Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

The Influence of Organizational Commitment on Information Security Policy Compliance

V.A. Hooper[1] and J. Ophoff[2]

[1]Victoria University of Wellington, New Zealand
[2]University of Cape Town, South Africa
e-mail: val.hooper@vuw.avc.nz; jacques.ophoff@uct.ac.za

Abstract

The influence of fear appeals, in terms of threat appraisals and coping appraisals, on security compliance has been examined by many researchers. However, findings have been mixed and this has been attributed to a possible misapplication of the Protection Motivation Theory. We address the issue of questionable personal relevance of the threat by introducing organizational commitment (affective, normative, continuance commitment) as a further influence on compliance behaviour. Using a survey of organizational employees we found that affective commitment exerted an influence on social influence while normative commitment influenced response cost. The threat severity did not exert an influence on compliance behaviour.

Keywords

Organizational commitment, Protection Motivation Theory, Affective commitment, Normative commitment, Continuance commitment

1. Introduction

Insider threat has been identified as one of the greatest sources of potential damage to a firm's IT security. Insider threats can be classified as intentional, often known as deliberate malicious behaviour such as manipulation, destruction and theft of IS assets; and unintentional behaviour, often caused by negligence, carelessness or lack of awareness with protocols (Willison and Warkentin, 2013).

In an attempt to understand what motivates employees to comply with security policies or not, researchers have approached the issue from two main perspectives: studies which examine what motivates employees to comply; and what motivates employees not to comply. In doing so, they have drawn on various disciplines. For instance, much IS security research is based on the Health Belief Model (Janz & Becker, 1984) and the derivative Protection Motivation Theory (PMT) (Rogers, 1975). These two theories identified the threat appraisal factors of threat severity and threat susceptibility; and the PMT added the coping factors of response efficacy and response costs, as well as self-efficacy (which was also later added to the HBM). The Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980) added the element of the influence of the subjective norm, or the impact of influential others on an individual's actions. The derivative of the TRA, the Theory of Planned Behaviour

(TPB) (Ajzen, 1991) added the further element of the ability to control the behaviour in question.

One of the big challenges for researchers, however, has been to understand the relevance to the individual of the perceived threat to the organizational assets. Do they really care if the organizational assets are threatened? We suggest that the concept of organizational commitment might hold the key to assessing that personal relevance. We argue that if an individual is very committed to an organization, he/she will value the organizational assets highly and any threat to those assets will be experienced in a manner similar to a threat to personal assets. By the same score, if the individual is not committed to the organization, he/she will not feel strongly about the organizational assets and even if the threat is perceived as severe, they might not feel particularly inclined to even comply with security policies, particularly if they are inconvenienced by them.

The following sections outline the theoretical basis of the research, the research model, the data collection, the results and analysis thereof, and a discussion of the findings and conclusion.

2. Theoretical background

Much of the research that has examined compliance with organizational security policies, or intentions to comply, has been based on the Protection Motivation Theory (PMT) (Anderson & Agarwal, 2010; Johnston and Wakentin, 2010; Lee & Larsen, 2009; Pahnila *et al.*, 2007; Workman *et al.*, 2008) Originally derived from the Health Belief Model, the PMT was based on fear appeals targeted at disease prevention behaviours. These appeals were to the individual and their appraisal of the disease threat. The appraisal consisted of their perception of the severity of the threat and their susceptibility to the threat. That appraisal was complemented by their appraisal of the respective coping mechanisms (Rogers, 1975). Together these appraisals influenced the prevention behaviour of the individual. Essentially, the theory was a behavioural change theory.

In due course, self-efficacy was added to the theory as a further coping means. This marked the change of theory from a fear-based behavioural change theory to a general motivation theory (Maddux & Rogers, 1983). However, this is where the inappropriateness of the PMT for organizational security compliance became questionable. While the PMT, as applied in the health sciences, treated the threat as personally relevant, in security compliance, the threat could not always be said to be personally relevant. It was relevant to the organization. The addition of self-efficacy highlighted the distinction between the components of the theory that were more relevant to the organization and those that were more relevant to the individual. Johnston *et al.* (2015) argued that this inappropriate application of the theory, could have been responsible for the mixed findings of researchers with regard to the factors influencing security compliance (e.g. Ifinedo, 2012 and Siponen *et al.*, 2014). They argued that such application of the PMT did not account for the nuances in the perceptions of the threat. A threat to organizational data and information or an

individual's data/information (i.e. their things) would, in all likelihood, not be perceived as severe as a threat to an individual's person. The PMT was thus not, in their view, suitable for providing threat warnings because it lacked the personal relevance. They furthermore pointed out that instead of the PMT being used as a behavioural change theory in security research, it had been used to identify the factors that motivated security compliance (Anderson & Agarwal, 2010; Herath & Rao, 2009) without regard for behavioural change.

Researchers such as Boss *et al.* (2015) have supported this critical assessment of the PMT and have addressed the shortcomings by adding maladaptive responses to the coping appraisal and an actual component of fear resulting from the threat appraisal and coping appraisal and influencing protection motivation and indirectly security behaviours. Yet others (Johnston *et al*., 2015) have attempted to introduce the personal relevance of the threat by balancing the elements of the PMT with those of Deterrence Theory – formal and informal sanction certainty, formal and informal sanction severity, and sanction celerity. Hsu *et al.* (2015) proposed social desirability and self-imposed costs such as shame, moral beliefs and commitment as social costs which also exerted restraining influences on intentions not to comply with security policies.

A further addition to research in security behaviour came from the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975) according to which an individual's behavioural intention is guided by their attitude towards that behaviour and their subjective norm. The latter, in particular, was relevant to security behaviour, and captured the individual's desire to comply with how significant influential others thought they should behave.

With regard to organizational commitment, Herath and Rao (2009) identified it as a positive influence on security compliance behaviour. Porter *et al.* (1974), O'Reilly and Chatman (1986) and Meyer and Allen (1991), all share the views of Wiener (1982), in which organizational commitment is seen as the total internalised pressures in to behave in a way that satisfies the organization's goal and interest. Thus, having a strong organizational commitment will lead an employee to have a strong belief to follow the correct action whilst they belong in their organization (Wiener, 1982; Randall, 1987).

Meyer and Allen (1991) categorised organisational commitment into three types: affective, continuance, and normative. Affective commitment refers to the emotional attachment of an individual to his or her organisation. Continuance commitment reflects the intention of an individual to remain with their current organization due to the potential reward for staying outweighing the cost of leaving. Normative commitment refers to a felt obligation to stay as a member of an organization (Meyer and Allen, 1991). Along similar lines, O'Reilly and Chatman (1986) suggested that the bond between an employee with their organisation could be represented by compliance, identification and internalization.

Despite Herath and Rao's (2009) findings that employee organizational commitment had a significantly positive impact on IS security compliance and perceived effectiveness of action, Stanton *et al.* (2003) found to the contrary and attributed it to the possibility that committed employees may consider themselves entitled to have some level of freedom of behaviour. Nevertheless, the majority of indications are that high organizational commitment will be associated with high levels of compliance with recommended actions (Meyer & Allen, 1991).

3. Research model and hypotheses

The research model (Figure 1) embraces the fear elements of the threat appraisal and coping appraisal mechanisms. From an organizational perspective, the threat is towards the organization. However, the model includes the individual threat appraisal aspect of self-efficacy. In addition, they are personally affected by the perceived response costs that they would consider in deciding whether to embark upon security behaviours or not. They are furthermore influenced by their work colleagues in making such a decision. In weighing up the extent to which they will allow themselves to be influenced in the last two decisions, the individual is guided by their over-riding commitment to the organization.

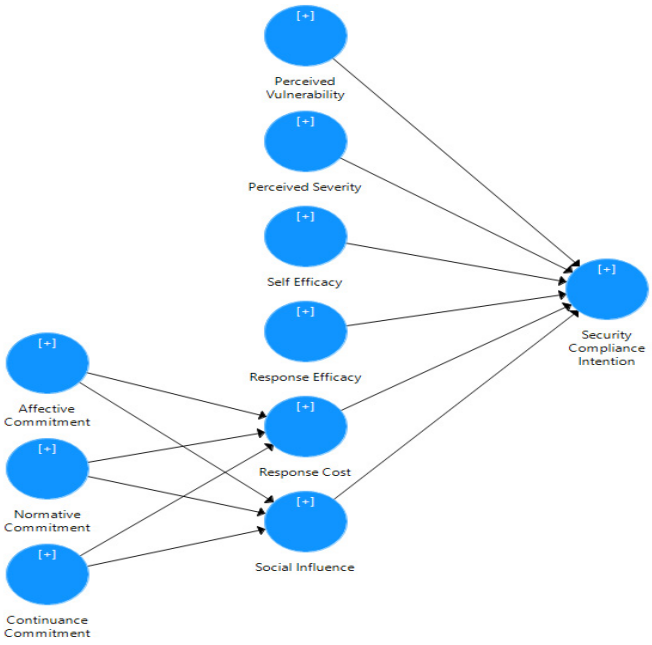

Figure 1: Research model

Wiener (1982) viewed organizational commitment as the total internalized pressures to behave in a way that satisfies the organization's goals and interests. This view was shared by Porter *et al*. (1974), O'Reilly and Chapman (1986) and Meyer and Allen (1991). Thus a strong organizational commitment will result in employees following organizational directions of appropriate actions (Randall, 1987). This has been found

to be the case with security policy compliance (Herath & Rao, 2009). Embracing Meyer and Allen's categorization of organizational commitment, we propose that if an individual is committed to the organization, he/she will not perceive the response cost of complying with security policies as being too large to warrant non-compliance. In addition, their organizational commitment will display a positive association with their desires to comply with the views of significant others, especially if these others are managers who are responsible for the execution of organizational policies.

> H1a: An increase in affective commitment will be negatively associated with perceived response costs
>
> H1b: An increase in affective commitment will be positively associated with social influence
>
> H2a: An increase in normative commitment will be negatively associated with perceived response costs
>
> H2b: An increase in normative commitment will be positively associated with social influence
>
> H3a: An increase in continuance commitment will be negatively associated with perceived response costs
>
> H3b: An increase in continuance commitment will be negatively associated with social influence

As Rogers (1983) maintained, and as ascertained by a number of researchers (Workman *et al*., 2008; Lee and Larsen, 2009; Herath and Rao, 2009; Ifinedo, 2012), an increase in how severe the threat is deemed to be by the individual, so his/her likelihood of adopting protection measures will increase.

> H4: An increase in perceived threat severity will be positively associated with security compliance intention

In appraising the threat, the perceived vulnerability will determine the extent of response. If an individual perceives that they are likely to be affected by a threat, then they are likely to adopt protective measures (Lee and Larsen, 2009; Ifinedo, 2012, Herath and Rao, 2009; Pahnila *et al.,* 2007).

> H5: An increase in perceived threat vulnerability will be positively associated with security compliance intention

When individuals feel capable of adhering to security policies, they are more likely to adopt those policies and security behaviours (Ifinedo, 2012; Siponen *et al*., 2014).

> H6: An increase in perceived self-efficacy will be positively associated with security compliance intention

Like Rogers (1983), Ifinedo (2012) and Herath and Rao (2009, we argue that if an individual deems that following certain preventative actions will reduce their chances of suffering damage from the threat, then they are likely to follow those actions.

> H7: An increase in perceived response efficacy will be positively associated with security compliance intention

Rippetoe and Rogers, 1987) argued that the cost of performing security compliance behaviour might be perceived as too onerous or inconvenient to lead to that behaviour. Like Burns *et al*. (2017) we argue that:

> H8: An increase in perceived response costs will be positively associated with security compliance intention

The influence of others on one's actions has been recognized as a strong motivational force (Fishbein & Ajzen, 1975). As such, it has been found that others' notions of appropriate action has had a strong positive influence on employees' intentions to comply with security policies (Ifinedo, 2012; Safa *et al.,* 2016)

> H9: An increase in social influence perceived vulnerability will be positively associated with security compliance intention

4. Data collection

An online survey was used to gather the data for this research. The items were drawn from validated research instruments which had been published. Ten instruments from previous research were used to form the instrument of this research. The perceived severity (PS), perceived vulnerability (PV), response efficacy (RE), and response efficacy were adapted from Workman et al. (2008) and Ifinedo (2012). Self-efficacy (SE), social influence (SI) and response cost were adapted from Bulgurcu *et al.* (2010) and Herath and Rao (2009). The organizational commitment sub-categories were adopted from Allen and Meyer (1990). Each of the items was measured using a seven-point Likert scale option. The instrument was pre-tested on 12 post-graduate students, the majority of whom were part-time students and employed in various organizations in both the private and public sector. Minor wording clarification was required for a couple of questions.

The intended sample for this research included members of public and private organizations who used computers as a part of their job routine. The survey participants were obtained by emailing invitations to the CEOs of five large, randomly selected organizations in New Zealand. Most emails were forwarded to an IT manager or an HR manager and if they agreed to participate, they were asked to distribute an invitation, containing a link to the research survey, via their corporate intranet. Employees who decided to participate were directed to the Qualtrics

questionnaire page. The survey was anonymous. An estimated 2,400 potential respondents received the invitation.

A total of 204 questionnaires were returned, of which 182 were usable, the rest having too large a portion of data missing. Twelve missing values in the 182 questionnaires were replaced with means.

5. Results and analysis

The results were analysed using structural equation modelling (SEM) which used a component-based variance method, referred to as partial least squares (PLS). First the measurement model was assessed to determine the validity of the various constructs. Then the structural model was assessed to determine the relationships between the constructs and the predictive validity of the model.

Convergent validity is the extent to which multiple measures of a construct are in agreement (Bagozzi at al. 1992). With reflective factors, as used in this model, for the factors to demonstrate convergent and discriminant validity, item loadings should have been at least 0.6 onto the relevant factor. All items loaded strongly onto their respective constructs, the majority being over 0.7 and so none was deleted.

In PLS analysis, convergent validity is also determined by examining the square root of the average variance extracted (AVE) of each construct, which should be above 0.7 (Fornell and Larcker 1981). All values were over 0.7. Another method for evaluating convergent validity is according to the composite reliability of the constructs, which should be above 0.7. These values were all above 0.8 and thus demonstrated an acceptable level of composite reliability.

The discriminant validity of the measurement model was determined by examining the correlations between constructs and ensuring that the square root of the AVE of a construct was greater than the correlations between the construct and other constructs (Siponen *et al.,* 2014). All the square roots of the AVEs were higher than the correlations of the relevant factor with the other factors.

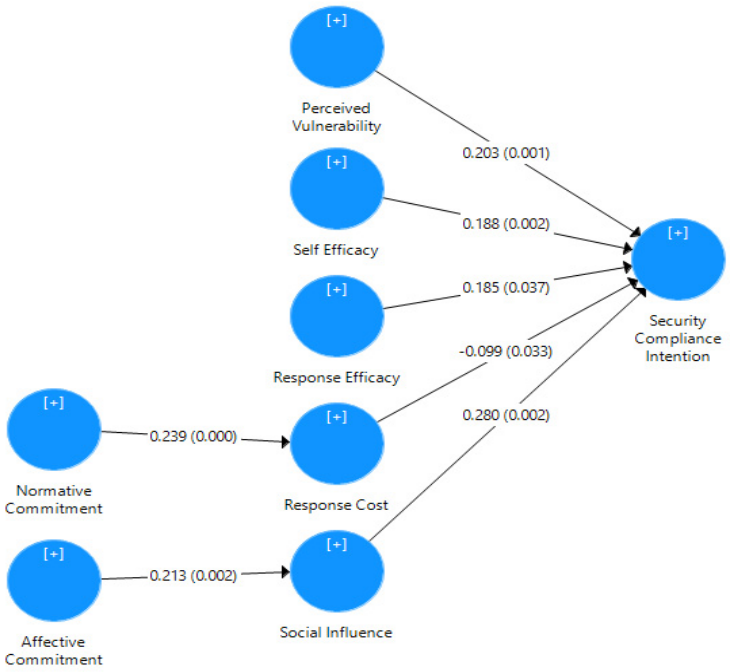

Figure 2: Refined model

To assess the structural model, we examined the predictive ability of the model in terms of the explanatory effect of the independent variables on the dependent variables, as well as the strength of the paths between constructs and their significance. The explanatory effect was determined by examining the explained variance in the dependent variable which should be above 0.1. The path coefficient provides an indication of the path strength and Hair *et al.* (2013) suggest that the minimum level for an individual R^2 should be greater than a minimum acceptable level of .10. A bootstrap procedure was applied to assess the significance of the paths between the constructs. Not all paths were sufficiently strong, nor were they all significant. Accordingly, while hypotheses H1a, H2b, H3a, H3b and H4 were not supported, all the other hypotheses were supported.

The weak and non-significant paths were thus deleted. The resultant model is depicted in Figure 2. The overall predictive ability (R^2) of the model in terms of security compliance intention is good at 0.45, and while normative commitment and affective commitment account for relatively small variance in response cost (0.09) and social influence (0.052) respectively, it is understandable that there would be many other factors influencing these variables.

6. Discussion and conclusion

This research tested a model and accompanying hypotheses that depicted the threat appraisal elements of perceived threat severity and perceived vulnerability; and the coping appraisal elements of perceived response efficacy, perceived self-efficacy and response cost as exerting an influence on employees' security compliance intentions.

In addition, social influence was hypothesized as influencing those intentions. In order to address the personal relevance of the perceived organizational threat, organizational commitment was proposed as exerting an influence on both response cost and social influence. In testing the model, organizational commitment was broken down into its three component types: affective commitment, continuance commitment and normative commitment.

As could be expected, the previously well-validated constructs of perceived vulnerability, response efficacy, self-efficacy, and social influence all exerted a positive influence on security compliance intention. Also to be expected, response cost exerted a negative influence on that intention. However, perceived threat severity failed to demonstrate any significant relationship with compliance intention. This could be, as Johnston *et al.* (2015) suggested, because the threat was not perceived as particularly relevant to them personally and they could thus even ignore it.

When broken down into its separate components, normative commitment was the only organizational commitment type to influence response cost. That could have been because normative commitment encapsulates an element of obligation, and any feeling of obligation to the organization would override any cost felt when responding to the threat. On the other hand, social influence could be construed as being more personal than any of the other independent variables influencing compliance. Thus it is not surprising that affective commitment, or the emotional attachment to the organization, exerted an influence on social influence. It is also understandable how continuance commitment might not exercise any influence on either response cost or social influence because even though the individual had made up his/her mind to stay with the organization, provided the costs of doing so weren't too high, the response cost or non-compliance with the views of significant others might be less easy to influence .In fact, the hypotheses' directions might well be reversed in future research.

This research was exploratory and has opened up a number of avenues for future research. In particular, it has rendered the fear appeal of the threat more personally relevant through the application of organizational commitment and it has offered a way to explore the nuances of organizational commitment and their influence on security compliance intention more deeply.

7. References

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

Ajzen, I. and Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. Prentice-Hall, Englewood Cliffs, NJ.

Allen, N.J. and Meyer, J.P. (1990), "Organizational socialization tactics: A longitudinal analysis of links to newcomers' commitment and role orientation", *Academy of Management Journal*, Vol. 33, No. 4, pp847-858.

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

Bagozzi, R.P., Davis, F.D. and Warshaw, P.R. (1992), "Development and test of a theory of technological learning and usage", *Human Relations,* Vol. 45, No. 7, pp659-686.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G. 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.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34, No. 3, pp523-548.

Burns, A.J., Posey, C., Roberts, T.L. and Lowry, P.B. (2017), "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals", *Computers in Human Behavior*, Vol. 68, pp190-209.

Fishbein, M. and Ajzen, I. (1975). Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research. Addison-Wesley, Reading, MA.

Fornell, C., and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 48, pp39-50.

Hair, J.F., Hult, G.T.M, Ringle, C. and Sarstedt. M.2013. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage Publications, London.

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.

Hsu, J.-S., Shih, S.-P., Hung, Y.W. and Lowry, P.B. (2017), "The role of extra-role behaviors and social controls in information security policy effectiveness", *Information Systems Research*, Vol. 26, No. 2, pp282-300.

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.

Janz, N.K. and Becker, M.H. (1984), "The health belief model: a decade later", *Health Education Behavior,* 11, No. 1, pp1-47.

Johnston, A.C., and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34, No. 3, pp549-566.

Johnston, A.C., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric", *MIS Quarterly*, Vol. 39, No. 1, pp113-134.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems,* Vol. 18, No. 2, pp177-187.

Lowry, P.B., Posey, C., Bennett, R.J. and Roberts, T.L. (2015), "Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust", *Information Systems Journal*, Vol. 25, pp193-230.

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, pp469-479.

Meyer, J.P. and Allen, N.J. (1991), "A three-component conceptualization of organizational commitment", *Human Resource Management Review*, Vol. 1, No. 1, pp61-89.

O'Reilly, C.A. & Chatman, J. (1986), "Organizational commitment and psychological attachment: The effects of compliance, identification, and internalization on prosocial behaviour", *Journal of Applied Psychology*, Vol. 71, No. 3, p492.

Pahnila, S., Siponen, M. and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In Spargue, R. H. Jr, ed. Proceedings of the 40th Hawaii International Conference on Systems Sciences (HICSS 2007) IEEE, Los Alamitos, CA, p156b.

Porter, L.W., Steers, R.M., Mowday, R.T. and Boulian, P.V. (1974), "Organizational commitment, job satisfaction, and turnover among psychiatric technicians", *Journal of Applied Psychology*, Vol. 59, No. 5, p603.

Randall, D.M. (1987), "Commitment and the organization: The organization man revisited", *Academy of Management Review*, Vol. 12, No. 3, pp460-471.

Rippetoe, P.A., and Rogers, R.W. (1987), "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat", *Journal of Personality and Social Psychology,* Vol. 52, No. 3, pp596-604.

Rogers, R.W. (1975), "A Protection Motivation Theory of fear appeals and attitude change", *Journal of Psychology*, Vol. 91, No. 1, pp93-114.

Rogers, R.W. (1985), "Attitude change and information integration in fear appeals", *Psychological Reports*, Vol. 56, No. 1, pp179-182.

Safa, N.S., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers & Security*, Vol. 56, pp70-82.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees' adherence to information security policies: An exploratory field study", *Information & Management*, Vol. 51, No. 2, pp217-224.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24, No. 2, pp124-133.

Wiener, Y. (1982), "Commitment on organizations: a normative view", Academy of Management Review, Vol. 7, No. 3, pp418-428.

Willison, R. and Warkentin, M. (2013), "Beyond deterrence: An expanded view of employee computer abuse", *MIS Quarterly,* Vol. 37, No. 1, pp1-20.

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.