DECISION SCIENCES INSTITUTE

Factors that influence employees' security policy compliance behavior: an Awareness-Motivation-Capability (AMC) perspective

Xiaofeng Chen
Western Washington University
Email: chenx@wwu.edu

Liqiang Chen
University of Wisconsin-Eau Claire
Email: chenliqi@uwec.edu

ABSTRACT

Information Security Policy (ISP) plays an important role in information security management. Past research investigated various factors from General Deterrence Theory (GDT), Protection and Motivation Theory (PMT), and Rational Choice Theory (RCT). However there is no unifying foundation/framework that can examines all of those factors in a harmonic way so that the research findings can guide the information security practice and research in the employees' ISP compliance management. This study proposes a research model based on the Awareness-Motivation-Capability (AMC) framework to unify the factors to predict employees' ISP compliance intention. We believe that a harmonic approach in managing employees' ISP compliance can create optimal outcomes.

KEYWORDS: Information Security Policy, AMC, Compliance

INTRODUCTION

High profiles of data breach in 2013 and 2014 highlighted the urgency for better data protection in industry. It happened to Home Depot, Target, Citi Bank, JPMorgan, and some other large multi-million dollar companies in the United States in just last several years. It costs $148 million alone for Target to clean up the mess caused by the data breach (Abrams 2014). This estimate may be very conservative since other estimation indicates the cost may top $300 million if all costs are included. The data breach happened at Target in 2013 ushered in a new era of data security. The data breach happened at Target is not because Target didn't have software and hardware measures in place to defend its data. It is because the network credentials was stolen from a third party partner through a malware email attack. It shows again that the weakest link in a security system lies in the human component of the security system (Gonzalez and Sawicka 2002; Misha and Dhillon 2006).

It is a common belief that a security policy is essential to increase the information security level of an organization (Sommestad et al. 2014). Prior research used various theories to study the factors that affect the behaviors of employees' security policy compliance, which include the theory of reasoned action (Bulgurcu et al. 2010), the theory of planned behavior (TPB) (Bulgurcu et al. 2010), protection and motivation theory (PMT) (Herath and Rao 2009; Johnston and Warkentin 2010; Lee et al. 2004; Vance et al. 2012), general deterrence theory (GDT) (D'arcy et al. 2009; Lee et al. 2004; Straub & Nance 1990; Straub & Welke 1998). One aspect that lacks in prior studies is the importance of user awareness of security policy. There is a limited effort in investigating the effect of user

awareness of security policy on security compliance. We use the awareness-motivation-capability (AMC) model as the base to build an integrated security compliance model that incorporates constructs from PMT, TPB, and GDT to understand employees' security policy compliance behavior. This framework has implications for both academia and practice. For practitioners, it shows that a systematic approach is needed to make security policy more effective, which includes arousing employee awareness of security policies through management support and building a culture of treating security as critical business practice, motivating employees to comply with the policies through awards and penalties, and increasing employees' capability to comply with the policies by providing necessary education and training. It provides a comprehensive understanding on how security policies should be implemented in organizations. For academia, this study approaches security policy compliance from a new perspective. AMC framework has been used to understand the competitive actions of organizations in strategic research (Chen 1996; Smith et al. 2001). It has yet to be used for interpreting personal actions in MIS research. We believe that the three components that influence an organization's decision to act will also influence a person's decision to act. Those three components can be manifested in a range of variables that are important in interpreting employees' behaviors towards complying with their organization's security policies. It is a systematic attempt to integrate various theories to form a broad view of employees' security policy compliance behavior.

THEORETICAL FOUNDATION AND RESEARCH MDOEL

Awareness-Motivation-Capability framework (AMC)

The organizational literature has identified three drivers that underlie organizational competitive actions: awareness of market conditions, motivation to act, and capability to take action (Chen 1996; Dutton and Jackson 1987; Kiesler and Sproull 1982; Lant et al. 1992). Chen (1996) summarized that awareness is considered a prerequisite for any action or move; with the awareness, an organization will be motivated to act or counter act; and their action will be limited by their capability. In the competitive dynamics research, Chen et al. (2007) suggested that the individual components of the AMC framework are manifested in a range of variables, including action visibility and firm size for awareness, territorial interests in different markets (Gimeno 1999) for motivation, and execution difficulty and information processing (Smith et al. 1991) for capability.

Although AMC has been used to understand competitive actions of organizations, we believe that it is also a good framework for personal actions. Specifically we use this framework to understand employees' action or their intention toward their organization's security policy: comply or not comply. The behavior drivers of AMC framework: awareness, motivation, and capability outlined in the AMC framework will serve as the second-order constructs in this study. We use the three constructs as dimensions to group the other factors that have been studied in prior information security studies. These other factors from various theories are the first-order constructs in this study. We examine the impact of the three behavioral drivers as well as the other factors on employees' intention to comply with their organizations' ISP. This study will build a harmonic model that unifies factors that may have impact on employees' intention to comply with their organizations' ISP. This model provides sound theoretical guidelines for employee ISP compliance programs. Our research model is pictured in Figure 1. In the next section we discuss our research model and hypotheses development.

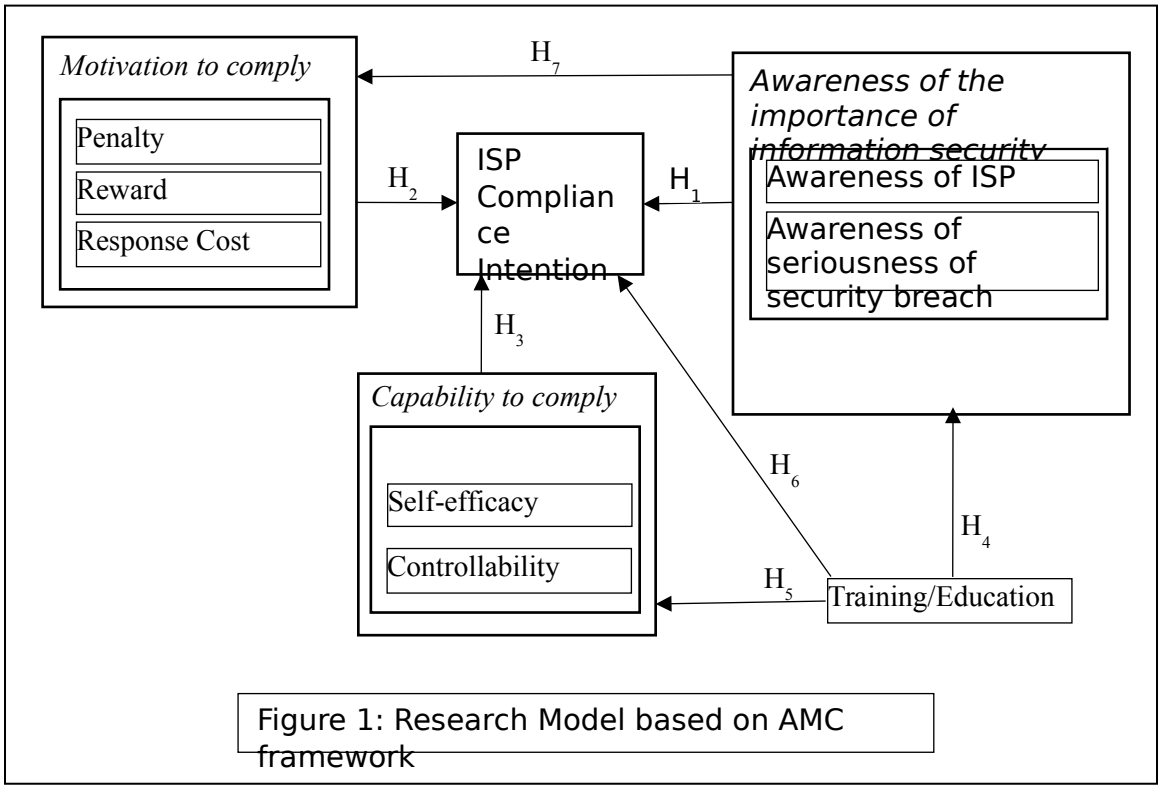

Figure 1: Research Model based on AMC framework

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Information security has drawn attentions in academia and practice alike due to potential huge economic consequences for organizations. The insiders, referred to the employees in the business context, are recognized as the key component of information security management (Bulgurcu et al. 2010; Hinde 2003; Misha and Dhillon 2006; Theoharidou et al. 2005). The recent trade reports and academic research verify and support the argument. Therefore, human behavior perspective of information security is an important area of information security research and has drawn a great attention from academic researchers. Human behavior in information security management is influenced by information security policy (ISP). ISPs are created in organizations to provide employees with guidelines regarding how to ensure information security when they use information systems to do their work (Whitman et al. 2001; Bulgurcu et al. 2010). We adopt Bulgurcu et al. (2010)'s ISP definition in this study, stating ISP is "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations." (Bulgurcu et al. 2010, p. 526). This definition is consistent with many other ISP definitions used in prior research (e.g., D'Arch et al. 2009; Herath and Rao 2009).

One of the research streams in MIS draw on criminological and health belief theories, such as The Theory of Planned Behavior (TPB), Protection Motivation Theory (PMT), Deterrence Theory (DT), and Rational Choice Theory (RCT), to study insiders' compliance behavior toward organizational information security policy (ISP). Factors from different theories were studied separately in some studies or altogether in others without an underline foundation to unify the factors. In this study, we use the AMC framework (Chen et al. 1996) as the unifying foundation to investigate the effect of different factors that underline the

behavior drivers and the effect of the behavior drivers on the employees' behavior of security policy compliance.

Effect of awareness on ISP compliance intention

Awareness factor gained a relatively low attention from information security researchers. Bulgurcu et al. (2010) examined the effect of information security awareness (ISA) on employees' attitude toward intention to comply with ISP. Bulgurcu et al. (2010)'s ISA consists of ISP awareness and general information security awareness (GISA). ISP awareness is defined as "an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements" and GISA is defined as "an employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (Bulgurcu et al. 2010, p. 532). Siponen and Pahnila (2010) indirectly investigated the awareness of ISP on employees' compliance with ISP via its impact of security visibility. They found that visibly promoting security is an important factor that influences employees' intention to comply with ISP. D'Arcy et al. (2009)'s study found that there is a direct impact of user awareness of security countermeasures on information systems misuse. Lee et al. (2004) conducted an interesting research whose finding are against the belief that information security policy is a key component of information security management. They found that information security policy does not have significant impact on preventing computer abuse, but security awareness does. We argue that the reason for these findings may lie in the employees' awareness of information security policy is low. We tested this assumption in our research. Past studies show the importance of ISP awareness factor. But the construct was not formally theorized in the studies on why it is an important factor for ISP compliance. We argue that according to AMC, awareness factor is an essential component for information security management. Awareness of the importance of an organization's ISP plays an important role in employees' behavior toward ISP compliance. This is one of the theoretical contributions of this study to our knowledge of information security management.

Based on the AMC framework and extant literature, we propose our first set of hypotheses:

H_1: Awareness of the importance of information security has a positive impact on employees' intention to comply with their organization's ISP.

H_{1a}: ISP awareness will positively affect employees' intention to comply with their organization's ISP.

H_{1b}: Awareness of the seriousness of security threats will positively affect employees' intention to comply with their organization's ISP.

Effect of motivation on ISP compliance intention

TPB is a base theory for many ISP compliance or non-compliance studies (e.g., Bulgurcu et al. 2010; D'Arcy et al. 2009; Herath and Rao 2009; Lee et al. 2004; Vance et al. 2012). The theory suggests that attitude, social norms, and behavior controls affect people's intention to perform the actual compliance behavior. Theories based on TPB, such as DT, PMT, and RCT, are used to investigate the antecedents and the antecedents' antecedents (two levels) to employees' attitude and intention to comply or not comply with their organization's ISP.

Although DT as a perspective has been applied to information security research, there is no general formalized definition of the theory (Williams and Hawkins 1986). The theory was

applied to the research on the assumption that "individuals are deterred from committing criminal acts only if they perceive legal sanctions as certain, swift, and/or severe" (Williams and Hawkins 1986, p. 545). DT was applied to studies to evaluate penalty factors, such as penalty severity and certainty that may be effective to prevent certain actions from happening, such as non-adherence to security policy (Cheng et al. 2013; D'Arcy et al. 2009; Herath and Rao 2009). The results are inconsistent. Perceived severity of sanctions has been found having direct negative impact on IS misuse intention (D'Arcy et al. 2009; Skinner and Fream 1997; Cheng el al. 2013; Vance et al. 2012); whereas perceived certainty of sanctions has no direct impact on IS misuse (negative measure) intention (Cheng et al. 2013; D'Arch et al. 2009; Hu et al. 2011). In other studies perceived certainty of sanctions has been found having direct impact on ISP compliance (positive measure) (Herath and Rao 2009; Li et al. 2010), but perceived severity of sanction having no (Li et al. 2010). We found that direct impact of perceived severity was mostly found in non-compliance studies, such as misuse or violation (D'Arcy et al. 2009; Skinner and Fream 1997; Cheng el al. 2013); whereas direct impact of perceived certainty was found in compliance studies (Herath and Rao 2009; Li et al. 2010). There is no plausible explanation about the inconsistent results. D'Arcy and Herath (2011) conducted a thorough review and analysis of deterrence theory in the IS security literature. They theorized that the inconsistent results of the effect of DT factors on security behavior may be due to the contingency variables that are not controlled in the studies. These contingency variables may have a moderating effect on the DT variables-to-behavior relationship. The identified two groups of key contingency variables: individual factors and contextual factors. The formal includes self-control, computer self-efficacy, and moral beliefs; the latter includes virtual status and employee position (D'Arcy and Herath 2011). We argue that contingency variables may not only have a moderating effect on the DT variables-to-behavior relationship but also be 'noises' for the relationship. Together all these variables may explain the variances of employees' ISP compliance behavior.

According to PMT (Rogers 1975), people intend to cope with a threat based on the results of two appraisals: threat appraisal and coping appraisal. The motivation to protect themselves from the threat depends on severity of the thread; probability of the occurrence of the threat; the efficacy of the recommended preventive behavior; and sell-efficacy (Rogers 1975; Rogers 1983; Herath and Rao 2009). Motivation can be divided into intrinsic and extrinsic motivation. From the AMC perspective, we believe that the last two factors from PMT are capability factors, not the motivation factors.

RCT argues that an individual's action is determined by balancing the costs and benefits of his options (Bulgurcu et al. 2010). People balance the overall assessment of costs and benefits associated with the outcomes of their actions to determine which actions to take (Paternoster and Pogarsky 2009). We argue that the assessments of costs and benefits can serve as motivations to take actions. Costs can be viewed as motivations to not take actions and benefits can be viewed as motivations to take actions.

We propose that the variables from DT, PMT, and RCT can be grouped into the motivation dimension of the AMC framework. Those variables can be generally placed in the extrinsic motivation category since they are "perceived to be instrumental in achieving valued outcomes that are distinct from the activity itself" (Davis et al. 2992). Extending the application of the AMC framework at the organizational level to the individual level, we theorize that the motivation dimension of the AMC framework determines if a person will take an action or not. After an individual is aware of a potential action, they need to be

motivated to take the action. The motivation to take an action can be influenced in the ISP compliance context from three categories of extrinsic factors: rewards, penalty, and cost. The intrinsic factors, which may include enjoyment for an action, may not be in play in this specific context. Both PMT and DT indicate that penalty can deter violations; therefore penalty can be considered as people's motivation to not commit violations outlined in their organization's ISP. Cost may have the same effect as penalty on ISP compliance. Numerous studies have shown that rewards can control behavior (Deci et al. 1999). Accordingly, our second set of hypotheses regarding employees' intention to comply with their organizations' ISP are:

H_2: Motivation has positive impact on employees' intention to comply with their organization's ISP.

H_{2a}: Penalty severity has inversed effect on employees' intention to comply with their organization's ISP.

H_{2b}: Reward has positive effect on employees' intention to comply with their organization's ISP.

H_{2c}: Cost to comply with ISP has negative effect on employees' intention to comply with their organization's ISP

Effect of capability on ISP compliance intention

According to the AMC framework, motivation is not enough for an individual to take an action. The individual has to have the capability to perform certain tasks for the action is actually carried out. In the context of ISP compliance, an employee has to have the capability to follow the policies and perform the tasks. The capability for performing the tasks is influenced by employees' ability to work with computer systems in general and security management (e.g., following the security policy, being about to use various security software) in specific. Several factors outlined in the security research using DT, PMT, and RCT can be placed in this dimension. These factors include self-efficacy with computer systems and employees' perception of controllability over compliance. The self-efficacy is well defined in the security research using PMT (e.g., Herath and Rao 2009). Controllability over compliance measures the employees' perception of support from management over compliance (Dinev and Hu 2007). Our next set of hypotheses are:

H_3: Capability has positive impact on employees' intention to comply with their organization's ISP.

H_{3a}: Self-efficacy with computer systems has positive effect on employees' intention to comply with their organization's ISP.

H_{3b}: Perception of controllability over compliance has positive effect on employees' intention to comply with their organization's ISP.

Security training and education has been found playing important role in security management (e.g., Furnell et al. 2002; Hentea 2005; D'Arcy et al. 2009; Bulgurcu et al. 2010). From the AMC perspective, security training and education can have impact on the awareness and capability dimensions as well as on ISP compliance intention itself. We propose:

H_4: Security training and education program has positive impact on employees' awareness of the importance of information security.

H_5: Security training and education program has positive impact on employees' capability to comply with their organizations' ISP.

H_6: Security training and education program has positive impact on employees' intention to comply with their organizations' ISP.

Effect of awareness of importance of information security on motivation to comply with ISP

The AMC framework proposes the three drivers for actions. However, it does not outline the relationships among the three drivers. There is a lack of empirical studies on the relationships among the three drivers. We argue that to be motivated to take an action, an individual needs to know what the action is concerned about, why it is important to take the action, and what are expected from them. Therefore, the awareness driver of AMC framework should have direct influence on the motivation driver of an action. As a result, we propose in the ISP compliance context:

H_7: Awareness of important of information security has positive impact on employees' motivation to comply with their organizations' ISP.

RESEARCH METHOD

There are two approaches in the research of employee security compliance. One approach is using scenarios to provide a specific security issue (Johnston and Warkentin 2010; Vance et al. 2012) followed by survey to collect information about what factors may affect the behavior of employees' security (compliance) behavior. The other approach is using survey to collect information regarding factors that may influence employees' compliance intention on a generic ISP that is defined as "a statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations." (Bulgurcu et al. 2010, p. 526). The latter is a main approach in the literature of investigating ISP compliance behavior (e.g., D'Arcy et al. 2009; Herath and Rao 2009). We choose to use the second approach in this study. We attempt to examine employees' intention to comply with ISP as defined in a general statement.

There are two techniques to assess a regression structural model: one is the covariance-based SEM as represented by LISREL and the other is component-based (or variance-based) as represented by Partial Least Square (PLS) modeling (Henseler et al. 2009). We will use PLS modeling in this study to investigate the relationships among the factors. PLS requires smaller sample size than covariance-based SEM techniques. In this study there are three second-order constructs, 10 first-order constructs, and over 35 indicators in total. The sample size may needs to be over 700 if we use covariance-based SEM, such as LISREL. Also LISREL may not be able handle the model with this complexity (Chin et al. 2003).

SUMMARY

In this study, we use the AMC framework to build an integrated model that investigates the factors that may influence employees' intention to comply with their organizations' ISP. Past research identified many factors that may affect employees' intention in several different models that do not have a unifying foundation, thus the research findings lack consistency. Also without a unifying foundation, different factors explain employees' compliance behavior from different perspectives. As a result, there is no theoretical consensus about how to implement employee ISP compliance programs and accordingly there is no consistent guidelines for practitioners to follow. By applying the AMC framework

in the ISP compliance research, we propose that many factors that may influence employees' compliance with ISP can be grouped into three categories of behavior drivers: awareness, motivation, and capability. The implications of this study are in two folds. In academia, this study for the first time investigates employees' compliance with ISP using the AMC framework. We built a model that uses the three behavior drivers outlined in the AMC framework as the unifying foundation. This unifying foundation re-posits the factors from different theories in the past information security research to understand what affect employees' compliance with their organizations' ISP. This model presents a new perspective in studying employees' ISP compliance. In practice, this study can provide guidelines for managers to design their information security management programs. Managers need to be aware that employees' compliance with their organizations' ISP is critical to secure their organizational information systems and usages. Employees' awareness of the importance of information security and ISP may play an important role in information security management. Other than promoting the importance of information security and ISP by creating awareness programs, managers need to pay attention to help employees to develop capability to comply with their ISPs. Security education and training can help build employees' capability to comply with their organizations' ISP and in turn improve the actual compliance practice. Managing employees' compliance with ISP in information security management is a harmonic process. It cannot be achieved through just one dimension.

Reference:

Abrams, R. "Target puts data breach costs at $148 million, and forecasts profit drop," *New York Times*, extracted at http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0

Bulgurcu, B., Cavusoglu, H, and Benbasat, I "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS Quarterly 34(3), 2010, pp. 523-548.

Chaudhuri, S. "Cost of replacing credit cards after Target breach estimated at $200 million," Wall Street Journal, http://www.wsj.com/articles/SB10001424052702304675504579391080333769014.

Chen, M.J. "Competitor analysis and inter-firm rivalry: towards a theoretical integration," Academy of Management Review, 21, 1996, pp. 100-134.

Chen, M.J., Su, K.H., and Tsai, W.P. "Competitive Tension: The Awareness-Motivation-Capability Perspective," *Academy of Management Journal* (50:1), 2007, pp. 101-118.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. "Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory," Computers & Security, 2013, pp. 1-13.

D'arcy, J., Hovav, A., and Galletta, D. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," Information Systems Research 20(1), 2009, pp. 79-98.

Deci, E.L., Koestner, R., and Ryan, R.M. "A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation," Psychological Bulletin (125:6), 1999, pp. 627-668.

Dinev, T. and Hu, Q. (2007) "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," Journal of the Association for Information Systems 8(7), Article 23.

Dutton, J.E. and Jackson, S.B. "Categorizing strategic issues: links to organizational action," Academy of Management Review 12, 1987, pp. 76-90.

Gimeno, J. "Reciprocal Threats in Multmarket Rivalry: Staking out 'Spheres of Influence' in the U.S. Airline Industry," *Strategic Management Journal* (20:2), 1999, pp. 101-128.

Herath, T. and Rao, H.R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems 18(2), 2009, pp. 91-109.

Hinde, S. "The law, cybercrime, risk assessment and cyber protection," Computers and Security 22(2), 2003, pp. 90-95.

Hu, Q., Xu, Z. Dinev, T., and Ling, H. "Does deterrence work in reducing information security policy abuse by employees?," Communications of the ACM 54(6), 2011, pp. 54-60.

Johnston, A. and Warkentin, M. "Fear appeals and information security behaviors: an empirical study," MIS Quarterly 34(3), 2010, pp. 549-566.

Kiesler, S. and Sproull, L. "Managerial response to changing environments: perspectives on problem sensing from social cognition," Administrative Science Quarterly 27, 1982, pp.548-570.

Lant, T.K., Milliken, F.J., and Batra, B. "The role of managerial learning and interpretation in strategic persistence and reorientation," Strategic Management Journal 13, 1992, pp. 585-608.

Lee, S.M., Lee, S., and Yoo, S. "An integrative model of computer abuse based on social control and general deterrence theories," Information & Management 41(6), 2004, pp. 707-718.

Misha, S. and Dhillon, G. "Information systems secdurity governance research: a behavioral perspective," 1st Annual Symposium on Information Assurance, 2006.

Paternoster, R. and Pogarsky, G. "Rational choice, agency and thoughtfully reflective decision making: the short and long-term consequences of making good choices," *Journal of Quantitative Criminology* (25:2), 2009, pp. 103-127.

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

Rogers, R.W. "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protected motivation," In Social Psychophysiology: a sourcebook (Cacioppo, J.T. and Petty, R.E., Eds), 1983, pp. 153-176, The Guilford Press, New York.

Siponen, M., Pahnila, S., and Mahmood, M.A. "Compliance with Information Security Policies: An Empirical Investigation", *Computer* 43(2), pp. 64-71, February 2010.

Siponen, M. and Vance, A. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly* 34(3), 2010, p. 487-502.

Smith K. G., Grimm, C. M., Gannon, M. J., Chen, M., Grimm, C. M., Gannon, M. J. "Organizational Information Processing, Competitive Responses, and Performance in the U.S. Domestic Airline Industry," *Academy of Management Journal* (34:1), 1991, pp.60-85.

Smith, K.G., Ferrier, W., and Ndofor, H. "Competitive dynamics research: critique and future directions". In M. Hitt, R. Freeman, & J. Harrison (Eds.). Handbook of Strategic Management, 2001, pp. 315-361. London: Blackwell.

Sommestad, T. Hallberg, J., Lundholm, K., and Bengtsson, J. "Variables influencing information security policy compliance," Information Management & Computer Security 22(1), 2014, pp. 42-75.

Straub, D. and Nance, W.D. "Discovering and disciplining computer abuse in organizations: a field study," MIS Quarterly 14(1), 1990, pp. 45-60.

Straub, D. and Welke, R. "Coping with systems risk: security planning models for management decision making," MIS Quarterly 22(8), 1998, pp. 441-465.

Teodor, S., Hallberg, J., Lundholm, K, and Bengtsson, J. "variables influencing information security policy compliance: a systematic review of quantitative studies," Information Management & Computer Security 22(1), 2014, pp. 42-75.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. "The insider threat to information systems and the effectiveness of ISO 17799," Computers & Security 24(6), 2005, pp. 472-484.

Vance, A., Siponen, M., and Pahnila S. "Motivating IS security compliance: insights from habit and protection motivation theory," Information & Management 49, 2012, pp. 190-198.

Vroom, C. and Von Solms, R. "Towards information security behavioral compliance," Computer Security 23(3), 2004, pp. 191-198.

Whitman, M.E., Townsend, A.M., and Aalberts, R.J. "Information systems security and the need for policy," in *Information Security Management – Global Challenges in the Next Millennium*, G. Dhillon, London: Idea Group, 2001, pp. 9-18.

Williams, K.R. and Hawkins, R. "Perceptual research on general deterrence: a critical review," Law & Society Review 20(4), 1986, pp. 545-572.