Understanding Precautionary Online Behavioural Intentions: A Comparison of Three Models

J. Jansen[1,2] and P. van Schaik[3]

[1]Faculty of Humanities and Law, Open University of the Netherlands
[2]Cybersafety Research Group, NHL University of Applied Sciences
[3]School of Social Sciences, Business and Law, Teesside University
e-mail: j.jansen@nhl.nl; p.van-schaik@tees.ac.uk

Abstract

We used a survey design to compare three social cognitive models in their ability to explain intentions of precautionary online behaviour. The models were protection motivation theory (PMT), the reasoned action approach (RAA) and an integrated model comprising variables of these models. Data from 1,200 Dutch users of online banking were analysed with partial-least-squares path-modelling. The two separate models explain about equally much variance in precautionary online behaviour; in the integrated model the significant predictors of the two models remained significant. We conclude that both PMT and RAA make a unique contribution in explaining variance. Our results give practitioners potentially a wider range of options to design preventative measures.

Keywords

Information Security Behaviour, Protection Motivation Theory, Reasoned Action Approach, Online Banking, Human Factors

1. Introduction

As more services to customers are offered online, such as banking, government and health, security becomes increasingly important. Harm can be done to individuals, the economy and society when security is compromised, for example, by means of data breaches and distributed denial of service attacks. It is evident that security needs to be addressed by service providers. However, it is equally important that end-users behave in a secure fashion, as they play an essential role in safeguarding the online domain. Moreover, they are essential for achieving online security (Furnell *et al.* 2006; Liang and Xue, 2010; Ng *et al.*, 2009).

The present study deals with safety and security of online banking from an end-user perspective. End-users are, for example, confronted with phishing and malware attacks (Jansen and Leukfeldt, 2015); techniques fraudsters use to obtain user-credentials in order to steal money from their bank accounts. Because banks cannot control their customers' behaviour nor the devices their customers use, it is important that end-users are aware of threats aimed at online banking and try to prevent threats from manifesting in harm (Jansen, 2015). In this paper, we study what motivates

end-users to protect themselves against online threats by analysing three social cognitive models. A better understanding of precautionary online behaviour is required to enhance safety and security from an end-user perspective.

To date, several models exist that try to explain and predict behaviour (Floyd *et al.* 2000). Our main interest is aimed at explained variance rather than assessing the quality of the models, see for example Prochaska *et al.* (2008). The current study evaluates three models in terms of their effectiveness in explaining precautionary online behaviour. We compare protection motivation theory (PMT) (Rogers, 1975), the reasoned action approach (RAA) (Fishbein and Ajzen, 2010) and an integrated model which comprises PMT and RAA variables. Although PMT and RAA are both evaluated as motivational models (Armitage and Conner, 2000), PMT is considered a stress-coping theory whereas RAA is a belief-attitude theory (Boer and Mashamba, 2005). Both models seem equally valuable in the present context and are discussed in more detail in Section 2. Added value of testing individual and integrated models is that, first, theoretical knowledge is advanced and, second, maximum effectiveness is pursued (Lippke and Ziegelmann, 2008; Sommestad *et al.* 2015). In addition, based upon Ifinedo's (2012) work, we expect the integrated model to provide a more comprehensive account of the determinants of precautionary online behaviour.

Both PMT and RAA (including RAA's predecessors), have been tested extensively to predict numerous behavioural intentions and actual behaviours. However, to our knowledge they have not been widely compared in the information security domain, nor have they been extensively tested in an integrated fashion. Comparison is needed to help researchers make informed decisions about the usefulness of social cognitive models in this area. Therefore, the aim of our study is to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. In addition, our study advances the understanding of precautionary online behaviour, which is still limited (Anderson and Agarwal, 2010; Liang and Xue, 2010; Ng *et al.* 2009). The results are useful for scholars and practitioners who want to study and improve online safety and security practices by end-users in general and safe and secure online banking in particular.

2. Background literature and development of hypotheses

In this section, a brief overview is given of PMT (2.1) and RAA (2.2), complemented with definitions of the predictor variables. Next, we discuss precautionary online behavioural intention, the target behaviour of our study (2.3). Finally, a set of hypotheses are presented (2.4) that are tested in this study.

2.1. Protection motivation theory

PMT is a social cognitive model that predicts behaviour and is often applied in the health domain (Milne *et al.* 2000), but has recently gained attention in the information security domain (Boss *et al.* 2015; Jansen, 2015; Vance *et al.* 2012). According to PMT, end-users are motivated to protect themselves based on threat appraisal and coping appraisal processes, which implies that end-users first evaluate

possible threats and second possible coping strategies. These evaluations determine users' protection motivation, i.e. their intention to proceed, continue or avoid a given behaviour (Floyd *et al.* 2000). According to these authors, PMT is one of the best explanatory models for predicting protective behaviour. It is also viewed as a framework to develop and evaluate persuasive communications (Norman *et al.* 2005).

In PMT, threat appraisal process consists of perceived vulnerability and perceived severity. Crossler (2010) describes perceived vulnerability as the personal probability or likelihood of a security incident occurring and perceived severity as the impact of consequences resulting from a security incident. Perceived risk is a unique component in PMT, not present in RAA. The coping appraisal process consists of response efficacy, self-efficacy and response costs. Milne *et al.* (2000) describe the first construct as the perceived effectiveness of a response in reducing a threat, the second as users' belief whether they are able to perform the recommended response and the third as how costly performing the response will be to the user. The combination of these constructs reflects PMT's core nomology (Boss *et al.* 2015).

2.2. Reasoned action approach

RAA, which evolved from the popular theory of reasoned action (Fishbein and Ajzen, 1975) and the theory of planned behaviour (Ajzen, 1991), is a more general model for predicting human behaviour. The essence of Fishbein and Ajzen's (2010) framework is that attitude towards behaviour, perceived norms and perceived behavioural control determine users' intention to perform a given behaviour. It is assumed that behavioural intention predicts actual behaviour. Moreover, they believe that their approach is unified, accounting for any behaviour. Therefore, their approach should also be appropriate for information security behaviour.

Attitude reflects a user's positive or negative feelings towards performing the target behaviour (Fishbein and Ajzen, 1975). Perceived norms, unique in RAA compared to PMT, refers to perceived social pressure and is made up of injunctive norms – perceptions what should or ought to be done – and descriptive norms – perceptions that others are or are not performing the target behaviour (Fishbein and Ajzen, 2010). The authors describe perceived behavioural control as perceptions about being capable of or having control over the target behaviour. Perceived behavioural control is viewed as a combination of self-efficacy (also found in PMT) and locus of control (Workman *et al.* 2008). Because these constructs are two distinct concepts, we have chosen to adopt these two categorizations instead of the single perceived behavioural control construct. Locus of control can be internal – when users believe they control the outcome of a certain event – or external – when users believe the outcome is controlled by fate or powerful others (Rotter, 1966; Workman *et al.* 2008).

2.3. Precautionary online behaviour

The outcome variable of this study is based on the uniform safety rules for online banking, which are part of the General Terms and Conditions of all Dutch banks.

These five rules comprise: keep your security codes secret, make sure that your debit card is not used by others, secure the devices you use for online banking properly, check your bank account regularly, and report incidents directly to your bank. Precautionary online behaviour includes both technical and non-technical measures against security threats.

Thus, the dependent variable consists of multiple actions. Although this approach is sometimes criticized (Blythe *et al.* 2015), because predictor variables might influence protection motivation for one behaviour, but not for another, others (Crossler and Bélanger, 2014) defend this approach, stating that precautionary behaviour against online threats constitutes taking multiple actions. Based on this notion and practical considerations (lack of validated scales for precautionary online behaviour and length of questionnaire), we chose to ask respondents questions about their intentions to adhere to the uniform safety rules.

2.4. Hypotheses

In Table 1, we present our hypotheses. These are based on PMT (H1, H2, H3, H5), RAA (H6, H7, H8, H9), and both PMT and RAA (H4).

#	Hypothesis
H1	Perceived vulnerability positively influences precautionary online behaviour.
H2	Perceived severity positively influences precautionary online behaviour.
H3	Response efficacy positively influences precautionary online behaviour.
H4	Self-efficacy positively influences precautionary online behaviour.
H5	Response costs negatively influence precautionary online behaviour.
H6	A positive attitude positively influences precautionary online behaviour.
H7	Injunctive norms positively influences precautionary online behaviour.
H8	Descriptive norms positively influences precautionary online behaviour.
H9	Internal locus of control positively influences precautionary online behaviour.

Table 1: Study Hypotheses

3. Method

In this section, we describe the methods used to test the hypotheses and evaluate which model is most effective in predicting users' motivation for precautionary online behaviour. We discuss the survey questionnaire, procedure and participants (3.1). We then discuss data analysis, validity and reliability of measures (3.2). Detailed information about measures is available from the authors upon request.

3.1. Survey questionnaire, procedure and participants

Based on literature study, using international databases ACM Digital Library, ScienceDirect and Web of Science, we developed a questionnaire. We based the questionnaire items on the work of Anderson and Agarwal (2010), Herath and Rao (2009), Ifinedo (2012), Ng *et al.* (2009), Witte (1996) and Workman *et al.* (2008). The items were translated in Dutch, programmed in LimeSurvey (an open-source

online survey tool), were presented in random order, and used a 5-point Likert-scale, ranging from totally disagree to totally agree. All predictor variables were measured by three items and precautionary online behaviour was measured by four items. Two examples of the items adopted: a) the uniform safety rules help in preventing online banking fraud (RE1) and b) it is my intention to comply with the uniform safety rules (PM4). The questionnaire (a concept and a programmed version) was pretested qualitatively by twelve persons, including target group, key figures from the banking sector and scientific peers and quantitatively by 34 students before data collection.

Respondents were recruited by an external recruitment service of online survey panels. The questionnaire was online in May-June 2015. In total, 1,200 Dutch users of online banking services completely filled out the online questionnaire. Participants' age ranged from 18 to 85 years ($M = 49$, $SD = 14.5$) and the gender distribution was 55% female and 45% male. Participants had completed at most lower secondary education (15%), upper secondary education (32%) and higher education (53%) and were employed (54%), self-employed (7%), retired (19%) or had a different work status (20%), such as student and unemployed.

3.2. Data analysis, validity and reliability

Partial-least-squares path-modelling (PLS), using SmartPLS 2.0 (Ringle *et al.* 2005), was used for data analysis. PLS can be described as a class of multivariate techniques to study relationships between measured variables and latent variables and relationships between latent variables (Hair *et al.* 2014). As recommended by Henseler *et al.* (2009), we used a standard bootstrapping procedure ($N = 5{,}000$) to test the significance of the model parameters.

Component loadings of the individual items, except one item of response costs which was subsequently deleted, loaded highly ($\geq .70$) on the corresponding component, providing evidence for unidimensionality of the items. However, we had to remove two self-efficacy and attitude items, because these items loaded high on protection motivation as well. Therefore, both constructs were represented by only one item in the structural models, posing a potential threat to reliability. Future research needs to address this limitation using more robust measures. Construct reliability was assessed using the composite reliability co-efficient; for all items, the cut-off point of .70 was exceeded.

Convergent validity was assessed using the average variance extracted (AVE) by a construct from its indicators, which all, except for locus of control (.64), exceeded the cut-off point of .70. Discriminant validity was assessed by analysing the square root of AVE by each construct from its indicators, which should be greater than its correlation with the remaining constructs (Fornell-Larcker-criterion). All values met this condition. Additional SPSS analyses showed no multicollinearity issues.

4. Results

In this section, the structural models with test results are presented in Figures 1-3. We evaluate the significance of the model predictors of precautionary online behaviour. The asterisks indicate a significance level of .001 and *ns* stands for not significant.

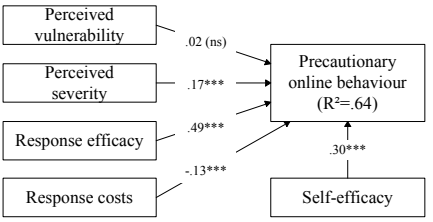

Figure 1: Structural Model PMT Variables

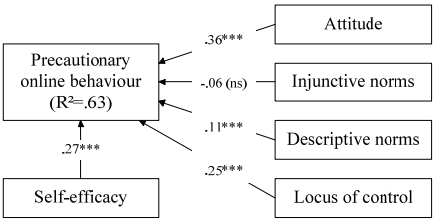

Figure 2: Structural Model RAA Variables

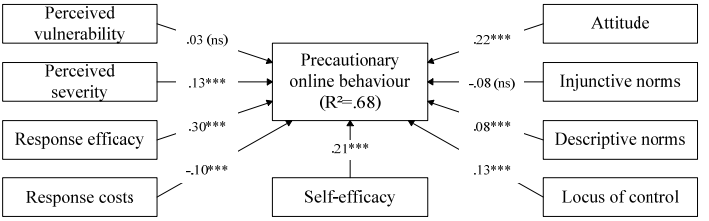

Figure 3: Structural Model PMT-RAA Variables

In the integrated model, explained variance of 68% is highest (Figure 3). The other structural models also provide high levels of explained variance, namely 64% for PMT variables (Figure 1) and 63% for RAA variables (Figure 2). In terms of the effect size f^2, the additional variance explained by PMT over and above RAA (f^2 = .16) and the additional variance explained by RAA over and above PMT (f^2 = .13) both represent approximately a medium effect (f^2 = .15; Hair *et al.* 2014).

PMT variables perceived severity, response efficacy and response costs, RAA variables attitude, descriptive norms and locus of control, and self-efficacy from both models were significant predictors of precautionary online behaviour (see Figures 1-3). Therefore, all hypotheses are accepted, except for H1 and H7 – thus perceived vulnerability and injunctive norms were not significant predictors.

5. Conclusions and Discussion

The aim of our study was to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. PMT and RAA both show good explanatory power, which indicates that both seem valuable in explaining this kind of behaviour. A main value of the combined model is that it shows that the individual predictors of the two

constituent models (PMT and RAA) remain significant, thereby potentially providing practitioners more opportunities for prevention to increase people's precautionary behaviour. Significant predictors can, for example, be manipulated in prevention campaigns leading to behavioural change. Increased precautionary behaviour of end-users is beneficial for banks as it might reduce the number of online banking fraud incidents. In contrast to Sommestad *et al.*'s (2015) findings, our results show that coping response (from PMT) is significant in explaining variance.

Considering predictor variables of PMT, response efficacy and self-efficacy are most important. This means that the more effective a measure is perceived and the better the ability of carrying out a measure is perceived, the more likely precautionary behaviour is, which concurs with previous studies (Crossler, 2010; Ifinedo, 2012; Lee, 2011; Liang and Xue, 2010; Workman *et al.* 2008). Attitude, from RAA, can also be considered a primary predictor variable. The more positive the attitude towards precautionary online behaviour, the more likely such behaviour is, which is also demonstrated in earlier studies (Venkatesh *et al.* 2003). Scholars and practitioners can use these findings to develop prevention campaigns by effectively addressing these variables. Experimental studies can provide insight in the impact of these determinants. To our knowledge, studies that investigate the power of either model's predictors to create preventative measures are lacking.

Secondary determinants of explaining precautionary online behaviour, which behave in accordance with literature, are perceived severity (Chenoweth *et al.* 2009; Gurung *et al.* 2009; Lee, 2011; Vance *et al.* 2012; Workman *et al.* 2008) and locus of control (Ifinedo, 2014; Workman *et al.* 2008). If end-users evaluate the impact of a threat as high and believe a threat can be prevented by themselves and is something they are responsible for, the more likely they adopt the appointed measure. Therefore, these variables should also be considered when testing and implementing prevention strategies. Future studies could benefit from including measuring fear and using fear appeals manipulations in order to enhance such strategies (Boss *et al.* 2015).

Perceived vulnerability had no significant effect on protection motivation. Earlier studies found mixed results for this construct. Gurung *et al.* (2009) and Vance *et al.* (2012) also reported a non-significant relationship. However, Chenoweth *et al.* (2009), Lee (2011) and Workman *et al.* (2008) found a positive relationship between perceived vulnerability and protection motivation. Crossler's (2010) study on the other hand revealed a negative relationship. Injunctive norms were non-significant as well, contradicting with earlier studies (Herath and Rao, 2009; Ifinedo, 2012, 2014). However, contrary to our study, these studies took place in organizations, while security of online banking may be seen as an individual rather than a social issue.

Although there seems to be overlap between the models, it is important to stress that theory is advanced by testing the usefulness of these theories in the study of online behaviours. However, considering the advancement of theory, Ogden (2003) argues that this is problematic due to the unspecific nature of the constructs involved. Indeed, though the scales we used and the relationships we found were predetermined based on theory, the questionnaire items needed to be specified to the

online domain in general and specifically to the online banking context. Another problem Ogden (2003) identifies is that social cognitive models often rely on analytic truths instead of synthetic truths. Qualitative exploratory research is recommended in order to identify predictor variables that are accountable for the variance we were not able to explain.

For now, it seems that the integrated model is most effective in explaining variance. However, as explained by Lippke and Ziegelmann (2008), one theory can be more suitable for explaining a specific behaviour across populations and another for explaining diverse behaviours in a specific population. Future research is needed – across different domains, behaviours and populations – to advance our knowledge of this domain and to understand which of these (or competing) models best explains precautionary online behaviour of end-users. In addition, it is interesting to study how precautionary behaviour relates to or contributes to overall online behaviour.

In conclusion, we relied on self-reported behavioural intention, which could be considered a limitation. Therefore, we recommend observing actual behaviour in future studies, particularly to overcome the intention-behaviour gap; see also Boss *et al.*'s (2015) commentary on PMT studies and Crossler *et al.*'s (2013) research agenda. A promising area, especially with regard to changing behaviour, could be examining behavioural enaction models, which are predominantly concerned with improving the intention-behaviour relation (Armitage and Conner, 2000).

6. Acknowledgements

This study is part of a research program on the safety and security of online banking. This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy, and the Dutch National Police.

7. References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp179–211.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34, No. 3, pp613–643.

Armitage, C.J. and Conner, M. (2000), "Social cognition models and health behaviour: A structured review", *Psychology and Health*, Vol. 15, No. 2, pp173–189.

Blythe, J.M., Coventry, L. and Little, L. (2015), "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors", *Proceedings of the 11th Symposium On Usable Privacy and Security*, pp103–122.

Boer, H. and Mashamba, M.T. (2005), "Psychosocial correlates of HIV protection motivation among black adolescents in Venda, South Africa", *AIDS Education and Prevention*, Vol. 17, No. 6, pp590–602.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", *MIS Quarterly*, Vol. 39, No. 4, pp837–864.

Chenoweth, T., Minch, R. and Gattiker, T. (2009), "Application of protection motivation theory to adoption of protective technologies", *Proceedings of the 42nd Hawaii International Conference on System Sciences*, pp1–10.

Crossler, R. and Bélanger, F. (2014), "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument", *ACM SIGMIS Database*, Vol. 45, No. 4, pp51–71.

Crossler, R.E. (2010), "Protection motivation theory: Understanding determinants to backing up personal data", *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pp1–10.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp90–101.

Fishbein, M. and Ajzen, I. (1975), *"Belief, attitude, intention and behavior: An introduction to theory and research",* MA: Addison-Wesley, ISBN: 978-0-2010-2089-2.

Fishbein, M. and Ajzen, I. (2010), *"Predicting and changing behavior: The reasoned action approach"*, New York: Taylor & Francis, ISBN: 978-0-8058-5924-9.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp407–429.

Furnell, S.M., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: A survey of end-users", *Computers & Security*, Vol. 25, No. 1, pp27–35.

Gurung, A., Luo, X. and Liao, Q. (2009), "Consumer motivations in taking action against spyware: An empirical investigation", *Information Management & Computer Security*, Vol. 17, No. 3, pp276–289.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014), *"A primer on partial least squares structural equation modeling (PLS-SEM)"*, SAGE Publications, Inc., ISBN: 978-1-4522-1744-4.

Henseler, J., Ringle, C.M. and Sinkovics, R.R. (2009), "The use of partial least squares path modeling in international marketing, In: Sinkovics, R.R. (Ed.), *Advances in International Marketing* (Vol. 20, pp277–320), Bingley: Emerald, ISBN: 978-1-84855-468-9.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: A framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18, No. 2, pp106–125.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31, No. 1, pp83–95.

Ifinedo, P. (2014), "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, Vol. 51, No. 1, pp69–79.

Jansen, J. (2015), "Studying safe online banking behaviour: A protection motivation theory approach", *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance*, pp120–130.

Jansen, J. and Leukfeldt, R. (2015), "How people help fraudsters steal their money: An analysis of 600 online banking fraud cases", *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust*, pp24–31.

Lee, Y. (2011), "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective", *Decision Support Systems*, Vol. 50, No. 2, pp361–369.

Liang, H. and Xue, Y. (2010), "Understanding security behaviors in personal computer usage: A threat avoidance perspective", *Journal of the Association for Information Systems*, Vol. 11, No. 7, pp394–413.

Lippke, S. and Ziegelmann, J.P. (2008), "Theory-based health behavior change: Developing, testing, and applying theories for evidence-based interventions", *Applied Psychology: An International Review*, Vol. 57, No. 4, pp698–716.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp106–143.

Ng, B.-Y., Kankanhalli, A. and Xu, Y.C. (2009), "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Vol. 46, No. 4, pp815–825.

Norman, P., Boer, H. and Seydel, E.R. (2005), "Protection motivation theory", In: M. Conner and P. Norman (Eds.), *Predicting health behaviour* (second edition, pp81–126), Open University Press, ISBN: 978-0-3352-1176-0.

Ogden, J. (2003), "Some problems with social cognition models: A pragmatic and conceptual analysis", *Health Psychology*, Vol. 22, pp424–428.

Prochaska, J.O., Wright, J.A. and Velicer, W.F. (2008), "Evaluating theories of health behavior change: A hierarchy of criteria applied to the transtheoretical model", *Applied Pyschology: An International Review*, Vol. 57, No. 4, pp561-588.

Ringle, C.M., Wende, S. and Will, A. (2005), "SmartPLS 2.0.M3", *Hamburg: SmartPLS, Retrieved from http://www.smartpls.com*.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, No. 1, pp93–114.

Rotter, J.B. (1966), "Generalized expectancies for internal versus external control of reinforcement", *Psychological Monographs: General and Applied*, Vol. 80, No. 1, pp1–28.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information & Computer Security*, Vol. 23, No. 2, pp200–217.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, Vol. 49, pp190–198.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: Toward a unified view", *MIS Quarterly*, Vol. 27, No. 3, pp425–478.

Witte, K. (1996), "Predicting risk behaviors: Development and validation of a diagnostic scale", *Journal of Health Communication*, Vol. 1, pp317–341.

Workman, M., Bommer, W.H. and Straub, D. (2008), "Security lapses and the omission of information security measures: A threat control model and empirical test", *Computers in Human Behavior*, Vol. 24, No. 6, pp2799–2816.