Behavioral Approach to Information Security Policy Compliance

Full Paper

Ashraf Mady
University of North Georgia
Ash.Mady@ung.edu

Saurabh Gupta
Kennesaw State University
sgupta7@kennesaw.edu

Abstract

Information security is among the top organizational priorities. Theoretically, the security of information in socio-technical networks is as much of a behavioral issue as it is of a technical issue. Protection motivation theory (PMT), the dominant theory used to investigate end-user security behavior, though has shown conflicting results - primarily due to the lack of contextualizing the theory to information security context from a healthcare context. In addition, extant research provides limited managerial levers to influence such behavior. In this paper, we outline a theoretically grounded conceptual model of the major factors influencing information security policy compliance. The model contextualizes the two independent variables of PMT. Threat appraisal evaluation is viewed as construal evaluation based on construal level theory, while coping appraisal evaluation is viewed as an outcome of training based on social cognitive theory. Overall, the model provides a well-grounded nomological network that aims to explain information systems security compliance behavior better. The paper also outlines key managerial levers that can be used to influence end-user behavior.

Keywords

Information security policy compliance, protection motivation theory, construal level theory, social cognitive theory, user behavior, conceptual model.

Introduction

Information use and security is vital to organizational success and strategic advantage (Doherty et al. 2009). Information security is concerned with protecting information from accidental or malicious incidents such as exposure of confidential information (threat to information privacy) (Arachchilage and Love 2014), deletion of data (threat to information availability) (Safa et al. 2016), and/or data modification (threat to information integrity) (Sen and Borle 2015). Information security breach incidents may have significant consequences such as financial and legal liabilities, loss of reputation, negative economic impact, or employees' demotivation (Bulgurcu et al. 2010). Therefore, information security has become among the top organizational priorities (Anderson et al. 2016). The global spending on security solutions and services was estimated to reach $86 billion in 2016 (Anderson et al. 2016), an 25% increase in budget (Kessel and Allan 2015). However, despite the spending growth and the attention, security breaches continuously increase, costing businesses billions of dollars (Safa et al. 2016).

Majority of the approaches to information security have primarily focused on technical issues to secure information systems (Crossler et al. 2013). Recent information security literature, though, advocates that the security of information is as much of a behavioral issue as it is of a technical issue (Chatterjee et al. 2015; Da Veiga and Martins 2015). The challenge is that organizations continue to underestimate behavioral risks (Anderson et al. 2016; D'Arcy et al. 2014). The key construct focusing on the behavioral component of this approach is user / employee behavior (Da Veiga and Martins 2015).

Employees' behavior will impact organizational information security and can cause serious security incidents because employees are in direct contact with information (Herath and Rao 2009b; Warkentin et al. 2016). Employees are the people who interact directly with the information system and handle the information in their day-to-day activities. One mechanism for directing human behavior within

organizations is the creation and implementation of information security policies (Doherty et al. 2009; Sommestad and Hallberg 2013). However, policy creation may not automatically translate to the desirable behavior (Safa et al. 2016; Sommestad et al. 2015). Organizations find the enforcement of security policies challenging (Chen et al. 2012; Herath and Rao 2009a).

The dominant theory used to investigate behavior in information systems security has been protection motivation theory (PMT) (Boss et al. 2015). However, key gaps exist in the literature drawing on this theory. First, the key independent variables have not shown consistent impacts. Second, PMT does not provide clear managerial levers that can be used to influence compliance. Thus, researchers have called for more theoretical development in this area.

The objective of the paper is to develop a theoretically grounded model addressing the concerns outlined above. The rest of the paper is organized as follows. First, a summary of the literature is presented highlighting the current understanding and gaps in the literature. Next, building on the literature review, the theoretical model with testable propositions is presented. The model clarifies existing constructs as well as adds new constructs. We conclude by highlighting the theoretical and managerial implications.

Literature Review

Protection motivation theory (PMT) argues that behavioral intention to comply is motivated by individuals' assessment of threats based on two cognitive processes, the threat appraisal and coping appraisal (Johnston and Warkentin 2010). In this section, we use PMT to organize existing literature, pointing out some major findings and gaps.

Threat Appraisal

Threat appraisal is the individual's assessment of the probability of exposure or vulnerability, the severity of the threat, and the potential rewards for noncompliance or engaging in maladaptive responses (Boss et al. 2015).

Threat severity is individual's perception regarding the level or the degree of the damaging impact of the threat (Sommestad et al. 2015). In the context of information security policy compliance, it refers to the evaluation of the severity of the damage and the possible negative events resulting from noncompliance with the recommended information security policies (Vance et al. 2012). Threat severity is utilized to enable individuals to understand the threat and its associated unwarranted consequences (Sommestad et al. 2015) because the overall assessment of severity of the threat is conceptualized to exert significant positive influence on an employee's attitude toward compliance (Bulgurcu et al. 2010; Siponen et al. 2014). Extant literature generally shows a positive impact of increased threat severity on compliance intention (Chen et al. 2012; Johnston et al. 2015). However, researchers have also found limited or even negative impact of threat severity on compliance intention. For example, Herath and Rao (2009a)) found that threat severity had a negative effect on compliance intentions. To explain the results, they argued that the excessive use of punishment would create hostile, stressful, and disruptive work environment. Warkentin et al. (2016)) supported the same conclusion stating that the communication of too much fear will generate stress resulting in a behavior oriented toward alleviating the fear rather than dealing with the threat itself. Other researchers addressed the importance of the context of application on perception arguing that the threat severity will have a positive impact on compliance intentions in a personal context (Boss et al. 2015).

Threat vulnerability is the extent of being susceptible to damage caused by information security risks (Anderson et al. 2016; Bulgurcu et al. 2010; Vance et al. 2012). The persuasive communication of vulnerability to the threat is used to deliver fear that will motivate individuals to comply with the recommended protective response (Boss et al. 2015). The existent literature supported the positive impact of threat vulnerability on compliance intentions (Siponen et al. 2014). However, researchers have also provided inconsistent results regarding the impact of threat vulnerability on compliance. Some researchers found threat vulnerability has an insignificant impact on compliance (Herath and Rao 2009b; Posey et al. 2015) because they measured organizational vulnerability to the threat. Vance et al. (2012)) supported the same finding and argued that individuals generally do not believe that their lack of compliance with the information security policy will cause them any personal harm. Johnston et al.

(2015)) reported that when measuring threat vulnerability on organizational information systems, threat vulnerability was not supported as a significant determinant for intentions to comply with information security policies. They asserted that PMT has been improperly applied in the context of information security. Literature explains that in order for threat vulnerability to be able to positively influence compliance behavior, the vulnerability must be on a personal level not toward the organization (Warkentin et al. 2016).

Maladaptive rewards are the benefits gained from committing the violation or indulging in a risky behavior (Posey et al. 2015). Maladaptive rewards present incentives associated with the undesired behavior influencing users to ignore the recommended protective behavior (Boss et al. 2015). Maladaptive rewards exhibit a significant negative relationship with employees' protection motivation (Vance et al. 2012). However, maladaptive rewards received the least empirical attention (Boss et al. 2015). Researchers often exclude maladaptive reward construct from models because of the difficulty of distinguishing maladaptive rewards from the cost of compliance (Sommestad et al. 2015). Bulgurcu et al. (2010) illustrated this approach by associating maladaptive rewards with the cost of compliance to empirically support the significant negative influence of the cost of compliance on employee's attitude toward compliance. Information security literature supports that with the increased maladaptive rewards, employees find it appealing to indulge in risky behavior and ignore protective behavior communicated by information security policy (Boss et al. 2015).

Coping Appraisal

The coping appraisal is the process by which individuals evaluate how effective, manageable and feasible the available risk mitigating response can be (Herath and Rao 2009a; Ifinedo 2012; Sommestad et al. 2015).

Response efficacy is the perception regarding the available mitigating strategies that can successfully diminish the threat (Posey et al. 2015). Information security literature reflects the positive impact of response efficacy on compliance intentions. Recent research efforts continue to confirm the significance positive influence of response efficacy (Johnston et al. 2015; Posey et al. 2015; Siponen et al. 2014). However, researchers argued factors that would impact the significance of response efficacy. Ifinedo (2012)) argued that response efficacy was enabled by employees' relevant knowledge, competence and capability to implement preventative security measures. Warkentin et al. (2016)) recommended that response efficacy is more appealing when relative to personal goals and aligned with abilities with individuals' abilities. Other researchers argued that habits (Siponen and Vance 2010) and complexity of the recommended response (D'Arcy et al. 2014) would diminish the significance of response efficacy. Bulgurcu et al. (2010)) did not even measure response efficacy in their model.

Self-efficacy is the degree to which individuals believe in their own abilities to perform what is required to avert the threat (Bandura 1977). Information security literature supports the significant positive impact of self-efficacy on compliance intentions (Bulgurcu et al. 2010; Ifinedo 2012). Warkentin et al. (2016)) argued that self-efficacy had the strongest positive impact to influence compliance intentions. However, other researchers argued factors that can weaken or even diminish the impact of self-efficacy on compliance. For example, D'Arcy et al. (2014)) argued that the increased complexity of security policy requirement would have a negative impact on self-efficacy. Other researchers could not even validate the impact of self-efficacy on compliance intentions (Posey et al. 2015). On the contrast of prior findings, Chatterjee et al. (2015)) suggested that self-efficacy was negatively associated with ethical use because it enables users to manipulate technology maliciously.

Response cost is mainly the extra time and efforts needed to mitigate the risk (Ifinedo 2012; Sommestad et al. 2015). Literature generally agreed on the significant negative impact of response cost on compliance (Boss et al. 2015; Herath and Rao 2009b). However, researchers argued different factors that will impact the evaluation of response cost. D'Arcy et al. (2014)) confirmed that the increased security demands and complexity would increase the cost of compliance. Other researchers asserted that cost of compliance is calculated as lack of productivity (Bulgurcu et al. 2010; Posey et al. 2015). Literature also supports that not only time and efforts impact cost of compliance, but also the loss of business opportunities will cause response cost to be perceived significantly higher (Posey et al. 2015; Siponen and Iivari 2006). Some researchers recommended the use of organizational rewards to reduce the cost of compliance (Chen et al.

2012). Contrary to the reported negative impact of response cost on compliance, Ifinedo (2012) reported results that did not support the negative impact of response cost.

The analysis of prior research using PMT in information security context has outlined the varied and conflicting results for reasons other than natural variation or measurement error suggesting that the conflicting results were due to the context of application (Sommestad et al. 2015). In an effort to minimize results variations and to increase our knowledge of information security policy compliance drives, some researchers suggested the inclusion of other variables such as certainty of punishment (Chen et al. 2012; Herath and Rao 2009a; Herath and Rao 2009b), attitude toward compliance (Bulgurcu et al. 2010; Ifinedo 2012; Siponen et al. 2014), social influence (Ifinedo 2012; Johnston and Warkentin 2010; Siponen et al. 2014), habit (Vance et al. 2012), or affective commitment (Posey et al. 2015). More work is needed to better understand the role of fear appeals constructs in various information security contexts (Boss et al. 2015; Crossler et al. 2013). Researchers called for future research to address the inconsistent findings regarding the impact of each of PMT constructs in the context of information security (Warkentin et al. 2016). Therefore, the literature review presents a need for a theoretically driven extension of PMT that addresses the issue of context better.

Theoretical Development and Propositions

The initial development and use of PMT was in healthcare (Rogers 1975). However, the direct application of PMT in information Systems context has shown inconsistent results leading some researchers to argue better contextualization of the theory (Johnston et al. 2015).

The theoretical model argued in this paper and presented in Figure 1, attempts to remove the above-mentioned misspecifications by focusing on contextualizing the two key independent variables of PMT: Threat appraisal and Coping appraisal. The model reconceptualizes threat appraisal by focusing on the context of the threat as it relates to the user. The model argues that it is important to view the threat appraisal evaluation by an individual in terms of the psychological distance from the threat. Coping appraisal, on the other hand, is conceptualized as an outcome of training. Each of these is discussed next in more detail.

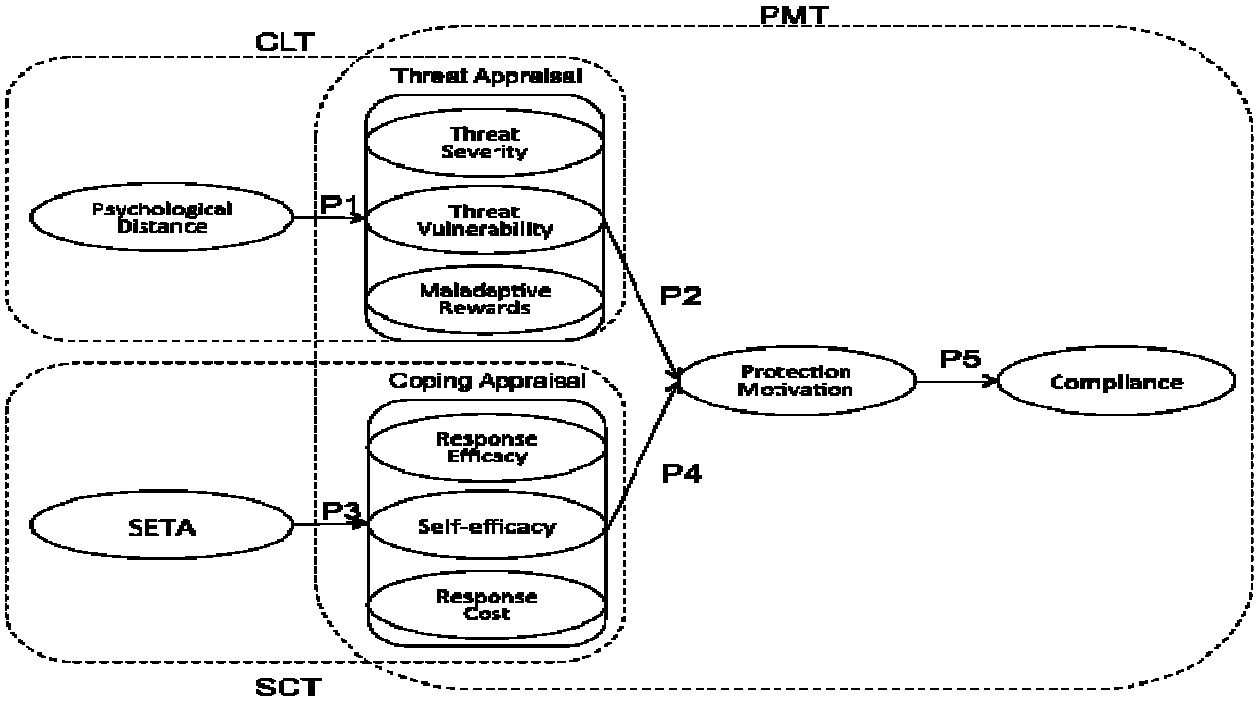

Figure 1. Conceptual Model Diagram

Psychological distance and Threat Appraisal Construal

Psychological distance is egocentric. Its reference point is the self in the here and now, and the different ways in which an object might be removed from that point constitute different distance (Trope and Liberman 2010). The different levels of construal impact individual's comprehension and thus mentally traverse psychological distances (Trope and Liberman 2003). The construal-level theory (CLT) explains the impact of psychological distance on the individual's perception and the associated behavior regarding any particular event (Trope and Liberman 2003). The theory argues that the closer the psychological distance between individuals and an event, the more concrete the event will be perceived, while as the psychological distance increases, the more abstract the event will become (Krishna 2012; Trope et al. 2007). The psychological distance will determine whether the core essential characteristics of the event will be used or just the peripheral characteristics to create people's perception and mental representation of an event (Liberman and Trope 1998). CLT also posits that the dimensions of the psychological distance relative to an event are temporal (will happen immediately or in the future), spatial (happening here or somewhere else), hypothetical (probability of occurrence), or social (will affect me or other people) (Trope et al. 2007). Therefore, according to CLT, an event will be at a greater psychological distance when it is farther into the future, occurs in remote locations, less likely to occur, or affect other people (Liberman et al. 2007).

Literature confirmed that information security threat to the organization does not create a personal fear experience consistent with contemporary PMT fear appeal applications (Warkentin et al. 2016). Threat appraisal is weakened in the absence of personal relevance (Crossler et al. 2013). Including the psychological dimensions is critical to explain threat appraisal. CLT proposes that low psychological distance will lead to low level of construal regarding events creating more concrete perception (Ho et al. 2015; Köhler et al. 2011).

Low psychological distance will influence people to perceive themselves to be closely associated with the event (Liberman et al. 2007; Trope and Liberman 2010). Low psychological distance will improve threat assessment (Tam et al. 2010) because events will be perceived concrete and in details (Krishna 2012). The use of psychological distance will provide egocentric reference or personal relevance (Trope and Liberman 2010). Personal relevance will positively influence threat appraisal (Johnston et al. 2015). Also concrete details about the threat will influence individuals to take immediate action (Tam et al. 2010). Concrete and detailed perception of a threat will increase threat appraisal.

On the contrast, high psychological distance will influence individuals to believe that events may not happen and if they take place, events will be somewhere impacting others (Trope et al. 2007). Lack of strong association to the threat will weaken threat appraisal (Crossler et al. 2013). Individuals are less likely to take security precaution when the psychological distance to the threat is high because people believe they are invulnerable to that threat (Workman et al. 2008). Abstract perception of the threat will omit details reducing the threat appraisal. Therefore, we suggest the following proposition:

Proposition P1: *Individuals with closer psychological distance to the threat are more likely to have a more concrete threat appraisal construal.*

Threat appraisal is the personal assessment of the damaging impact of the threat compared with the potential noncompliance benefits or maladaptive rewards (Boss et al. 2015; Herath and Rao 2009a; Ifinedo 2012; Posey et al. 2015). The perception of threat severity at a personal level enables individuals to understand the threat and its associated unwarranted consequences (Sommestad et al. 2015). Threat appraisal will shape employees' attitude towards compliance (Herath and Rao 2009b; Warkentin et al. 2016). Individuals are more likely to follow protective behavior when their perception of the threat's damaging impact is high (Workman et al. 2008). When organizational information policy reflects the severity of the threat and emphasizes employees' degree of vulnerability to the risk while minimizing the maladaptive rewards, the policy will establish the needed threat appraisal (Chatterjee et al. 2015; Sommestad et al. 2015).

The conceptualization of threat appraisal will exert significant positive influence on an employee's attitude toward compliance (Bulgurcu et al. 2010; Siponen et al. 2014). The perception of the severity of the damage and the possible negative events resulting from noncompliance with the recommended secure behavior will create the desired level of threat appraisal that will influence compliance (Vance et al. 2012).

Information security literature supports that severity of the threat and its harmful impact significantly affect employees' concerns regarding security breaches and will have a positive effect on attitude towards information security policy compliance (Chen et al. 2012; Herath and Rao 2009b).

On the contrast, the absence of vulnerability and severity perceptions to the threat and the increased maladaptive rewards gained from noncompliance will have a negative impact on compliance intentions (Bulgurcu et al. 2010; Siponen et al. 2014). Information security policies must communicate a severe threat on a personal level to motivate protective behavior. Therefore, we suggest the following proposition:

Proposition P2: *Individuals with strong threat appraisal are more likely to have higher motivations to protect information security.*

Training and Coping Appraisal

Information security literature review shows results inconsistency regarding the impact of the coping appraisal constructs, response efficacy and self-efficacy, on compliance. The social cognitive theory (SCT) (Bandura 1986) can be used to explain the development of coping appraisal mechanisms within the context of information security. SCT outlines the influence of perceived self-efficacy and result anticipation on individuals' behavior (Ng et al. 2009). Self-efficacy is the degree to which individuals believe in their own abilities to perform what is required to avert the threat (Boss et al. 2015). SCT maintains that when people perceive that they have the capabilities to take an action that benefits them, they will spend the needed effort to complete the beneficial action anticipating the desired outcome (Bandura 1986). Self-efficacy makes a difference in how people act (Ng et al. 2009). The beliefs about the consequences of one's action and self-efficacy influence goal pursuit (Rhee et al. 2009). In the context of information security, self-efficacy is instrumental in influencing protective response (Posey et al. 2015). Therefore, according to SCT, enabling self-efficacy will influence the desirability of certain actions and would be more effective in encouraging protective behavior (Warkentin et al. 2016).

Information security policies remain to be techno-centric communications of hard to follow recommendations that limit self-efficacy (Doherty et al. 2009). According to the SCT, enabled self-efficacy influences people to be more proactive in taking precautionary measures against possible security threats (Workman et al. 2008). Security training will enable self-efficacy and will reduce the ambiguity regarding threat-mitigating mechanisms (D'Arcy et al. 2014). Security education, training, and awareness (SETA) will improve coping appraisal because information security knowledge and awareness will lead to comprehension, familiarity, and skills to manage security incidents and mitigate risks to information (Sohrabi Safa et al. 2016). The impact of self-efficacy on behavioral change suggests that training to enable employees to perform protective actions will be the most effective approach to engage protective behavior (Warkentin et al. 2016). The use of SETA is consistent with SCT as a critical antecedent to the coping appraisal. Response cost is mainly the extra time and efforts spent to mitigate the risk (Ifinedo 2012; Sommestad et al. 2015). Therefore, SETA will also reduce response cost. Researchers supported the importance of SETA as an integral strategy leading to compliance (Da Veiga and Martins 2015; Posey et al. 2015).

The three elements of SETA are education, training, and awareness (Posey et al. 2015). SETA aims to articulate and communicate goals, expectations, and procedures designed for employees to enable their information security compliance behavior (Johnston et al. 2015). Literature proposed the use of SETA as a strategy to promote secure behavior and minimize accidental security breaches (Warkentin et al. 2016). SETA is used to aid individuals to form the desired security perception (Tsohou et al. 2015). Although information security policies, the behavioral controls, must be in place to protect information, it is important to develop awareness of safe and ethical use (Chatterjee et al. 2015).

SETA programs will advance security skills and knowledge, which will minimize the conflict between policy demands and productivity requirements (Siponen and Vance 2010). Training manifests policy requirements in employees' behavior (Johnston et al. 2015). SETA efforts help form adequate evaluation and understanding regarding threats and recommended behavior (Posey et al. 2015). Training and awareness have a significant positive impact on the information security coping mechanisms in the organization (Da Veiga and Martins 2015). The impact of self-efficacy on behavioral change suggests that training to enable employees to perform protective actions will be the most effective approach to engage

protective behavior (Warkentin et al. 2016). SETA was also found to promote the security culture in the organization, which minimizes the perception of conflict between job requirements and policy demands (Da Veiga and Martins 2015). Organizations can also reduce security-related complexity with SETA initiatives communicating the latest security knowledge and improving employees' technical skills (D'Arcy et al. 2014).

Lack of information security knowledge and experience is the leading cause for information security incidents created by users (Sohrabi Safa et al. 2016). Lack of security training and awareness will increase the perception of the conflict between business opportunities and security demands (Siponen and Iivari 2006). When the response causes performance delay, cost of response will increase and employees will be reluctant to comply (Anderson et al. 2016). SETA programs are needed to enable coping appraisal and influence information security compliance. Therefore, we suggest the following proposition:

Proposition P3: *Individuals with security education, training, and awareness are more likely to have a higher coping appraisal evaluation.*

The coping appraisal is the process by which individuals evaluate the effectiveness and feasibility of the available risk mitigating response (Herath and Rao 2009a; Sommestad et al. 2015). Coping appraisal process utilizes self-efficacy, response efficacy, and response cost (Boss et al. 2015). Coping appraisal is enabled by employees' relevant knowledge and competence to implement preventative security measures (Ifinedo 2012).

Information security literature reflects the positive impact of response efficacy and self-efficacy on compliance intentions (Johnston et al. 2015). Individuals are more motivated to comply with information security policy when they have a belief that the threat is preventable and the ability to participate in the threat mitigating action (Posey et al. 2015; Siponen et al. 2014). The awareness of feasible and manageable response will have a significant positive impact of compliance intentions (Warkentin et al. 2016).

Lack of coping mechanism or low self-efficacy negatively impacts secure behavior because individuals believe that all outcomes are predetermined and therefore, the threat impact is inevitable (Workman et al. 2008). Also, the related literature generally agreed on the significant negative impact of response cost on coping appraisal (Boss et al. 2015; Herath and Rao 2009b). The conflict with organizational goals (Bulgurcu et al. 2010) and the increased security demands and complexity (D'Arcy et al. 2014) will increase the response cost and will negatively impact coping appraisal demotivating individuals' to comply with security policies. Therefore, we suggest the following proposition:

Proposition P4: *Individuals with strong coping appraisal are more likely to have higher motivations to protect information security.*

User Behavior

The primary focus of PMT is to predict intentions toward protection motivation (Maddux and Rogers 1983). Information security literature supports that protection motivation is the strongest predictor of behavioral change (Boss et al. 2015). PMT can be extended to change the actual security behaviors not just to increase protection motivation (Crossler et al. 2013). This paper proposes to measure the impact on actual compliance, the dependent variable. Prior research efforts demonstrated a clear linkage between intention and actual behavior (Johnston et al. 2015). This approach is supported by numerous empirical research studies because intention is viewed to be an indicative of a precondition to a behavioral act (Siponen et al. 2014). Compliance intention is an antecedent and a strong predictor to actual behavior (Sommestad and Hallberg 2013). Therefore, we suggest the following proposition:

Proposition P5: *Strong protection motivation is more likely to lead to actual compliance with information security policies.*

Conclusion

This paper proposed a theoretically grounded model for information security policy compliance utilizing the protection motivation theory (PMT). While PMT has been used before, this is the first paper, to our knowledge, that contextualizes PMT by using concepts from construal level theory to explain the

evaluation of threat appraisal. This helps provide greater specificity to theory. Additionally, the theoretical model also incorporates how and what component SETA does influence. Overall, this provides a more complete nomological map for information security compliance behavior. While beyond the scope of the current paper, we hope that the model presented in the study needs to be empirically tested. The current paper provides well-grounded and theoretically justified propositions that can be tested in multiple contexts to further enhance the theory within the information security context.

Managerially, the model provides two key levers on influencing user behavior besides having a security policy. First lever is to reduce the psychological distance between the user and the threat context. This can be done by increasing organizational commitment, or by communicating how the threat personally impacts the user. The second lever deals with training. The model implies that training needs to be viewed as an ongoing process and not just during initial software implementation. In addition, it needs to include not just task knowledge, but also security knowledge.

REFERENCES

Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D., and Jenkins, J.L. 2016. "How Users Perceive and Respond to Security Messages: A Neurois Research Agenda and Empirical Study," *European Journal of Information Systems* (25:4), pp. 364-390.

Arachchilage, N.A.G., and Love, S. 2014. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective," *Computers in Human Behavior* (38), pp. 304-312.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological review* (84:2), p. 191.

Bandura, A. 1986. *Social Foundations of Thought and Action : A Social Cognitive Theory*. Englewood Cliffs, N.J.: Prentice-Hall.

Boss, S.R., Galletta, D.F., Benjamin Lowry, P., Moody, G.D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp. 523-548.

Chatterjee, S., Sarker, S., and Valacich, J.S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical It Use," *Journal of Management Information Systems* (31:4), pp. 49-87.

Chen, Y., Ramamurthy, K., and Wen, K.W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157-188.

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.

D'Arcy, J., Herath, T., and Shoss, M.K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

Da Veiga, A., and Martins, N. 2015. "Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study," *Computers & Security* (49), pp. 162-176.

Doherty, N.F., Anastasakis, L., and Fulford, H. 2009. "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies," *International Journal of Information Management* (29:6), pp. 449-457.

Herath, T., and Rao, H.R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), 5//, pp. 154-165.

Herath, T., and Rao, H.R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Ho, C.K.Y., Ke, W., and Liu, H. 2015. "Choice Decision of E-Learning System: Implications from Construal Level Theory," *Information & Management* (52:2), pp. 160-169.

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.
Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS quarterly*), pp. 549-566.
Johnston, A.C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-A117.
Kessel, P.v., and Allan, K. 2015. "Ey's Global Information Security Survey," Ernst & Young.
Köhler, C.F., Breugelmans, E., and Dellaert, B.G.C. 2011. "Consumer Acceptance of Recommendations by Interactive Decision Aids: The Joint Role of Temporal Distance and Concrete Versus Abstract Communications," *Journal of Management Information Systems* (27:4), pp. 231-260.
Krishna, A. 2012. "An Integrative Review of Sensory Marketing: Engaging the Senses to Affect Perception, Judgment and Behavior," *Journal of Consumer Psychology* (22:3), pp. 332-351.
Liberman, N., and Trope, Y. 1998. "The Role of Feasibility and Desirability Considerations in near and Distant Future Decisions: A Test of Temporal Construal Theory," *Journal of personality and social psychology* (75:1), p. 5.
Liberman, N., Trope, Y., and Wakslak, C. 2007. "Construal Level Theory and Consumer Behavior," *Journal of Consumer Psychology* (17:2), pp. 113-117.
Maddux, J.E., and Rogers, R.W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of experimental social psychology* (19:5), pp. 469-479.
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.
Posey, C., Roberts, T.L., and Lowry, P.B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.
Rhee, H.-S., Kim, C., and Ryu, Y.U. 2009. "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," *Computers & Security* (28:8), 11//, pp. 816-826.
Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), p. 93.
Safa, N.S., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.
Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.
Siponen, M., and Iivari, J. 2006. "Six Design Theories for Is Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:7), pp. 445-472.
Siponen, M., Mahmood, M.A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & management* (51:2), pp. 217-224.
Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly* (34:3), p. 487.
Sohrabi Safa, N., Von Solms, R., and Furnell, S. 2016. "Information Security Policy Compliance Model in Organizations," *Computers & Security* (56), pp. 70-82.
Sommestad, T., and Hallberg, J. 2013. "A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance," in *Security and Privacy Protection in Information Processing Systems*. Springer, pp. 257-271.
Sommestad, T., Karlzén, H., and Hallberg, J. 2015. "A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour," *International Journal of Information Security and Privacy* (9:1), pp. 26-46.
Tam, L., Glassman, M., and Vandenwauver, M. 2010. "The Psychology of Password Management: A Tradeoff between Security and Convenience," *Behaviour & Information Technology* (29:3), pp. 233-244.
Trope, Y., and Liberman, N. 2003. "Temporal Construal," *Psychological review* (110:3), p. 403.
Trope, Y., and Liberman, N. 2010. "Construal-Level Theory of Psychological Distance," *Psychological review* (117:2), p. 440.
Trope, Y., Liberman, N., and Wakslak, C. 2007. "Construal Levels and Psychological Distance: Effects on Representation, Prediction, Evaluation, and Behavior," *Journal of consumer psychology* (17:2), pp. 83-95.

Tsohou, A., Karyda, M., and Kokolakis, S. 2015. "Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs," *Computers & Security* (52), pp. 128-141.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3–4), pp. 190-198.

Warkentin, M., Walden, E., Johnston, A.C., and Straub, D.W. 2016. "Neural Correlates of Protection Motivation for Secure It Behaviors: An Fmri Examination," *Journal of the Association for Information Systems* (17:3), pp. 194-215.

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.