant)

support for *H1*. Considering risk assessments using priority, the interaction term is significant for three of the respondents; considering the risk assessments using insurance premium, the interaction term is significant for two of the respondents. Furthermore, the contribution of the interaction term is small in the regression models for all respondents. At most, the interaction term adds 0.096 (statistically non-significant) explained variance to a regression model which explains 0.193 of the variance (Participant #5) and 0.082 (statistically significant) of explained variance to a model which explains 0.453 of the variance (Participant #8). Overall, the mean additional variance obtained by introducing the interaction term is 0.015 for priority and 0.024 for insurance premium. This should be related to an additive model, which explains 0.540 and 0.384 of the variance.

It should be added that the insignificance of the multiplicative term is not because the additive terms are present. The mean variance in risk (priority) explained by a model with only the multiplicative term is 0.049, and it is only statistically significant for the three respondents (as it was with the additive terms in the model). Furthermore, it is worth noting that these results hold within all quadrants of the probability–severity spectrum, i.e. for probability and severity that is high/low, low/high, low/low and high/high. A graphical illustration of the overall relation between perceived risk (as priority), perceived probability and perceived severity is given in Figure 1. Probabilities and severities are arranged in deciles to smoothen out the graph, and the mean value of the respondent's perceived risk as priority is depicted.

3.2 Variables related to the tendency to multiply

There were no statistically significant correlations between expertise and the tendency to multiply probability and severity to decide either risk as a priority or risk as an insurance. Nor were there any statistically significant correlations between decision-making style and tendency to multiply probability and severity to decide risk as a priority or risk as insurance. However, as described above, there was no general tendency in the studied population to multiply probability and severity when assessing

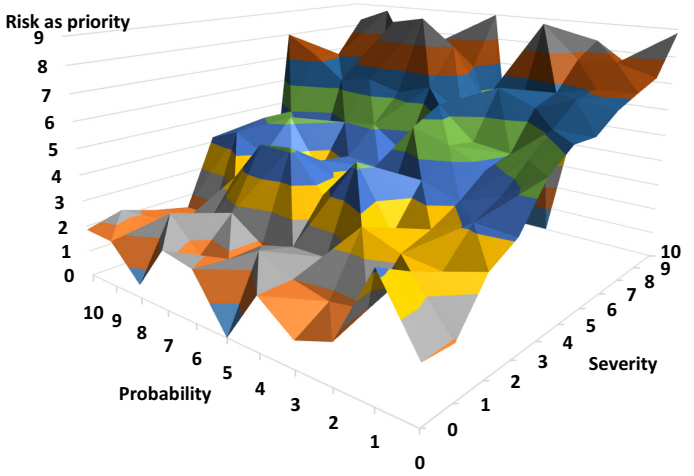

Figure 1.
Mean risk priority assigned to incidents with different probability (in deciles) and severity (in deciles)

risk. As a consequence, attempts to identify variables that relate to such a tendency (i.e. *H2* and *H3*) are doomed to fail.

4. Discussion

Most of the respondents seem to have an idea of probabilities and severities associated with information security incidents. For eight out of ten respondents, the probabilities and severities provided at different weeks for the same incidents had very strong correlations (>0.75). This perception of probabilities and severities is also, to some extent, shared among the respondents. Between-subjects correlations are considerable for probabilities (0.46), severities (0.52) and risks (0.48). Thus, their responses seem to stem from some partially shared perception of the information security threats. This suggests that the survey is able to measure the perceptions it set out to measure. Nevertheless, there are many possible reasons for the fact that our result – in contrast to the one of Weinstein (2000) – does not support a multiplicative relationship between severity and probability in people's minds when calculating risk. The results indicate that information security risk assessments are determined by the severity.

Similarly to Weinstein's study, the present study used a limited non-random sample. Our participants were more homogenous in terms of profession and slightly more homogenous in terms of age and gender than the sample of Weinstein. Any of these factors may explain the focus on incident severity and the insignificance of the multiplicative terms in this test. However, it is unclear to the authors why they should. On the contrary, it is hard to see how and why a population of researchers, of which many had considerable risk assessment experience, should be unable or unwilling to perceive risk as a product of probability and severity.

The scales and measurement procedure used in this test is different from the ones used by Weinstein (2000) in several ways. First, Weinstein's first questionnaire concerned (compound) risk where he let half of the participants assess risks. The present study instead measured (compound) risk in the second questionnaire, whereas probability and severity were measured in the first. This may have caused our participants to be more prone to thinking of risk as a product of probability and severity,

so this is not an issue considering our results. Second, the present study required all the participants to rate risk both by priority and insurance premium. It is hard to see why answering risk questions formulated in two ways would reduce the tendency to multiply probability and severity. Third, the present study described risk interventions with a slightly different phrasing. The phrasing in Weinstein's study was that the risk treatment options would remove the probability that the incident would materialize. The phrasing used in the present study stated that they could either remove the probability that the threats materialize or render them harmless if they did. Measures against the consequence part of risks, e.g. backups, are not uncommon in the information security domain. It was also the part of the risk respondents considered most important in the present study. It is therefore hard to see why this way of formulating the questions would confuse the respondents. Fourth, the participants in the present study needed to reason in terms of insurance premiums that were considerably larger than in Weinstein's study. This may have made the appreciation more difficult and introduced more measurement error. However, it is hard to see this as a possible reason for the insignificant multiplicative term for risk as priority. Fifth, a significant difference to Weinstein's survey concerns the timeframe considered. In Weinstein's study, probabilities were (implicitly) restricted, in that incidents should happen in the respondents' remaining lifetime. For an organization, there is no natural timeframe of this sort. To avoid infinite possibilities, a timeframe was set to 10 years. It is unclear why an absolute time frame of 10 years as in the present study would make respondents less prone to multiply probability and severity. Especially given that the probability assessments were relatively stable within and between respondents.

Perhaps the most important difference between the measurements in our study and in Weinstein's (2000) study is the content of the incidents. In our case, the incidents relate to the participants' organization rather than the participants themselves, and our incidents are less well-known than say pneumonia or rash from poison ivy. Weinstein partly based his incidents on a standard compendium of diseases, while this study was constructed for a specific organization. This may have led to incidents that were more difficult to interpret with greater variance between subjects. Our results, however, suggest that the respondents' assessments agreed and the performed test–retests suggest that most respondents understood the questions well enough to answer them similarly. Thus, the scenarios were clearly comprehendible. Furthermore, as in Weinstein's study, the perceptions of probability and severity in the present study are correlated. Information security incidents of high probability have low severity and vice versa. Such multicollinearity could be an issue in regression models. However, average correlation between probability and severity is this study (-0.37) is lower than that Weinstein reported (-0.56). Thus, this should not explain the difference in the result between the two studies.

5. Conclusions

The results of this study suggests that neither information security experts nor other information system professionals perceive information security risk associated with an incident as a result of a multiplication of its probability and its severity. Instead, the respondents of this study tend to see the severity of an incident as sufficient for assessing the priority of removing the risk and the value of an insurance premium for the risk. This is in stark contrast to the established idea that the risk should be

determined through a multiplication of probability and severity. The result is a good justification for procedures described in many information security risk assessment methods that force the users to assess probability separately from severity and then multiply the two factors. For example, the use of two-dimensional risk assessment matrixes with probability and severity as inputs will help to make sure that risk is assessed in a rational way.

References

Allinson, C.W. and Hayes, J. (1996), "The cognitive style index: a measure of intuition-analysis for organizational research", *Journal of Management Studies*, Vol. 33 No. 1, pp. 119-135, available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6486.1996.tb00801.x/full (accessed 28 October 2014).

Blakley, B. and Mcdermott, E. (2002), "Information security is information risk management", *Proceedings of the 2001 Workshop on New Security Paradigms*, ACM, Cioudcroll, NM, pp. 97-104.

Cismaru, M. and Lavack, A.M. (2007), "Interaction effects and combinatorial rules governing Protection Motivation Theory variables: a new model", *Marketing Theory*, Vol. 7 No. 3, pp. 249-270, available at: http://mtq.sagepub.com/cgi/doi/10.1177/1470593107080344 (accessed 29 August 2013).

Club de la Sécurité de l'Information Français (2011), "MEHARI 2010 Processing guide for risk analysis and management", CLUSIF, Paris, pp. 1-32, available at: www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf (accessed 12 March 2016).

Das, E.H.H.J., de Wit, J.B.F. and Stroebe, W. (2003), "Fear appeals motivate acceptance of action recommendations: evidence for a positive bias in the processing of persuasive messages", *Personality & Social Psychology Bulletin*, Vol. 29 No. 5, pp. 650-664, available at: www.ncbi.nlm.nih.gov/pubmed/15272997 (accessed 12 September 2013).

Gordon, L.A. and Loeb, M.P. (2002), "The economics of information security investment", *ACM Transactions on Information and System Security*, Vol. 5 No. 4, pp. 438-457, available at: http://portal.acm.org/citation.cfm?doid=581271.581274

Karabacak, B. and Sogukpinar, I. (2005), "ISRAM: information security risk analysis method", *Computers & Security*, Vol. 24 No. 2, pp. 147-159, available at: http://dx.doi.org/10.1016/j.cose.2004.07.004

Lund, M.S., Solhaug, B. and Stolen, K. (2011), *Model-driven Risk Analysis: The CORAS Approach*, Springer Verlag, Berlin Heidelberg.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479, available at: http://linkinghub.elsevier.com/retrieve/pii/0022103183900239 (accessed 20 October 2012).

McShane, S.L. (2006), "Activity 8.8: decision making style inventory", *Canadian Organizational Behaviour*, McGraw-Hill Education, available at: http://highered.mheducation.com/sites/0070876940/student_view0/chapter8/activity_8_8.html

NIST (2012), NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments, available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed 12 march 2016).

Pechmann, C., Zhao, G., Goldberg, M.E. and Reibling, E.T. (2003), "What to convey in antismoking advertisements for adolescents: the use of protection motivation theory to identify effective

message themes", *Journal of Marketing*, Vol. 67 No. 2, pp. 1-18, available at: http://journals.ama.org/doi/abs/10.1509/jmkg.67.2.1.18607 (accessed 12 September 2013).

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation", in Cacioppo, J. and Petty, R. (Eds), *Social Psychophysiology*, Guilford Press, New York, NY.

Scott, S.G. and Bruce, R.A. (1995), "Decision-making style: the development and assessment of a new measure", *Educational and Psychological Measurement*, Vol. 55 No. 5, pp. 818-831, available at: http://epm.sagepub.com/cgi/doi/10.1177/0013164495055005017 (accessed 24 October 2014).

Sommestad, T., Ekstedt, M. and Johnson, P. (2010), "A probabilistic relational model for security risk analysis", *Computers & Security*, Vol. 29 No. 6, pp. 659-679, available at: https://eeweb01.ee.kth.se/upload/publications/reports/2010/IR-EE-ICS_2010_051.pdf (accessed 10 July 2010).

Weinstein, N.D. (2000), "Perceived probability, perceived severity, and health-protective behavior", *Health Psychology: Official Journal of the Division of Health Psychology, American Psychological Association*, Vol. 19 No. 1, pp. 65-74, available at: www.ncbi.nlm.nih.gov/pubmed/10711589

Corresponding author
Teodor Sommestad can be contacted at: Teodor.Sommestad@foi.se