WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View

Merrill Warkentin
Mississippi State University, m.warkentin@msstate.edu

Nirmalee Malimage
Mississippi State University

Kalana Malimage
Mississippi State University

Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View

Merrill Warkentin [1]
College of Business, Mississippi State University,
Mississippi State, MS, USA

Nirmalee Malimage
College of Business, Mississippi State University,
Mississippi State, MS, USA

Kalana Malimage
College of Business, Mississippi State University,
Mississippi State, MS, USA

ABSTRACT

IS security policy non-compliance is a problem experienced globally. Organizations have implemented formal and informal sanctions to enforce policy compliance. Sanctions can be positive (rewards) or negative (punishment) and may influence employees differently across different cultures. We propose an examination of antecedents that influence IS security policy compliance utilizing Protection Motivation Theory (PMT) and Deterrence Theory in a global context. Using six different countries, we plan to find if protection motivation and deterrence factors differ among different cultures through the influence of Hofstede's cultural dimensions.

Keywords: Informal Sanctions, Deterrence Theory, Protection Motivation, Cross-cultural research, Security Policy Compliance, Security Countermeasures.

[1] Corresponding author. m.warkentin@msstate.edu +1 662 325 3928

INTRODUCTION

Organizations continue to daily struggle protecting their information systems from various threats and spend billions of dollars to build defenses to counter these threats. Some of these threats include natural and manmade disasters, errors by internal employees, acts of competitors with malicious intent, hackers, spyware and viruses (Loch et al. 1992; Willison and Warkentin 2012). The reliance of organizations on information systems and increased connectivity of organizational information systems to the internet has increased the exposure to threats from hackers, spyware and viruses (Whitman 2003). The increased threats, along with increased reliance on information systems, have made most organizations enforce strong countermeasures to deter these threats. Measures such as physical controls and strict information security policies have been implemented across most organizations to counter threats to their information systems.

The threat landscape is further complicated by globalization – organizations have offices and conduct business operations in multiple countries and employ individuals from different cultures. In global organizations, special difficulties arise in creating and maintaining effective information security policies (Long 2004), due to differences in espoused values, traditions, and practices among business units, as well as variations in their political, economic and legal environments. Individual attitudes and behaviors, influenced by the national culture of each individual, have exacerbated these cross-cultural challenges as employees from different cultural backgrounds interpret global information security policies differently. Many studies have found that cultural differences significantly influence an individual's behavioral intention to perform secure actions and actual secure behaviors themselves because perceptions about certain facets of attitudes and behaviors differ in each culture. In IS research, cross-cultural studies have found that individual's cultural background significantly influences the design, adoption and use of information systems (Im et al. 2011; Jong-min 2004). In the context of information security, although many studies have looked at security policy compliance intention of employees using theories such as Protection Motivation Theory (Rogers 1975), Deterrence Theory (Straub and Nance 1990), Neutralization Theory (Siponen and Vance 2010), there have been few studies conducted that evaluated security-related behaviors across cultures, let alone the impact of cultural values on security policy compliance by individuals. A recent cross-cultural study on information systems misuse in the U.S and South Korea (Hovav and D'Arcy 2012) found that deterrent effects of certain security counter measures varied between the two countries along with age and gender, but the role of culture itself as a direct or indirect antecedent of secure behaviors was not evaluated.

The proposed study will focus on formal and informal sanctions which are also known as punishment or "negative sanctions." This study will also focus on formal and informal rewards which are also known as "positive sanctions." According to the Rational Choice Theory (RCT) and several other criminology theories, humans try to achieve pleasure (rewards/positive sanctions) and avoid pain (punishment/negative sanctions). Our study will investigate the differential effect of national culture on how protection motivation and rewards and punishment (formal and informal sanctions) will influence employees' intention to comply with organizational policies. How do employee compliance intentions differ across several unique countries with vastly different cultures? Under the right circumstances, various punishments (negative sanctions) have been shown to deter undesirable or deviant behavior. Both formal and informal sanctions are normally viewed only as negative tools by management (or by society).

But “sanctions” can encompass both positive and negative organizational events, as illustrated in Table 1. As exemplified in the table, while a demotion is a negative work-related sanction, a raise or promotion would be a positive one. Moreover sanctions can also be formal or informal. Being insulted for poor job performance is a negative informal sanction, but receiving pubic praise for good work performance is a positive sanction. Thus the objective of our study is to 1) determine if influences of protection motivation differs across cultures; 2) to determine if the influence of the presence of positive and negative formal and informal sanctions towards behavioral intentions differ across cultures; 3) to determine if the security policy compliance intentions influenced by protection motivation and presence of sanctions differ across different cultures.

Table 1. Examples of positive and negative formal and informal sanctions

	Rewards (Positive Sanctions)	Punishment (Negative Sanctions)
Formal	pay raise at the job, performance bonus, job promotion	reprimand, demotion, or employment termination
Informal	praise or recognition for a job well done	public ridicule or insult for bad job performance, social or self-disapproval

RESEARCH BACKGROUND

Protection Motivation Theory (Rogers 1975) and Deterrence Theory (Straub and Nance 1990; Straub 1990) form the primary foundations for the present study. Protection Motivation Theory (PMT) suggests that individuals act to avoid and prevent threats to their safety and security if and when they perceive that the threat is sufficiently severe and if they perceive that they are susceptible to the threat (Rogers 1975). In addition to the appraisal of threat severity and threat susceptibility, individuals also form perceptions of the recommended response to the threat by assessing their own individual capabilities (self-efficacy), coupled with an assessment of the effectiveness of the response (response efficacy) (Bandura and Adams 1977; Witte 1992; Witte et al. 1996). These two parallel appraisals, threat appraisal and coping appraisal, form the foundation for the individual user’s behavioral intention to carry out or execute the recommended response to the threat (Witte 1992, Witte 1996). Previous studies have shown that threat appraisal and coping appraisal variables, which are the foundation of the Protection Motivation Theory influence security behavior of individuals (Johnston and Warkentin 2010; LaRose et al. 2008; Lee and Larsen 2009; Woon et al. 2005; Workman et al. 2008). When individuals are facing a threat, they are likely to adopt protective behaviors or technologies to deter the threat.

Theory of Reasoned Action (TRA) (Ajzen and Fishbein 1980) and Theory of Planned Behavior (TPB) (Ajzen 1991), which explains the relationships between attitude, intention and behavior of individuals, have been used widely in IS research and IS security research as well. TPB defines attitude as an individual’s like or dislike towards a specific behavior and posits that attitude influences an individual’s intention to carry out that behavior. The relationship between attitude and behavioral intention has been tested in the context of information security where behavioral intention to comply with security policies was found to be significantly influenced by attitudes towards those policies (Bulgurcu et al. 2010; Herath and Rao 2009). Further, intention has been established as a primary antecedent of behavior.

Having information security policies in place will not protect an organization from security threats unless the employees actually follow them (Puhakainen and Siponen 2010). Employees who are aware of their organization's IS security policies may still violate them in certain instances. General Deterrence Theory (GDT), borrowed from the criminology discipline, has been used by IS security researchers to identify the influence of deterrents or sanctions on negative behavior such as disobedience of or noncompliance with rules and policies ("deviant behavior"). GDT posits that security countermeasures can serve as deterrent mechanisms by increasing perceptions of the certainty, severity and celerity of punishment for non-compliance of security policies, thus improving security of information systems of organizations. Findings in criminology show that perceived certainty, severity and celerity of sanctions are negatively associated with the intention to engage in criminal or socially deviant behaviors (Nagin and Pogarsky 2001). Previous research in IS Security has adopted and extended deterrence theory in different contexts, such as testing for influence on behaviors such as software piracy (Peace et al. 2003), security policy compliance (Bulgurcu et al. 2010; Herath and Rao 2009; Pahnila et al. 2007), IS Security effectiveness (Kankanhalli et al. 2003), and IS Misuse intention (D'Arcy et al. 2009).

Perceived certainty of detection and perceived severity of sanctions were both found to have a significant negative impact on behavioral intention to behave in noncompliant behavior while some studies found only one of those variables significant. Although previous IS Security research seems to have moderately consistent findings on perceived certainty of detection and perceived severity of sanctions, extant studies have largely ignored the perceived celerity of sanctions. Perceived celerity is defined as the swiftness with which sanctions are applied after the detection of non-compliance or maladaptive behavior. Research indicates that some individuals (in some cultures) have a shorter term perspective and others are oriented toward longer-term processes and outcomes, which may lead to differences in the influence of sanction celerity.

Our study seeks to find if differences exist in attitudes of individuals in different cultures towards security policy compliance and if the perceptions of certainty, vulnerability and celerity of formal and informal, positive and negative sanctions influence behavioral intention to comply with security policies differently among individuals of different cultures.

CONCEPTUAL MODEL AND HYPOTHESIS DEVELOPMENT

The present study proposes and tests a theoretical model, shown in Figure 1, assuming that the behavioral intention of individuals to comply with organizational security policies are strongly influenced by formal sanctions, informal sanctions and security policy attitude, where the security policy attitude is influenced by the threat appraisal and coping appraisal of PMT.

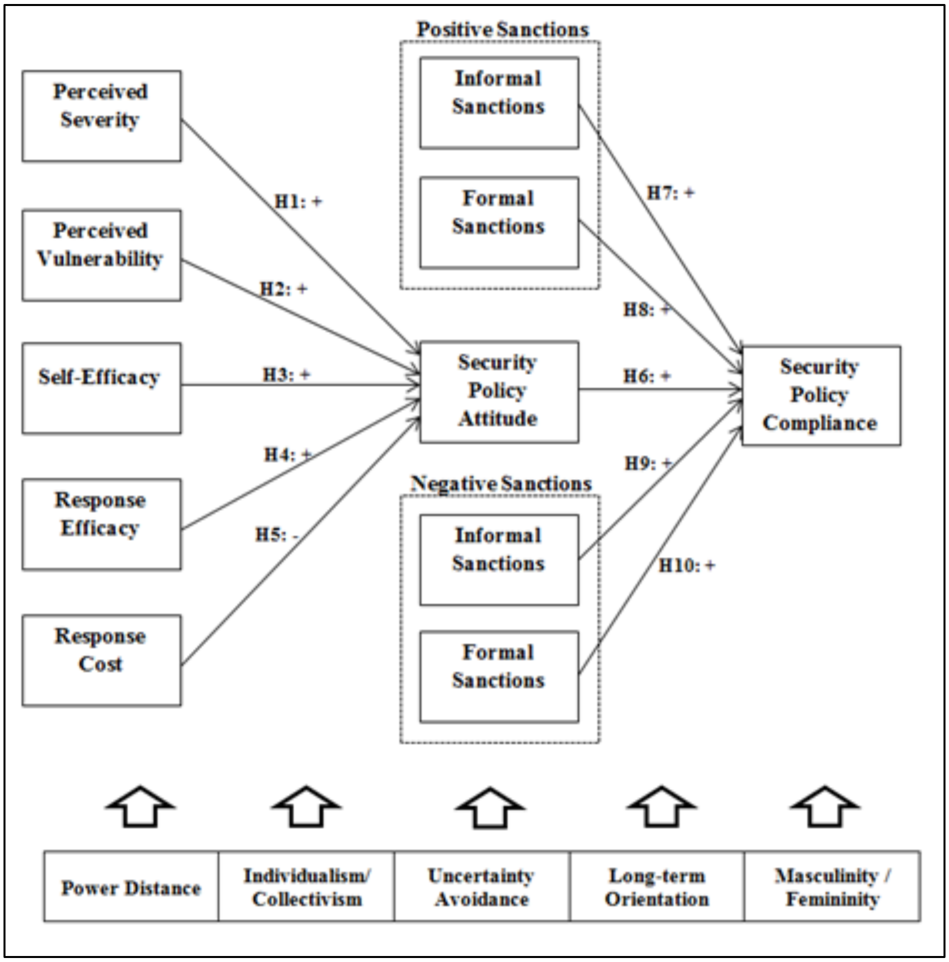


Figure 1. Theoretical Model

According to the TPB and TRA, attitude influences behavioral intention. Previous IS research models utilizing TRA and TPB has found this relationship to be significant (Karahanna et al. 1999). IS security research models that hypothesized employee's attitude towards behavioral intention to comply with security policies have yielded mixed results. For example, whereas Bulgurcu et al. (2010) supported a significant relationship, Herath and Rao (2009) found the relationship insignificant. In different cultures where attitudes are shaped through their national culture, we expect the attitudes to have different influence levels, including those found in the six countries we will study.

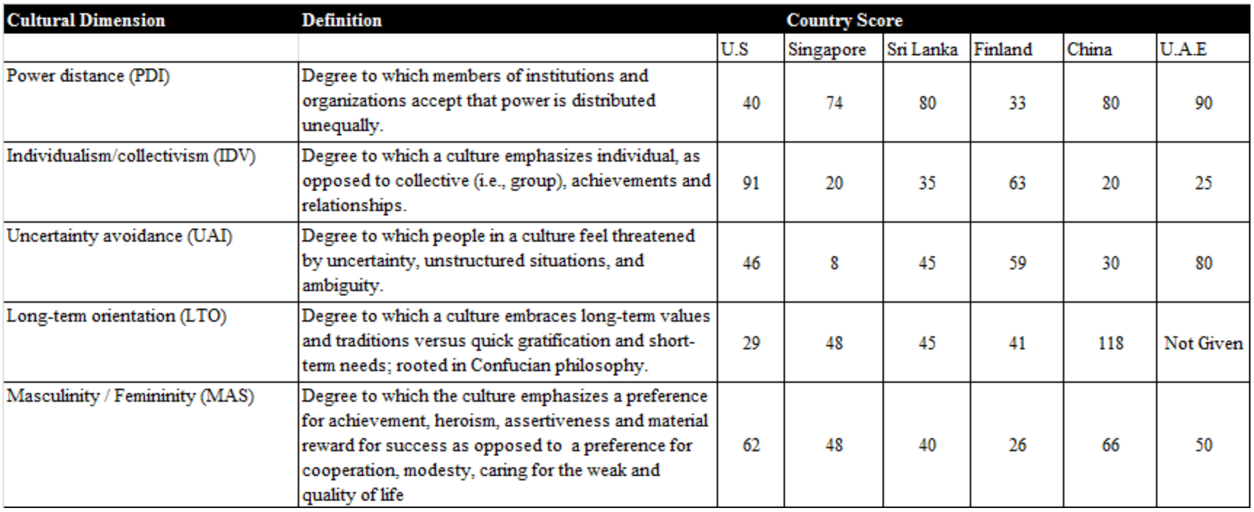
We hypothesize the threat appraisal variables (perceived severity, perceived vulnerability) and the coping appraisal variables (self-efficacy and response efficacy) to have a positive influence on attitudes towards security policies whereas the coping appraisal variable response cost to have a negative influence on security policy attitudes. The security policy attitudes in turn will positively affect employee security policy compliance. The informal positive, informal negative, formal positive and formal negative sanctions will also have a positive influence on security policy compliance. Furthermore, we hypothesize the perceived severity, certainty and celerity of formal and informal negative and positive sanctions will have a positive influence on security policy compliance.

RESEARCH METHOD

In testing our model, an instrument containing a scenario followed by a set of questions will be administered to the selected set of respondents from each of the six countries described below. The questions will measure all the Protection Motivation variables (perceived severity, perceived venerability, self-efficacy, response efficacy, response cost), perceived severity, perceived certainty and perceived celerity of positive and negative informal and formal sanctions, security policy attitude and the behavioral intention to comply with security policies. Our sample will consist of employees from a diverse set of organizations within the selected countries. Furthermore, the instrument will capture Hofstead's five cultural dimensions as explained in Table 2.

For the proposed study, we will evaluate employees in Singapore, Sri Lanka, U.A.E, Finland, and the U.S. These countries were selected for several reasons. First, these countries have significantly different scores on Hofstede's cultural dimensions as shown on Table 2, which suggests individuals within these countries may exhibit different intentions and behaviors, based on differences in espoused cultural values. Though Singapore, U.A.E, and Sri Lanka are all Asian cultures, they have significant differences on several dimensions and are significantly different from U.S. in all dimensions. Second, the U.S. (Leidner and Kayworth 2006) and Singapore (Teo et al. 2008; Yang 2005) have been studied in prior cross-cultural studies in prior IS research and Singaporean culture is similar to the culture of South Korea, which is a country frequently used in cross cultural studies. Third, Finland, as a European country, represents another unique perspective in terms of cultural differences. Finally, one or more authors of this study has visited, lived in, and experienced the cultures of each of the six countries which enables us to effectively develop the hypotheses and interpret the results utilizing the in-depth understanding of each of these cultures. We focused our comparison of the six countries on all of Hofstede's cultural dimensions. Even though (Hovav and D'Arcy 2011) believe that Hofstede's masculinity/femininity dimension is not deemed closely related to the IS security domain, we believe in certain Asian cultures it may have a prominent influence in an organizational environment.

Table 2: Hofstede's cultural dimensions



Cultural Dimension	Definition	Country Score					
		U.S	Singapore	Sri Lanka	Finland	China	U.A.E
Power distance (PDI)	Degree to which members of institutions and organizations accept that power is distributed unequally.	40	74	80	33	80	90
Individualism/collectivism (IDV)	Degree to which a culture emphasizes individual, as opposed to collective (i.e., group), achievements and relationships.	91	20	35	63	20	25
Uncertainty avoidance (UAI)	Degree to which people in a culture feel threatened by uncertainty, unstructured situations, and ambiguity.	46	8	45	59	30	80
Long-term orientation (LTO)	Degree to which a culture embraces long-term values and traditions versus quick gratification and short-term needs; rooted in Confucian philosophy.	29	48	45	41	118	Not Given
Masculinity / Femininity (MAS)	Degree to which the culture emphasizes a preference for achievement, heroism, assertiveness and material reward for success as opposed to a preference for cooperation, modesty, caring for the weak and quality of life	62	48	40	26	66	50

CONTRIBUTION

If the proposed hypotheses are supported, the findings of our study will have contributions in terms of IS security research and practice by examining whether deterrence theory and protection motivation theory influences individuals' policy compliance differently when it comes to diverse cultures. In terms of research contributions, our study would be the first to combine Protection Motivation Theory along with Deterrence Theory in a cross cultural context. The findings will also be helpful in organizational decision making process when dealing with creation of organizational policies. Some of the US-based organizations have branches located in several countries of the world. Having a 'one policy fits all' approach may not necessarily be successful to these companies, as employees in different cultures are likely to perceive threats and sanctions differently. The findings will assist these organizations to gain an in-depth understanding of how these different cultures perceive the threat and coping appraisal variables and how they perceive the positive and negative informal and formal sanctions. With that understanding, these organizations can customize their security policies at different locations across different countries, to cater the cultural aspects of the organization and their employees.

REFERENCES

Ajzen, I. 1991. "Theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Ajzen, I., and Fishbein, M. 1980. "Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control," *Journal of Experimental Social Psychology* (22), pp. 453–474.

Bandura, A., and Adams, N. E. 1977. "Analysis of self-efficacy theory of behavioral change," *Cognitive Therapy and Research* (1), pp. 287–308.

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), pp. 523–548.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

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), pp. 106–125.

Hovav, A., and D'Arcy, J. 2011. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," *Information & Management*Elsevier B.V.

Hovav, A., and D'Arcy, J. 2012. "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Information & Management* (20:1), pp. 79–98.

Im, I., Hong, S., and Kang, M. S. 2011. "An international comparison of technology adoption☆ Testing the UTAUT model," *Information & Management* (48:1), pp. 1–8.

Johnston, A. C., and Warkentin, M. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Quarterly* (34:3), pp. 549–566.

Jong-min, C. 2004. “The consideration of cultural differences in the design of information systems,” *Information &amp; Management* (41:5), pp. 669–684.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., and Wei, K.-K. 2003. “An integrative study of information systems security effectiveness,” *International Journal of Information Management* (23), pp. 139–154.

Karahanna, E., Straub, D. W., and Chervany, N. L. 1999. “Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs.,” *MIS Quarterly* (23:2), pp. 183–213.

LaRose, R., Rifon, N. J., and Enbody, R. 2008. “Promoting Personal Responsibility for Internet Safety,” *Communications of the ACM* (51:3), pp. 71–76.

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.

Leidner, D. E., and Kayworth, T. 2006. “REVIEW: A REVIEW OF CULTURE IN INFORMATION SYSTEMS RESEARCH: TOWARD A THEORY OF INFORMATION TECHNOLOGY CULTURE CONFLICT,” *MIS Quarterly* (30:2), pp. 357–399.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. “Threats to Information Systems: Today’s Reality, Yesterday's Understanding,” *MIS Quarterly* (16:2), pp. 173–186.

Long, G. P. 2004. “Security Policies in a Global Organization,” *SANS Institute InfoSec Reading Room*.

Nagin, D. S., and Pogarsky, G. 2001. “Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence,” *Criminology* (39:4), pp. 865–891.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. “Employees’ behavior towards IS security policy compliance,” In *40th Hawaii International Conference on System Sciences*Hawaii, USA.

Peace, A. G., Galletta, D., and Thong, J. 2003. “Software piracy in the workplace: a model and empirical test,” *Journal of Management Information Systems* (20:1), pp. 153–177.

Puhakainen, P., and Siponen, M. 2010. “Improving Employee’s Compliance Through Information Systems Security Training: An Action Research Study,” *MIS Quarterly* (34:4), pp. 757–778.

Rogers, R. W. 1975. “A protection motivation theory of fear appeals and attitude change,” *The Journal of Psychology* (91), pp. 93–114.

Siponen, M., and Vance, A. 2010. “Neutralization : New Insights Into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly* (34:3), pp. 487–502.

Straub, D. W. 1990. “Effective is security: an empirical study.,” *Information Systems Research* (1:3), pp. 255–276.

Straub, D. W., and Nance, W. D. 1990. “Discovering and disciplining computer abuse in organization,” *MIS Quarterly* (14:1), pp. 45–60.

Teo, T., Luan, W. S., and Sing, C. C. 2008. “A cross-cultural examination of the intention to use technology between Singaporean and Malaysian pre-service teachers: an application of the Technology Acceptance Model (TAM),” *Educational Technology & Society* (11:4), pp. 265–280.

Whitman, M. E. 2003. “Enemy At The Gate: Threats to Information Security,” *Communications Of The ACM* (46:8), pp. 91–95.

Willison, R., and Warkentin, M. 2013. “Beyond Deterrence: An Expanded View Of Employee Computer Abuse,” *MIS Quarterly* (37:1).

Witte, K. 1992. “Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model,” *Communication Monographs* (59), pp. 329–349.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. “Predicting Risk Behaviors: Development and Validation f a Diagnostic Scale,” *Journal of Health Communication* (1), pp. 317–341.

Woon, I. M. Y., Tan, G. W., and Low, R. T. 2005. “A Protection Motivation Theory Approach to Home Wireless Security,” In *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, pp. 367–380.

Workman, M., Bommer, W., and Straub, D. W. 2008. “Security Lapses and the Omission of Information Security Measures: An Empirical Test of the Threat Control Model,” *Journal of Computers in Human Behavior* (24:6), pp. 2799–2816.

Yang, K. C. C. 2005. “Exploring factors affecting the adoption of mobile commerce in Singapore,” *Telematics and Informatics* (22), pp. 257–277.