Employees' Intended Information Security Behaviour in Real Estate Organisations: a Protection Motivation Perspective

Full Paper

Deepa Mani
University of South Australia
deepa.mani@mymail.unisa.edu.au

Alireza Heravi
University of South Australia
alireza.heravi@mymail.unisa.edu.au

Sameera Mubarak
University of South Australia
sameera.mubarak@unisa.edu.au

Kim-Kwang Raymond Choo
University of South Australia
raymond.choo@unisa.edu.au

ABSTRACT

Due to the amount of identifiable customer personal, financial and other information stored by real estate organisations in their information systems, the threats are real. Challenges to secure the organisational (and customer) data are compounded by the nature of the industry (e.g. the core business and employees' qualifications are non-security-related). To investigate the factors that influence real estate employees' intended information security behaviour, we propose a research model based on Protection Motivation Theory (PMT) where we also include previous incidents as constituting threat appraisal components. Our findings from a survey of 105 real estate business employees in Australia reveal that perceived vulnerability, perceived severity, previous incidents, and response efficacy have a positive impact on real estate employees' information security behavioural intention whereas self-efficacy does not. Our study also determines that response cost has a negative significant effect on intended information security behaviour.

Keywords

Information security behavioural intention, Protection motivation theory, Real estate organisations, Structural equation modeling.

Introduction

Real estate organisations in their daily business operations use information systems to store collect and transmit customers' data. In Australia, real estate organisations routinely collect personally identifiable information (PII), financial information and other personal details of their customers when they rent, buy, or sell a property. Documents submitted by customers include photocopies of passport, driver's license, credit card, bank statements, letter of employment detailing the place of work and the salary earned, utility and phone bills, and healthcare card. Therefore, there is a clear need for organisations that collect and store PII and other sensitive personal information to ensure that there is an adequate data security and privacy system in place. Banks, financial institutions and other security-related or conscious organisations generally have established information security policies and practices in place (Abbas 2014; Anderson and Moore 2006; Choo 2011; Salvi 2013). In the real estate sector, however, our earlier studies revealed that information security policies are not well practiced or may not exist at all (Mani et al. 2014a, 2015). In one of our studies, we found that large real estate businesses (i.e. more than 100 employees, annual turnover of more than 5 million AUD) generally have information security policies but do not fully practice them, and medium size (i.e. 20-100 employees, annual turnover 3-5 million AUD) and small size organisations (i.e. 6-20 employees, annual turnover of less than 3 million AUD) do not generally have such policies (Mani et al. 2014a). Lack of an information security culture or awareness can lead to information security breaches. In August 2013, for example, the system of one real estate organisation in

the UK was hacked and resulted in 10,000 customer usernames, passwords and email addresses being compromised (Leyden 2013).

Challenges to ensure the security and privacy of customer data are compounded by the non-IT-focused and mobile nature of the real estate industry. For example, in the United States, a company laptop was stolen from one real estate employee. The stolen laptop contained unencrypted personal information, including social security numbers for more than 600 residents. The organisation was subsequently fined $15,000 for not encrypting the laptop and for failing to follow its own written information security program (Larose and Veness 2012). When the information systems of real estate organisations are compromised, the risk is not only to those of their customers. For example, in August 2014, the system of a real estate company was reportedly affected by a malware which allowed the cybercriminals to access the company's online banking system and steal $50,000 (Jennings 2014). A breach or a security incident could potentially expose the real estate organisations to reputational, financial, and regulatory risks. Reputational risk refers to how negative an organisation might be perceived by their customers, financial risk refers to the amount of money that an organisation might lose, and regulatory risk refers to the penalties due to criminal investigations or civil litigations (Tipton 2011).

Technological measures such as firewalls, antivirus software, and anti-spam filters may be commonly deployed by real estate organisations, but technological protections are unlikely to adequately protect an organisation against the myriad of security threats. As explained by researchers such as Imgraben, Engelbrecht and Choo (2014), Ifinedo (2012), Martini and Choo (2014), and Ng, Kankanhalli and Xu (2009), the diversity of attack vectors and threat actors necessitates upskilling of the workforce and embedding a culture of security in the organisation. Such measures will help mitigate insider-related security threats and reduce the likelihood of unintentional actions (e.g. clicking on a suspicious email attachment).

A number of studies suggested introducing policies and employees' security policy compliance behaviour to mitigate insider risks (Workman et al. 2008). Recent studies of real estate organisations in Australia, however, found that they are generally ill-equipped to implement or enforce information security policies and the level of security awareness is generally very low (Mani et al. 2014a, 2014b).

It is therefore necessary to understand the factors that positively influence or motivate real estate industry employees' information security awareness in Australia. This is the aim of this study. We use Protection Motivation Theory (PMT) (Rogers 1975) as the underlying theoretical lens to determine the behaviour of real estate organisation employees in the event of a security breach. We also examine the influence of threat and coping appraisal (see Figure 1). We also include the "lesson learned from a previous incident" component as part of the threat appraisal of PMT because we believe that people would be more aware of the threat if they were previously victimised. For example, previous research in the health sciences has determined that past experience has a significant influence on current experience (Dimsdale 2000; Dolan and Tsuchiya 2005; John 1992).

The paper is organised as follows. The next two sections present an overview of protection motivation theory, and the research methodology and findings, respectively. In the last section a brief discussion of the findings is presented.

Theoretical Background and Hypotheses

PMT

Protection Motivation Theory (PMT), first proposed by Ronald Rogers in 1975, examined how fear or a threat of danger leads to changes in attitude (Rogers 1975). The theory suggests that the severity of a threat, the probability of the occurrence of a threat, and the effectiveness of a protective response can cause a cognitive mediation process in individuals who is motivated to protect oneself from the potential threat (Chenoweth et al. 2009). In other words, PMT can be used to determine whether one should take precautions or to ignore the warnings based on a risk-benefit analysis of the situation. One key concept in the theory is that individuals are motivated to protect themselves if they feel threatened in risky scenarios. There are, according to the theory, two cognitive processes encouraging people to participate in actual protection behaviour: threat appraisal and coping appraisal (Rogers 1983). Firstly, threat appraisal defines an individual's assessment of the level of threat posed by a threatening event (Maddux and Rogers, 1983). The components of the threat appraisal are *perceived vulnerability* and *perceived severity*. Secondly, coping appraisal describes the individual's /organisation's assessment of the ability to cope with

the potential damage the threat poses (Woon et al. 2005). Coping appraisal consists of three components, *self-efficacy*, *response efficacy*, and *response cost*. Both cognitive processes are equally important since a person will adopt a suggested coping behaviour only when he or she believes that the threat is serious. Hence, the two cognitive processes result in the intention to enact adaptive response behaviours (Lee et al. 2008). However, some medical researchers support the view that coping appraisal components such as self-efficacy, response efficacy and response costs have greater predictive validity than threat appraisal components (Chenoweth et al. 2009; Milne et al. 2000; Floyd et al. 2000).

PMT has been widely used in a diverse range of studies ranging from healthcare-related threats (Milne et al. 2000; Plotnikoff et al. 2010) to environmental hazards (Vaughan 1993) to security policy compliance in organisations (Herath and Rao 2009) to anti-plagiarism software (Lee 2011) to home wireless security (Woon et al. 2005). By applying this theory with reference to intended information security behaviour in real estate organisation employees, we believe that it will be possible to determine the factors that motivate these employees to adopt information security measures. Our research model is illustrated in Figure 1.

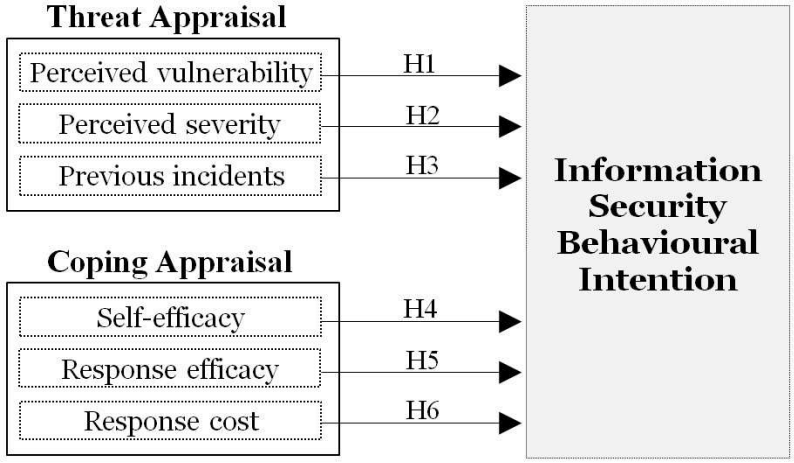

Figure 1. Research Model

Threat Appraisal

Perceived Vulnerability

Perceived vulnerability is the probability to which a person believes threatening incidents will occur to the individual (Lee et al. 2008). Therefore the likelihood of adopting the necessary protection increases when a person perceives he or she will experience higher vulnerability (Lee 2011). For example, past studies have revealed significant effects on the intention to use anti-spyware software (Chenoweth et al. 2009), virus protection behaviour (Lee et al. 2008), and anti-malware software (Lee and Larsen 2009). In this study, we will examine whether employees believe a threat to their organisation and their customers is more likely to lead to the adoption of information security measures. We hypothesise that:

H1: Perceived vulnerability positively influences real estate organisation employees' information security behavioural intention.

Perceived Severity

Perceived severity refers to the magnitude of the consequences of an incident if the threat succeeds (Milne et al. 2000). In this study, the consequences are damage to the organisation's reputation, compromise and leakage of customers' data and financial records, etc. The more an individual perceives the threat can significantly damage them, their customers and their organisation, the individual is more likely to be concerned (Herath and Rao 2009). Hence, we hypothesise that:

H2: Perceived severity positively influences real estate organisation employees' information security behavioural intention.

Previous Incident

A prior unpleasant experience (in our context, victim of a previous security incident) makes individuals take their subsequent security measures more seriously (Weinstein 1989). Employees who have experienced a real threat are more cautious than individuals who only have a ("theoretical") knowledge about a threat. Therefore, in our model, we include previous incidents as a component of the threat appraisal. We hypothesise the following:

H3: A previous incident positively influences real estate organisation employees' information security behavioural intention.

Coping Appraisal

Self-efficacy

Self-efficacy refers to the expectancy of an individual's ability to perform the recommended task; hence, when an individual believes he or she has the skills to do that task, the individual will take the necessary action (Lee et al. 2008). Researchers have determined that self-efficacy can be a predictor of behaving with the intention to implement virus protection (Lee et al. 2008) in an effort to make information security more effective (Workman et al. 2008). Further, from the employees' policy compliance perspective, there is a positive relationship between self-efficacy and behavioural intent (Bulgurcu et al. 2010). Since self-efficacy posits employees' knowledge about malicious attacks and information security policies, we hypothesise that:

H4: Self-efficacy positively influences real estate organisation employees' information security behavioural intention.

Response efficacy

Response efficacy refers to a belief that the recommended preventive measures will be effective in protecting oneself or others from an undesirable threat (Woon et al. 2005). For example, in our context, these include adopting information security measures such as backing up of organisation data, participating in training, and employees complying with information security policies to enhance the information security in their workplace. Consequently, we hypothesise that:

H5: Response efficacy positively influences real estate organisation employees' information security behavioural intention.

Response cost

Response cost is the perceived cost incurred by a user in performing a recommended coping behaviour (Chenoweth et al. 2009). When an employee believes that the recommended coping mechanism provides protection from a threat, then that individual is more likely to follow the adaptive behaviour (Ifinedo 2012). On the other hand, if the employee has less trust in a measure's efficacy, then the individual may not be willing to accept it (Rippetoe and Rogers 1987). Accordingly, employees who believe that the information security is necessary and coping mechanisms will reduce threats are more likely to follow it (Herath and Rao 2009). Thus, we hypothesise that:

H6: Response cost negatively influences real estate organisation employees' information security behavioural intention.

Research Methodology

Data collection

The survey was conducted in three Australian states, namely South Australia, Western Australia, and New South Wales. The questionnaire was published in the weekly email newsletter by the real estate industry's peak bodies of South Australia (Real Estate Institute of South Australia- REISA) and Western Australia (Real Estate Institute of Western Australia-REIWA). In New South Wales we directly contacted the real estate business through email. A total of 105 real estate organisation employees responded to the survey. Table 1 shows the breakdown of survey respondents by state, organisation size and job position.

Category	Subcategory	Frequency	Percentage
Australian jurisdiction	South Australia	55	52%
	Western Australia	26	25%
	New South Wales	24	23%
Organisation size	Micro Organisation	30	29%
	Small Organisation	44	42%
	Medium Organisation	18	17%
	Large Organisation	13	12%
Job position	Managing Director	11	10%
	Property Manager	16	15%
	Salesperson	23	22%
	Owner/Manager	55	53%

Table 1. Respondents' demographic details (n = 105)

We developed the measurement scales based on a comprehensive literature review and wherever possible we used existing scales. However, we had to change or create some scales so that they fitted the context of this study (see Appendix A).

Data Analysis and Results

Reliability and Validity

The data analysis was performed using the SmartPLS software package (Ringle et al. 2005) and SPSS 21. With the data gathered from real estate organisation employees, the individual constructs were tested for reliability, convergent validity, and discriminant validity. Cronbach's alpha (Cronbach 1951) was used for reliability analysis to examine each construct's internal consistency measure. Results in Table 2 indicated that the constructs ranged from 0.69 to 0.96.

Construct	No. of items	Cronbach's Alpha (α)
Perceived Vulnerability (PV)	3	0.96*
Perceived Severity (PS)	2	0.92*
Previous Incidents(PI)	2	0.90*
Self-Efficacy (SE)	2	0.93*
Response Efficacy (RE)	3	0.93*
Response cost (RC)	2	0.69***
Information Security Behavioural Intention (ISBI)	3	0.78**

Table 2. Reliability of Constructs

Note: * Cronbach's alpha level $\alpha \geq 0.9$ is considered to be an excellent indicator of internal consistency

** Cronbach's alpha level $0.7 \leq \alpha < 0.9$ is considered to be a good indicator of internal consistency

*** Cronbach's alpha level $0.6 \leq \alpha < 0.7$ is considered to be an acceptable indicator of internal consistency (George and Mallery 2003; Kline 2013)

Convergent validity specifies the degree to which a measure correlates with other measures and is considered to be adequate if the standardised factor loadings are above .50 (Anderson et al. 1998). Table 3 confirms that the factor loadings are adequate. The convergent validity was also assessed by Average Variance Extracted (AVE). The data analysis shows that the AVE and the composite reliability (CR) of all the constructs have adequate convergent validity since both values were above the recommended 0.5 and 0.6 levels, respectively.

Item	PV	PS	PI	SE	RE	RC	ISB
PV1	**0.969**	0.120	0.128	-0.028	0.104	-0.096	0.220
PV2	**0.963**	0.163	0.199	-0.013	0.085	-0.118	0.224
PV3	**0.945**	0.069	0.121	0.032	0.033	-0.109	0.174
PS1	0.127	**0.969**	0.162	0.219	0.087	-0.129	0.270
PS2	0.115	**0.955**	0.137	0.184	0.031	-0.042	0.224
PI1	0.183	0.167	**0.964**	0.172	0.157	-0.186	0.325
PI2	0.110	0.126	**0.940**	0.085	0.089	-0.166	0.254
SE1	-0.044	0.256	0.184	**0.956**	0.127	-0.040	0.136
SE2	0.022	0.166	0.101	**0.976**	0.173	-0.039	0.185
RE1	0.114	0.036	0.169	0.114	**0.920**	-0.081	0.305
RE2	0.022	0.070	0.132	0.190	**0.959**	-0.164	0.371
RE3	0.099	0.071	0.078	0.134	**0.932**	-0.116	0.335
RC1	-0.138	-0.072	-0.221	-0.006	-0.139	**0.903**	-0.242
RC2	-0.046	-0.094	-0.087	-0.074	-0.083	**0.832**	-0.187
ISA1	0.118	0.234	0.238	0.044	0.383	-0.263	**0.856**
ISA2	0.116	0.078	0.245	0.187	0.260	-0.175	**0.806**
ISA3	0.291	0.300	0.285	0.205	0.250	-0.178	**0.830**

Table 3. Factor loadings

Discriminant validity states the degree to which a construct is not correlated with other constructs (Fornell and Larcker 1981) and was assessed by comparing the square root of the AVE with each construct's correlation. As shown in Table 4, the discriminant validity of the constructs is sufficient because the square root of the AVE for each construct is larger than its correlation with other constructs. Consequently, the measurement model demonstrates adequate validity that is required for further testing.

Construct	CR	AVE	PV	PS	PI	SE	RE	RC	ISBI
PV	0.97	0.92	**0.96**						
PS	0.96	0.93	.123	**0.96**					
PI	0.95	0.91	.153	.154	**0.95**				
SE	0.97	0.93	-.010	.219	.144	**0.96**			
RE	0.96	0.88	.080	.062	.131	.153	**0.94**		
RC	0.86	0.75	-.100	-.094	-.167	-.050	-.122	**0.86**	
ISBI	0.87	0.69	.202	.242	.301	.163	.361	-.241	**0.83**

Table 4. Composite Reliability, AVE, and Inter Item Correlations

Note: CR= Composite Reliability, AVE= Average Variance Extracted, Bold fonts in the leading diagonals represent the square root of AVE.

Assessment of the structural model

Structural Equation Modeling (Anderson and Gerbing 1988) was employed using the SmartPLS 2.0.M3 (Ringle et al. 2005) software package to test the hypotheses. The Partial Least Squares (PLS) and bootstrapping test were respectively employed for the analysis. The hypothesised path significance levels (t-values) were calculated by the bootstrapping test while the PLS analysis indicates how well the measures relate to each construct (Rusu and Shen 2011). The computed results are shown in Table 5. The outcomes obtained in this study confirm that the research model is structurally sound.

Hypothesis	Hypothesised path	Path coefficient(β)	t-value	Result
H1	PV ⟶ ISBI	0.127*	2.935	Supported
H2	PS ⟶ ISBI	0.170*	3.901	Supported
H3	PI ⟶ ISBI	0.189**	4.197	Supported
H4	SE ⟶ ISBI	0.057	1.153	Not Supported
H5	RE ⟶ ISBI	0.287**	7.132	Supported
H6	RC ⟶ ISBI	-0.145*	3.700	Supported

Table 5. Summary of the findings

Note: ** indicates that the item is significant at $p<0.01$, and * at $p<0.05$.

Discussion and Implications

This study investigates the factors that influence real estate organisation employees' information security behavioural intention. In this study, a model with threat and coping appraisal based on PMT was proposed. Analysis shows that five out of the six proposed hypotheses were supported. Perceived vulnerability, perceived severity, previous incident, and response efficacy had a positive effect on employees' information security behavioural intention.

The data analysis strongly supported hypothesis H1, which shows that there is a positive relationship between perceived vulnerability and employees' information security behavioural intention. The finding suggests that employees who believe a threat to their organisation will affect their customers are more likely to engage in information security behaviours. Our findings echoed observations reported by Chenoweth, Minch and Gattiker (2009) and Ifinedo (2012).

As shown in Table 5 the perceived severity also has a positive effect on information security behaviours and therefore supports hypothesis H2. The data analysis indicated that it had a good statistical result (t-value) and the direction of the path strength (positive) is also consistent with the prediction made. Employees, who believe that losing information or adopting unsafe behaviours (e.g. clicking on unknown on-line links or suspicious email attachments) is dangerous, are more likely to take appropriate steps to implement information security measures.

Likewise, our results indicated that there is a positive relationship between previous incidents and information security behavioural intention; thus Hypothesis 3 is supported. Employees who had experienced information security threats are more likely to engage in information security behaviours. This also suggested that most employees are following a reactive approach; in other words, taking remediation steps only after an incident had occurred.

We found that self-efficacy did not positively influence employees' information security behavioural intention; thus, not supporting Hypothesis 4. The t-values related to self-efficacy did not lead to a good statistical outcome. This finding is similar to that reported in the study by Chenoweth, Minch and Gattiker (2009). They contended that the behavioural intention to use anti-spyware software is not significant as it is difficult to install and maintain this kind of software. In our context, self-efficacy measures an individual's ability, such as real estate organisation employees' qualifications and actual job scope are not related to information security. It is also possible that they may not be aware of current information security threats or the outcome might be due to our small research sample size. Proper and regular

information security training provided to real estate organisation employees can improve their self-efficacy when implementing information security.

As shown in previous security-related studies, response efficacy had a strong impact on employees' information security behavioural intention, and consequently H5 is supported. These results imply that employees will improve their intention if they believe that the recommended preventive measures will be effective in protecting them from an undesirable threat. This finding is similar to those of previous studies, which also found response efficacy to be significant (Ifinedo 2012).

The hypothesised (H6) negative impact of response cost on information security behavioural intention was also supported by the data. In other words, if employees are more concerned with response cost because effort or difficulty is too much, then their intention to follow adequate security measures may decline (Chenoweth et al. 2009).

The findings of the study have important implications for real estate organisations. From their perspective this study identifies gaps and provides further insights which can facilitate designing their information security policies. For example, it is important for employees to have regular and ongoing training to update their knowledge about cybersecurity threats. Crossler et al. (2013) also highlighted that for protecting and mitigating threats to information systems, it is necessary to provide regular information security training to employees to improve their awareness and efficacy.

Drawing on PMT, we offered a research model where the previous incident was considered to be a component of threat appraisal. We developed a scale to examine the effects of the previous incident on the information security behavioural intention.

The findings indicated that threat appraisals have a particularly stronger impact than coping appraisal on employees' intended behaviour to implement information security. The outcomes of our research are, to some extent, consistent with the findings of previous studies (Lee 2011), which found that threat appraisal variables exerted more significant influence than coping appraisal.

Conclusion

This study investigates the factors that influence real estate organisation employees' information security behavioural intention using a model based on Protection Motivation Theory (PMT). Our findings indicated that perceived vulnerability, perceived severity, previous incident, and response efficacy positively influence real estate employees' information security behavioural intention. Conversely, response cost negatively influences real estate employees' information security behavioural intention. Thus, the findings from our study indicated that threat appraisal has greater predictive validity than coping appraisal, and suggested that information security training for employees enhances their information security behavioural intention.

Future work would include extending the study to other Australian states and territories (e.g. Australian Capital Territory, Queensland, Northern Territory, Tasmania, and Victoria) to obtain statistically sound national data and a much broader national understanding of the current and emerging information security threats faced by the real estate sector in Australia.

REFERENCES

Abbas, K. 2014. "Middle East Bank Improves Information Security" (available online at www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-1-January-2014.aspx/, accessed on January 01,2015).

Anderson, R., and Moore, T. 2006. "The economics of information security," *Science*, (314:5799), pp. 610-613.

Anderson, James C, and Gerbing, David W. 1988. "Structural equation modeling in practice: A review and recommended two-step approach," *Psychological Bulletin, (*103:3), pp. 411- 423.

Anderson, Rolph E, Black, William C, Hair, Joseph F, and Tatham, Ronald L. (1998). *Multivariate data analysis*: Prentice-Hall, London.

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* (34:3).

Chenoweth, T., Minch, R., and Gattiker, T. 2009. "Application of protection motivation theory to adoption of protective technologies," in *HICSS'09, 42nd Hawaii International Conference on System Sciences, Waikoloa, Big Island, Hawaii, USA*, IEEE, pp. 1-10.

Choo K-K R 2011. "Cyberthreat landscape faced by financial and insurance industry", *Trends & Issues in Crime and Criminal Justice* no 408: 1–6.

Cronbach, Lee J. 1951. "Coefficient alpha and the internal structure of tests," *Psychometrika, (*16:3), pp. 297-334.

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* (32), pp. 90-101.

Dimsdale, Joel E. 2000. "Stalked by the past: the influence of ethnicity on health". *Psychosomatic Medicine, (62*:2), pp. 161-170.

Dolan, Paul, and Tsuchiya, Aki. 2005. "Health priorities and public preferences: the relative importance of past health experience and future health prospects". *Journal of Health Economics, (*24:4), pp.703-714.

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* (30:2), pp. 407-429.

Fornell, Claes, and Larcker, David F. 1981. "Evaluating structural equation models with unobservable variables and measurement error". *Journal of Marketing Research,(* 18:1), pp. 39-50.

George, D. Mallery, P.(2003). *SPSS for Windows Step by Step: A Simple Guide and Reference 11.0 Update* (4th ed.). Boston: Pearson Education, Inc.

Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security* (31:1), pp. 83-95.

Imgraben, J., Engelbrecht, A., and Choo, K.-K. R. 2014. "Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users," *Behaviour & Information Technology* (33:12), pp. 1347– 1360.

Jennings, A. 2014. "Cyber thieves steal $50,000 from real estate agency." (available online at http://www.rebonline.com.au/breaking-news/7583-cyber-thieves-steal-50-000-from-real-estate-agency, accessed on February 20, 2015).

John, Joby. 1992. "Patient satisfaction: the impact of past experience". *Journal of Health Care Marketing, (*12:3), pp. 56-64.

Kline, P. 2013. *Handbook of psychological testing,* Routledge: London.

Larose, C., and Veness, A. 2012. "Massachusetts Attorney General Data Breach Investigation Results in $15,000 Settlement with Property Management Firm." (available online at http://www.privacyandsecuritymatters.com/2012/04/massachusetts-attorney-general-data-breach-investigation-results-in-15000-settlement-with-property-management-firm/, accessed on January 01, 2015).

Lee, D., Larose, R., and Rifon, N. 2008. "Keeping our network safe: a model of online protection behaviour," *Behaviour & Information Technology* (27:5), pp. 445-454.

Lee, Doohwang, Larose, Robert, and Rifon, Nora. 2008. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, (*27:5), pp.445-454.

Lee, Y. 2011. "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective," *Decision Support Systems* (50:2), pp. 361-369.

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* (18:2), pp. 177-187.

Leyden, J. 2013. "Hacked estate agency Foxtons breaks glass, pulls password reset cord," *The Register*, (available online at http://www.theregister.co.uk/2013/08/21/foxtons_password_reset/, accessed on October 3,2013).

Maddux, James E, and Rogers, Ronald W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology, (*19:5), pp. 469-479.

Mani, D., Choo, K.-K. R., and Mubarak, S. 2014a. "Information security in the South Australian real estate industry: A study of 40 real estate organisations," *Information Management & Computer Security* (22:1), pp. 24-41.

Mani D, Heravi A, Choo KKR and Mubarak S 2015. "Information Privacy Concerns of Real Estate Customers and Information Security in the Real Estate Industry: an Empirical Analysis", *In Proceedings of Australasian Information Security Conference (ACSW-AISC 2015),* pp. 53–56,

Sydney, New South Wales, Volume 161 of the ACS Conferences in Research and Practice in Information Technology (CRPIT) series, Australian Computer Society, 27 – 30 January.

Mani, D., Mubarak, S., and Choo, K.-K. R. 2014b, "Understanding the Information Security Awareness Process in Real Estate Organizations Using the SECI Model". in *20th Americas Conference on Information Systems, AMCIS 2014,* Savannah, Georgia, USA, pp. 1-11.

Martini, B., and Choo, K.-K. R. 2014, "Building the next generation of cyber security professionals". In *22nd European Conference on Information Systems (ECIS 2014),* Tel Aviv, Israel, pp. 1-13.

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* (30:1), pp. 106-143.

Mohamed, N., and Ahmad, I. H. 2012. "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior* (28:6), pp. 2366-2375.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems* (46:4), pp. 815-825.

Plotnikoff, R. C., Lippke, S., Trinh, L., Courneya, K. S., Birkett, N., and Sigal, R. J. 2010. "Protection motivation theory and the prediction of physical activity among adults with type 1 or type 2 diabetes in a large population sample," *British Journal of Health Psychology* (15:3), pp. 643-661.

Ringle, C., Wende, S., and Will, A. 2005. "Smart PLS 2.0 M3, University of Hamburg."

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* (52:3), pp. 596.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp. 93-114.

Rogers, R. W. 1983. "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation." In J. Cacioppo and R. Petty (eds.), *Social Psychophysiology*, Guilford Press, New York\, pp. 153-176.

Rusu, R. F., and Shen, K. 2011. "An empirical study on E-Banking acceptance in the United Arab Emirates (UAE)," *International Business Information Management Conference*, IBIMA Publishing, Australia, pp. 1-9.

Salvi, V. 2013. "Information Security Management at HDFC Bank: Contribution of Seven Enablers", (available online at www.isaca.org/Knowledge-Center/Documents/Information-Security-Management-at-HDFC%20Bank-Contribution-of-Seven-Enablers_1113.pdf/, accessed on January 01, 2015).

Tipton, H. F. 2011. *Official (ISC) 2® Guide to the ISSMP® CBK®*, CRC Press.

Woon, I., Tan, G.-W., and Low, R. 2005. "A protection motivation theory approach to home wireless security," *ICIS 2005 Proceedings*, Paper. 31, pp. 367-380.

Weinstein, N. D. 1989. "Effects of personal experience on self-protective behavior," *Psychological Bulletin* (105:1), pp. 31-50.

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* (24:6), pp. 2799-2816.

Appendix A - Measurement items

Construct	Items
Perceived Vulnerability (adapted from Ifinedo 2012)	PV1: I know a data breach in my organisation would have an adverse impact on our customers. PV2: The likelihood of a data breach in my organisation is… PV3: I could be subjected to a serious information security threat if I share passwords with others.
Perceived Severity (adapted from Mohamed and Ahmad 2012)	PS1: I believe that losing information or files from the computer would be a serious problem. PS2: Opening a link from an unknown source is a serious problem.
Previous Incidents (Self-developed)	PI1: I gained my awareness about information security threats through previous computer security incidents. PI2: The information security threats that happened before enhanced my intention to implement a precautionary measures
Self-Efficacy (adapted from Al-Omari et al. 2012)	SE1: I have the necessary knowledge to understand the existence of malicious attacks targeting mobile and portable devices. SE2: I have the necessary knowledge to understand the information security document policies of my organisation.
Response-Efficacy (adapted from Siponen et al. 2010)	RE1: Complying with information security policies keeps information security breaches to a minimum. RE2: Information security training for employees can reduce information security breaches. RE3: Backing up of data prevents the loss of information or files from our organisation.
Response cost (adapted from Vance et al. 2012)	RC1: The impact of information security policies on my work is… RC2: Complying with a formal information security-related policy would require considerable investment of effort apart from time.
Information Security Behavioural Intention (adapted from Ifinedo 2012)	ISBI1:I regularly update the antivirus software in my computer, and mobile and portable devices. ISB2: I am aware of the existence of malicious attacks (virus, worm, Trojan horse, etc.) targeting mobile and portable devices. ISB3: My organisation's data may be compromised if I don't pay adequate attention to information security policies.