Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture

Qing Hu
Department of Information Systems
College of Business
Iowa State University
e-mail: qinghu@iastate.edu

Tamara Dinev
Department of Information Technology and Operations Management
College of Business
Florida Atlantic University
e-mail: tdinev@fau.edu

Paul Hart
Department of Information Technology and Operations Management
College of Business
Florida Atlantic University
e-mail: hart@fau.edu

Donna Cooke
Department of Management Programs
College of Business
Florida Atlantic University
e-mail: cooke@fau.edu

Acknowledgement

This project was partially funded by a grant to the authors from the Defense Information Systems Agency (DISA) of the Department of Defense (DoD). The authors would like to express their thanks to the editor, senior editor, associate editor, and two anonymous reviewers for their detailed and constructive comments and suggestions throughout the review process.

ABSTRACT

We develop an individual behavioral model that integrates the role of top management and organizational culture into the theory of planned behavior in an attempt to better understand how top management can influence security compliance behavior of employees. Using survey data and structural equation modeling, we test hypotheses on the relationships among top management participation, organizational culture, and key determinants of employee compliance with information security policies. We find that top management participation in information security initiatives has significant direct and indirect influences on employees' attitudes toward, subjective norm of, and perceived behavioral control over compliance with information security policies. We also find that the top management participation strongly influences organizational culture which in turn impacts employees' attitudes towards and perceived behavioral control over compliance with information security policies. Furthermore, we find that the effects of top management participation and organizational culture on employee behavioral intentions are fully mediated by employee cognitive beliefs about compliance with information security policies. Our findings extend information security research literature by showing how top management can play a proactive role in shaping employee compliance behavior in addition to the deterrence oriented remedies advocated in the extant literature. Our findings also refine the theories about the role of organizational culture in shaping employee compliance behavior. Significant theoretical and practical implications of these findings are discussed. [Submitted: November 5, 2010. Revised: April 29, 2011; August 11, 2011; November 6, 2011. Accepted: December 9, 2011.]

Keywords: Compliance Behavior, Information Security, Organizational Culture, Theory of Planned Behavior, Top Management.

INTRODUCTION

One of the key challenges in information security management is to understand how organizational, individual, and technical factors together affect the outcomes of information security in an organization. Although computer hackers and criminals are often headlined in the mainstream media, evidence suggests that more information security incidents occur as a result of internal employee actions (Richardson, 2008). In fact, human agents inside an organization could be more dangerous than those outside the organization due to their intimate knowledge of the organizational information systems and access to data in the course of their routine work activities (Bulgurcu, Cavusoglu, & Benbasat, 2010; Siponen & Vance, 2010; Johnston & Warkentin, 2010; Herath & Rao, 2009a, 2009b). A recent survey of IT managers of global companies indicates that people remain the weakest link for information security in organizations and 50% of the respondents stated that organizational awareness is the most significant challenge to delivering successful information security initiatives (Van Kessel, 2008). According to Symantec and Ponemon (2009), 59% of ex-employees admit that they steal confidential company data, such as customer contact lists. The CSI Computer Crime & Security Survey (Richardson, 2008) shows that 44% of the respondents reported insider abuse of computer systems, making it the second most frequent form of security breach, only slightly behind virus incidents, but well above the 29% of respondents who reported unauthorized access from external sources.

The threats to organizational digital assets from external and internal sources have prompted organizations not only to install advanced hardware and software systems for defending against the potential malicious attacks from outsiders, but also to establish various information security policies and procedures to reduce and deter intended or unintended behavior of employees that could either weaken the effectiveness of the hardware or software defense systems or render them entirely useless. For example, two common components in most information security policies are the prohibitions of using private USB drives on corporate computers and visiting non-work related

Web sites via corporate computers. Non-compliance with either rule can have disastrous consequences for an organization regardless of how much the organization has invested in security hardware and software. Yet, numerous accounts of significant security breaches can be attributed to non-compliance behavior of employees. An unsuspecting employee visiting a benign but compromised shopping site using a work computer could easily have malware installed on the computer and open the door for attacks by the proprietor of a botnet (Stone-Gross, Cova, Cavallaro, Gilbert, Szydlowski, Kemmerer, Kruegel, & Vigna, 2009; Markoff, 2010); and inserting an infected USB drive into a corporate computer could install malicious software that captures and transmits confidential data from the computer to outside entities (Holmes, 2008; Mills, 2010).

While the significant role of human agents in organizational information security has long been recognized by scholars, there are important differences in the literature about what causes the non-compliance behaviors and therefore how to effectively manage the behaviors. Scholars investigating information security issues have based their analyses on a variety of theories, including general deterrence theory (Straub, 1990; D’Arcy, Havav, & Galletta, 2009), control theory (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009), theory of planned behavior (Dinev & Hu, 2007; Bulgurcu et al., 2010), institutional theory (Björck, 2004; Hu., Hart, & Cooke, 2007), communication theory (Johnston & Warkentin, 2010), learning theories (Puhakainen & Siponen, 2010), and criminology theories (Willison & Backhouse, 2006; Siponen & Vance, 2010; Hu, Xu, Dinev, & Ling, 2011). However, the effect of organizational culture, one of the key constructs in organizational and individual behavior literature, on information security has not been rigorously examined. Moreover, a key organizational component, the top management, has not been adequately investigated in theoretical or empirical models in the extant literature, with the notable exception of the study by Puhakainen and Siponen (2010). Given the critical role of top management in many organizational areas−culture, employee behavior, and performance (Kouzes & Posner, 1987; Jarvenpaa & Ives, 1991; Schein, 2004; Liang, Saraf, Hu, & Xue, 2007; Puhakainen

& Siponen, 2010)−studies on the single and combined effects of top management, organizational culture, and employee cognitive beliefs on information security compliance behavior are needed to develop a better theoretical understanding and devise more effective information security management practices.

In this study, we address these gaps in the literature by adopting an integrative approach to understanding employee compliance behavior with consideration toward organizational stimuli and individual cognitive processes in the context of information security. We set out to study two central research questions that have not been adequately investigated in the information security literature: (i) What is the role of organizational culture in shaping employee intention to comply with information security policies? (ii) How does the top management influence employee intention to comply with information security policies? We attempt to answer these two questions by conceptualizing and empirically testing an integrated behavioral model that combines the theoretical frameworks of top management championship, organizational culture, and planned behavior with survey data collected from employees in a wide range of firms.

Our focus on how top management and organizational culture influence employee cognitive beliefs which in turn shape their compliance intention sets this study apart from the majority of the extant studies, which primarily offer an instrumental view of employee compliance intention based on the rational choice framework of economic theory (e.g., Bulgurcu et al., 2010; Siponen & Vance, 2010) or the deterrence theory of criminology (e.g., Straub, 1990; D'Arcy et al., 2009; Herath & Rao, 2009a). In addition, by showing how top management actions can shape perceived organizational cultural values, we have the potential to offer top management the practical insights for designing workplaces that inspire self-regulation and foster rule adherence among employees. In doing so, we fill a significant gap in the information security research and practice—how top management and organizational culture complement each other in shaping employee behavior intentions and therefore behavior toward compliance. Finally, our finding that the influences of top management and organizational culture on employee compliance intention are fully mediated by the constructs of the theory of planned behavior not only refines our understanding of how these two critical organizational factors work but also challenges the established theories about the how top management and organizational culture influence employee behavioral intentions.

The rest of the paper is arranged as follows. In the next section, we review the extant research on information security from the socio-organizational perspective and based on this review we develop research hypotheses and propose a theoretical model that highlights how organizational factors influence employee behavior towards information security policy compliance. This is followed by a description of our research design and data collection, as well as analyses of the data using structural equation modeling. We then present a discussion on the theoretical and practical implications of the findings, especially on how our findings could inform management on shaping the information security policy compliance behavior of employees. After a brief discussion of the study's limitations, we highlight the conclusions and discuss future research directions.

LITERATURE REVIEW

Culture, Leadership, and Employee Behavior

Culture in organizational literature has been studied by a variety of scholars and has been defined in a range of ways (Ouchi & Wilkins, 1985; Smircich, 1983; Tsui, Zhang, Wang, Xin, & Wu, 2006; Cameron & Quinn, 2006). In a review of early studies on organizational culture, Smircich (1983) argued that culture, when conceived as shared key values and believes, fulfills at least four important functions in organizations: (i) culture conveys a sense of identity to organizational members; (ii) facilitates the generation of commitment to something larger than itself; (iii) enhances the stability of social systems; and (iv) serves as a sense-making device that can guide and shape the behavior of the members. Smircich (1983) further concluded that the stream of research on organizational culture "offers a tantalizing prospect—that organization culture may be another critical lever or key by which strategic managers can influence and direct the course of their organizations" (p. 346). This view articulates two critical aspects about organizational culture: organizational culture shapes and guides the behavior of organizational members via shared values among the members and commitment to the organization, and organizational culture can be influenced and managed by organizational leadership (i.e., the top management). Accordingly, two streams of research in the literature can be identified that closely follow this instrumental view of organizational culture.

One stream of research in the organizational culture literature focuses on how culture shapes employee value, cognition, and behavior in organizational settings. In Smircich's (1983) view, organizational culture expresses the values of social ideals and the patterns of beliefs that are shared by organizational members and manifested by symbolic devices such as myths, rituals, stories, legends, and specialized languages. Harris (1994) investigated how organizational culture influences the mental schema employees use to make sense of organizational phenomena and to formulate responses, such as "I think it means this and I would be inclined toward this response" (p. 309). He identified categories of "in-organization" schemas that capture the range of knowledge need for the sense-making effort and concluded that organizational culture is reflected in the emergence of congruent schemas among the members which are similarly salient to organizational stimuli (i.e. concepts, events, people, and groups), and which shape and are shaped by the social sense-making process of intra-psychic mental dialogue between self and others. Jones, Jimmieson, and Griffiths (2005) conducted a longitudinal study on how employees' perception of organizational culture values influences their readiness to change and ultimately the success of organizational change implementation. They found that employees who perceive their workplace to be dominant in human relations values (training and development, open communications, and participative decision making) are more likely to hold positive views towards organizational change, have higher levels of readiness for change, and report higher levels of satisfaction. Similarly, studies have found that organizational culture influences many other aspects of employees' cognitive, attitudinal, and behavioral outcomes (Lund, 1986; Douglas, Davidson, & Schwartz, 2001; Schrodt, 2002).

Another stream of organizational culture research focuses on the relationship between organizational culture and organizational leadership on the premise that organizational culture itself can be shaped and manipulated by the top management (Trice & Beyer, 1993; Bass, 1998; Schein, 2004), suggesting that organizational culture can be objectively managed, a critical theoretical foundation for this study. Bass and Avolio (1993, p. 113) argued that

> [t]here is a constant interplay between culture and leadership. Leaders create mechanisms for cultural development and the reinforcement of norms and behaviors expressed within the boundaries of the culture. Cultural norms arise and change because of what leaders focus their attention on, how they react to crises, the behaviors they role model, and whom they attract to their organizations. The characteristics and qualities of an organization's culture are taught by its leadership and eventually adopted by its followers.

Ke and Wei (2008) argued a one-to-one correspondence between the behaviors of top management and the characteristics of organizational culture, such as power sharing behavior and power sharing culture, participative behavior and participative decision making culture, and transformative vision and risk-tolerance culture. Although the assumption that top management is the main shaper and builder of organizational culture has been taken for granted by functionalists who focus on the consequence of organizational culture, Tsui, Zhang, Wang, Xin, and Wu (2006) argued that there is still significant debate on the issue of whether leaders, especially top executives, can create or change organizational culture, and offered a contingency perspective. Nonetheless, the instrumental role of top management in shaping organizational culture has been supported with some empirical evidence (Hartog, Muijen, & Koopman, 1996; Jaskyte, 2004; Tsui et al., 2006).

Top Management, Organizational Culture, and Information Security

Despite a rich literature on culture and leadership in management and IS studies, the significant influences of organizational culture and top management on employee behavior have not attracted adequate attention in information security literature. IS scholars have focused their attention primarily and justifiably on employees—the weakest link in the information security defense—when studying information security in organizational settings. While many important theoretical frameworks and models have been advanced and many organizational and individual factors have been found to influence employee information security behavior, the dominant theoretical frameworks are cognitive theories (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Herath & Rao, 2009b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010) and criminological theories (Straub, 1990; Willison & Backhouse, 2006; D'Arcy, Havav, & Galletta, 2009; Siponen & Vance, 2010; Hu, Xu, Dinev, & Ling, 2011). Von Solms and Von Solms (2004a) are perhaps the first to argue that security policies must be instilled into organizational culture in order to be effective. They argued that a security culture involves two components: the shared assumption about information security, and the education of these shared assumptions among the members of the organization. They further argued that the shared assumption can be established by management through drafting a series of organizational security policies that are acceptable to the members. Education activities can reinforce these assumptions, frame organizational culture, and influence desired employee behavior. Von Solms and Von Solms (2004b) were also among the first to identify top management as one of the most critical elements in information security when they listed "not realizing information security is a corporate governance responsibility" as the top of the ten deadly sins in information security management. Similarly, Young and Windsor (2010) argued the importance of top management from the information security planning perspective based on literature. However, no empirical evidence was provided to support the arguments in these studies.

Puhakainen and Siponen (2010) and Chang and Lin (2007) are among the few studies that directly tested the role of top management and organizational culture with empirical data in an information security context. In an action research about designing and implementing effective training programs for information security policy compliance, Puhakainen and Siponen (2010) found that the perceived passiveness of the CEO in promoting and following the established information security policies was one of the main reasons the employees ignored the policies that required encryption of emails. After the CEO changed his attitude toward information security and became actively involved in information security issues, there were measureable changes in employee attitudes toward information security policy compliance and as well as employee participation in information security discussions and initiatives.

Drawing on the competing value framework of Quinn and Spreitzer (1991), Chang and Lin (2007) operationalized and measured organizational culture in terms of four cultural traits (cooperativeness, innovativeness, consistency, and effectiveness) and linked these four traits to four information security management constructs (confidentiality, integrity, availability, and accountability) in a fully connected structural model. The authors found that flexibility oriented cultures (cooperativeness and innovativeness) have no or negative impact on information security measures, while control oriented cultures (effectiveness and consistency) have significant and positive impact on information security measures.

Theoretical Gaps in Information Security Research

Based on the above literature review, we argue that there are at least three major theoretical gaps in the literature, which also create major voids in guidance for effective information security management practices. First, despite the fact that scholars have noted and studied the important role of organizational culture in information security, the studies we found generally lack strong theoretical foundations for linking organizational culture or cultural values to information security outcomes. It is not clear whether organizational culture directly influences information security outcomes or the effect of organizational culture is mediated by other organizational or individual level factors, since no alternative models have been advance or tested. Second, it is notable that in the empirical information security studies we found, the role of top management is either absent from or not explicit in the models. Although the case evidence provided by Puhakainen and Siponen (2010) is significant, it is not clear that such a strong relationship between top management actions and employee security behavior will hold in a large sample of organizations or in what ways top management actions impact employees' cognitive processes. Finally, given our previous review of the leadership role in shaping organizational culture and influencing employee behavior, as well as the consensus in the literature that top management is one of the critical success factors in almost every IS initiative in organizations (Jarvenpaa & Ives, 1991; Sharma & Yetton, 2003; Liang et al., 2007), articulating and testing the explicit role of top management in shaping organizational culture and the combined effect of top management and organizational culture on employee security behavior will fill a major void and make a significant contribution to the theory and practice of information security management. In the next section, we present our conceptual and research models and hypotheses that explicate how top management could shape employee information security compliance intentions directly and indirectly in conjunction with organizational culture values.

THEORY AND HYPOTHESES DEVELOPMENT

Conceptual Model

The extant literature on individual behavior primarily focuses on belief constructs thought to influence individual conduct, as typified by the theory of planned behavior (Ajzen, 2005). These constructs are salient beliefs and attitudes toward a focal behavior in a social context. Employee behavior, on the other hand, is often shaped and constrained by organizational culture, value, structure, processes, and rules enacted by management (Smircich, 1983; Kouzes & Posner, 1987; Harris, 1994; Sharma & Yetton, 2003; Schein, 2004). However, the linkages between top management actions, organizational culture, and employee behavior have not been articulated and tested in much of the empirical literature on information security. The effects of top management and organizational culture must be accounted for in order to fully understand the employee information security behavior in organizations and to develop effective information security management practices.

The behavior of interest in this study is the individual's intention to comply with organizational information security policies. We need to understand why information security policies are followed by some employees and ignored by others, and why in some organizations employees have a stronger sense of responsibility and accountability towards information security than in others. To accomplish that, we draw on the findings of prior literature on human behavior, leadership, and organizational culture, and argue that it is necessary to integrate different theoretical paradigms and analyze the roles of top management and organizational culture in shaping employees' beliefs and attitudes, which in turn dictate their compliance intention according to the theory of planned behavior (Ajzen, 2005). The fundamental thesis of this study is that in organizations, top management can shape and influence the dominant values, beliefs, and norms shared by employees and thus certain aspects of organizational culture; the actions of the top managers and certain organizational cultural value dimensions then affect employees' salient beliefs and attitudes toward information security policies, which in turn, affect the employees' intention and behavior towards information security policy compliance. This logic is depicted in Figure 1. While the thesis is not a radical departure from current literature in any sense, explicating how top management actions, what organizational cultural value dimensions, and which employee salient belief constructs are significant, and testing how these elements work together in forming the causal map of employee compliance intention, constitute the main contributions of this study.

Insert Figure 1 Here

The Role of Individual Cognition

A rich body of literature exists on individual behavioral models and theories. For our purpose, we draw on the well-established theoretical model for individual behavior, the theory of planned behavior (TPB) by Ajzen (2005), to form the nomological core of our research model of employee compliance behavior. TPB contends that a person’s behavior is determined by his or her intention (INT) to perform the behavior of interest. Although understanding and predicting individual behavior is the goal of the theory, measuring the actual behavior has not been an easy task for scholars, especially those studying in organizational settings. Therefore, considering the strong correlation between intentions and actual behavior (Ajzen, 2005), when faced with practical difficulties for measuring actual behavior, researchers have often chosen to investigate behavioral intentions as the dependent variable (e.g., Gefen, Karahanna, & Straub, 2003; Pavlou & Fygenson, 2006; Herath & Rao, 2009a, 2009b; Bulgurcu et al., 2010; Siponen & Vance, 2010). So is the case with this study.

Intention is assumed to capture the motivational factors that influence an individual’s behavior. In the TPB framework, intention is determined by three factors: attitude toward the behavior (ATT), subjective norm (SN), and perceived behavioral control (PBC). ATT refers to a person’s judgment as to whether it is good or bad to perform a behavior of interest. SN reflects the person’s perceptions of whether the behavior is accepted and encouraged by his or her social circles consisting of people who are important to him or her. In an organizational setting, when the behavior of interest is associated with organizational policies and practices, the person’s relevant social circle of important people are his or her colleagues, subordinates, and superiors. Perceived behavioral control (PBC) is the perceived ease or difficulty of performing a behavior and a personal sense of having the skills and resources to perform it (Ajzen, 2005).

Extensive literature and numerous IS studies (e.g. Taylor & Todd 1995; Harrison, Mykytyn, & Riemenschneider, 1997; Ajzen, 2005; Pavlou & Fygenson 2006; Dinev & Hu, 2007) on individual behavior in a variety of organizational and social settings have rendered strong support for the fundamental propositions of this theory that an individual's attitude, subjective norm, and perceived behavioral control significantly influence the individual's behavioral intention. Most recently, Bulgurcu et al. (2010) found that attitude, normative beliefs, and self-efficacy all have significant impact on employee compliance intention to information security policies. Adapting the propositions of the theory of planned behavior to the context of organizational information security, it is a straightforward logical deduction for us to propose that:

H1a: Stronger positive attitude towards information security policy compliance leads to stronger behavioral intention to comply with the policies.

H1b: Stronger subjective norm about information security policy compliance leads to stronger behavioral intention to comply with the policies.

H1c: Stronger perceived control over information security policy compliance leads to stronger behavioral intention to comply with the policies.

The Role of Organizational Culture

While there is significant debate on whether organizational culture, or culture in general, can be measured and at what level (Denison, 1996), in this study we adopt the value perspective of culture in order to carry out a quantitative inquiry about the role of culture in organizational settings. That is, we define organizational culture in terms of the values that "represent a manifestation of culture that signify espoused beliefs identifying what is important to a particular cultural group" (Leidner & Kayworth, 2006, p. 359), which is similar to the definition by Tsui et al. (2006) that organizational culture is "a set of core values consensually shared by organizational member" (p. 117). To operationalize these shared beliefs and values which are assumed to be the manifestation of the underlying organizational culture, we followed many organizational studies and adopted the competing value framework (CVF) of organizational culture proposed by Quinn (1988).

Quinn's (1988) value-based organizational culture framework has been widely adopted and adapted in quantitative studies of organizational culture and has served as a useful tool for empirically testing a wide range of relationships between organizational cultural values and organizational and individual behavior (e.g., Buenger, Daft, Conlon, & Austin, 1996; Vandenberghe & Peiro, 1999; Jones et al., 2005; Iivari & Huisman, 2007). Just like the definition of culture itself, there are a number of alternative organizational cultural value dimensions and frameworks in the literature, including the six-dimension framework by Hofstede, Neuijen, Ohayv, and Sanders (1990), the five value dimensions by Tsui et al. (2006), and a number of others as reviewed by Cameron and Quinn (2005). In addition, Quinn's (1988) framework has evolved over the years with different labeling for the four cultural value orientations (e.g., Quinn & Rohrbaugh, 1983; Quinn, 1988; Quinn & Spreitzer, 1991; Cameron & Quinn, 2005). However, the characteristics of the basic framework remain largely unchanged. We use the Van Muijen et al.'s (1999) adaptation of Quinn's (1988) original CVF in this study because we believe it is more parsimonious and appropriate for the objectives and the context of this study, given our task of integrating multiple theoretical frameworks.

In the Van Muijen et al. (1999) model, organizational culture is described in terms of four basic values: support orientation, innovation orientation, goal orientation, and rule orientation. These are located in the four quadrants formed by the two opposing value orientation poles (flexibility vs. control, external vs. internal). Support orientation refers to the spirit of sharing, cooperation, team, trust, and individual growth; innovation orientation describes the creative, open-to-change, anticipative, and experimental elements of the organizational culture; goal orientation refers to rationality, accomplishments, accountability, and contingent awards; and finally, rule orientation is characterized as respect for authority, rationality for procedures and rules, hierarchical structure, and formal communications (Van Muijen et al., 1999).

Instead of considering all four cultural orientations in our research model, which will significantly increase model complexity and reduce theoretical clarity, we chose the two cultural orientations in the lower half the CVF framework in the direction of control and opposite of flexibility, which includes rule orientation and goal orientation quadrants. There are two main reasons for this decision. First, it is evident that in the context of compliance with information security policies, the most salient cultural values that shape security related behaviors are goal-orientation and rule-orientation. This is because the focal behavior is about conforming to existing policies, about following established rules and practices, and about accomplishing an objective of a higher level of information security. For most employees, this behavior does not constitute core activities that lead to expected work outcomes, it is usually not measured in key performance indicators, and is rarely rewarded like other personal or team achievements. Information security compliance behavior is a “follow the rules” behavior that is not designed to invoke creativity, thought processes, or critical thinking. Instead, a desired behavior is one that is internalized and automatic for employees, much like a driver following road signs and rules so he or she can safely and efficiently reach the destination. Second, in an empirical study by Chang and Lin (2007), the authors tested the relationship between the four cultural orientations (albeit with slightly different labels) and information security outcome measures with a series of regression analysis, and found that only the cultural values related to control (consistency and effectiveness) have a significant impact on information security outcomes. A similar approach was used by Jones et al. (2005) in which only the cultural orientations of the upper half of the CVF (in the direction of flexibility) were used for testing the impact of organizational culture on the success of organizational change. Therefore, in this study, we focus on the role of goal orientation and rule orientation cultural values in influencing individual cognitive beliefs towards information security policies. In particular, we use the perceived values of these cultural value dimensions at the individual level instead of the collective concept at the organizational level as they are defined. Tsui et al. (2006) argued that if organizational culture is defined as shared knowledge about the prevalent rules, norms, or values that shape preferences or actions of participants, then the subjective interpretation of the participants is preferred over objective indicators as ways to measure organizational culture. Similarly, Srite and Karahanna (2006) strongly argued for using espoused (individually perceived) cultural values when studying how national culture shapes individual behavior towards technology acceptance.

The cultural value of goal orientation reflects a collective understanding of organizational goals, individual responsibility, and individual accountability. As a manifested value of the underlying organizational culture, goal orientation emphasizes planning and goal setting in organizational processes in order to achieve efficiency and productivity (Quinn & Rohrbaugh, 1983). Studies suggest that goal orientation has two distinctive dimensions (Dweck, 1986; Heyman & Dweck, 1992; Button, Mathieu, & Zajac 1996): the learning dimension in which individuals develop competence by acquiring new skills and mastering new situations; and the performance dimension in which individuals demonstrate and validate competence by seeking favorable judgments and avoiding negative judgments. Extensive empirical work by Button et al. (1996) further showed that both dimensions can be dispositional and situational, thus making the link between organizational culture and individual goal orientation plausible. Research shows that learning oriented individuals see intelligence as malleable, continually seek challenges, and persistently examine the results of their behavior in order to determine the best strategy for their next attempt at the same task or situation (Lin & Chang, 2005). Colquitt and Simmering (1998) found that goal oriented individuals have stronger motivation to learn both before the task and after the performance feedback is given. Dimensions of goal orientation have been shown to influence individuals' task-specific efficacy, learning strategy, feedback seeking behavior, and other cognitive and attitudinal beliefs (Payne, Youngcourt, & Beaubien, 2007). The findings of these studies link goal orientation directly to attitude, subjective norm, and perceived behavioral control constructs. Given the fact that effective compliance with information security requires employees to overcome technical and social barriers and adapt to new organizational realities, we expect that goal oriented culture and individual goal orientation will likely shape employees' attitudes, subjective norms, and task-specific self-efficacy—in this case the perceived behavioral control—toward new information security initiatives, programs, and policies. Therefore, we propose:

> *H2a: Stronger perceived goal oriented cultural value leads to stronger positive attitude towards compliance with information security policies.*
>
> *H2b: Stronger perceived goal orientated cultural value leads to stronger subjective norm about compliance with information security policies.*
>
> *H2c: Stronger perceived goal orientated cultural value leads to stronger perceived behavioral control over compliance with information security policies.*

The culture of rule orientation reflects authority and compliance. It seeks stability and control via effective information management and communication processes within an organization (Quinn & Rohrbaugh, 1983). An organization with strong rule orientation would invest a significant amount of time developing and implementing carefully designed policies, and make a significant amount of effort on training employees. A rule-oriented organization culture would signal strong expectations via multiple channels such as internal communications and formal training programs to employees including their social circle of peers, superiors, and subordinates to ensure compliance with the rules and policies. These expectations would influence the employee's attitudes and norms regarding the information security policies. Additionally, clearly stated rules help employees model their behavior, facilitate their compliance, and make it easier for them to internalize the rules and practices (Boss et al., 2009). That is, employees will feel more in control of their actions and outcomes.

There is limited and indirect empirical work on the effectiveness of rule oriented organizational culture on shaping employee beliefs and behavior in organizational settings. Weaver and Treviño (1999) found that ethical programs that emphasize compliance with rules and behavioral monitoring of compliance are significantly associated with lower observed unethical conduct, willingness to seek ethical advice, and awareness of ethical issues at work. Puhakainen and Siponen (2010) found that properly designed training programs improved employee awareness about the possible consequences of non-compliance toward established information security policies, resulting in increased level of compliance. As a cultural value, we can reasonably expect that rule-oriented influence on employee beliefs and behavior should be similar to the expected influence of culture in general in the context of compliance with information security policies where rule following is the focal concern. For example, a rule oriented culture should be favorable to employees who view compliance with information security policy positively, thus fostering a stronger organizational norm for compliance. It can also be argued that a rule oriented culture would motivate employees to acquire new knowledge and skills in order to be in compliance with specific policies, thus leading to a stronger sense of efficacy for compliance. It is logical to speculate that in rule oriented organizations in which communication and training about rules and policies are emphasized, employees will have a higher level of information security awareness which has been show to be positively related to employees' attitudes toward information security policy compliance (Bulgurcu et al., 2010). Awareness of protective technologies against spyware was found to play a central role in influencing individual attitude and subjective norm in the context of individual use of these technologies (Dinev & Hu, 2007). The positive relationships between deterrence variables and employee compliance behavior in the information security literature (e.g., Straub, 1990; D'Arcy et al., 2009; Herath & Rao, 2009a) also provide indirect evidence that rule orientation in organizations can influence individuals' attitudes, subjective norm, and perceived control related to information security compliance, based on the theory of planned behavior. Therefore, we propose that:

H3a: Stronger perceived rule orientated cultural value leads to stronger positive attitude toward compliance with information security policies.

H3b: Stronger perceived rule orientated cultural value leads to stronger subjective norm about compliance with information security policies.

H3c: Stronger perceived rule orientated cultural value leads to stronger perceived behavior control over compliance with information security policies.

These hypotheses assume that the influences of organizational culture via its manifested values on employee behavior are mediated by the salient employee belief constructs (attitude, subjective norm, and perceived behavioral control). However, the studies on organizational culture often suggest significant direct linkages between the perceived cultural values and the behavior or behavioral intentions of individuals. In two separate studies of employee adherence to organizational rules, Tyler and Blader (2005) consistently found that an employee's perception of the legitimacy of the rules and the moral value congruence between the organization and the employee are the most significant predictors to the three forms of rule adherence: compliance, deference, and rule breaking. Later, Tyler, Callahan, and Frost (2007) found the same results, that these perceived values strongly influence the rule adherence behaviors of the law enforcement agents. In a study on employee compliance with ethical rules, Weaver and Treviño (1999) found that employees' perceptions of the value-based orientation of their organization, as measured by items such as "counseling employees," "encourage shared values," "supporting employee goals and aspirations," "evaluating performance in light of company values," and "helping employees make decisions," strongly influence compliance with ethical rules. In an empirical study of organizational culture's impact on information security, Chang and Lin (2007) found that control oriented organizational values (consistency and effectiveness) are significantly associated information security measures (confidentiality, availability, and accountability). Although these studies did not test the effect of other organizational values on employee compliance behavior, we can reasonably infer that both the goal orientation and rule orientation, which are similar to the values measured in these studies, should have similar effects on employee compliance behavior toward information security rules and policies. Thus, we propose that:

> *H4: Stronger perceived goal orientated cultural value leads to stronger intention to comply with information security policies.*
>
> *H5: Stronger perceived rule orientated cultural value leads to stronger intention to comply with information security policies.*

The Role of Top Management

In organizational settings, cognitive beliefs of employees, including attitudinal, normative, and control beliefs, are inevitably influenced by the observed conduct of top management (Jarvenpaa & Ives, 1991; Armstrong & Sambamurthy, 1999; Sharma & Yetton, 2003; Puhakainen & Siponen, 2010), in addition to the perceived organizational cultural values and other factors. Following Jarvenpaa and Ives (1991) and Liang et al. (2007), we use top management participation (TMP) as the most direct indicator of the top management's involvement in the organization's information security related issues from the perspective of employees. TMP is defined as the behavior and actions of top managers in facilitating organizational actions in the focal phenomenon (Liang et al., 2007). However, since TMP is an organizational level measure in its theoretical origin, we adapted and measured it as the perceived top management participation (PMP) by individual employees in order to be consistent with the model and the rest of the constructs used in this study. The theoretical justification for this adaption is similar to the one for using perceived cultural values when studying individual behavior. We argue that if the actions of top management are to have any impact on employee cognitive beliefs, they must be observed and comprehended by the employees. Thus, we argue that PMP is preferred over the objective indicators for TMP, following a similar logic advanced by Tsui et al. (2006) concerning the measurement of organizational culture and by Srite and Karahanna (2006) concerning the measurement of national culture.

The critical role of top management participation in IT implementation and assimilation in organizations has been clearly established in the literature (Jarvenpaa & Ives, 1991; Armstrong & Sambamurthy 1999; Sharma & Yetton 2003; Liang et al., 2007). Literature on top management suggests at least three significant mechanisms through which top management can shape the beliefs, norms, and attitudes of employees towards new programs, initiatives, or policies. The first is the legitimacy mechanism. By championing the new initiatives, programs, or policies through articulating a clear vision and strategy and setting the goals and measures about the initiatives, programs, or policies, top management renders legitimacy to these initiatives, programs, and policies. Legitimacy of the new initiatives, programs, and policies related to information security is especially important since such initiatives, programs, and policies are often considered as “extra work” or even a burden to routine job related tasks (Albrechtsen, 2007; Hu, Hart, & Cooke, 2011). Tyler and Blader (2005) and Tyler et al. (2007) showed that an individual’s judgment about the legitimacy of organizational rules and policies has a significant impact on the individual’s intention to follow the rules and defer to the policies. Top management participation in security initiatives could send a strong signal to other managers and employees about the legitimacy of the initiatives.

The second mechanism is commitment. Top management participation conveys a strong commitment to the established goals and objectives to all members of an organization. If the commitment is perceived as creditable, employees will respond by trusting management and by making decisions in congruence with the championed initiatives, programs, or policies (James, 2000). It is up to the top managers to follow up with the execution of these goals, to hold lower level managers and employees accountable for non-actions or non-compliance, and to convey the seriousness and risks of non-performance. Top management participation also helps resolve conflicts among different stakeholders, allocate and commit resources, and create organizational structures and roles that facilitate the implementation of the new initiatives, programs, and policies which otherwise could have been bogged down or derailed due to inter-unit politics and power struggles (Smith, Winchester, Bunker, & Jamieson, 2010).

The third is the fairness and justice mechanism. Tyler et al. (2007, p. 467) argued that

> “[w]ithin work settings it has been shown that employees are more likely to view as legitimate and to comply with workplace rules and policies if they view the organization within which they work as exercising their authority via fair procedure. This procedural justice effect is widespread and shows that procedural justice encourages legitimacy, commitment, and rule adherence.”

This argument is based on a psychological model of human behavior suggesting that an organizational environment characterized by fair procedures will activate strong employee organizational identification, lead them to engage in desirable workplace behavior, and hold positive attitudes toward the organization (Tyler et al., 2007). Top management participation in the new initiatives, programs, and policies provides opportunities for employees to express their opinions, have input in evaluations, control the influence of bias, and design systems of management that are sensitive to procedural concerns, which contribute to the perceived fairness and procedural justice related to the initiatives, programs, and policies (Tyler et al., 2007).

While most of the literature we cited here is from outside the context of information security, the underlying logic in these arguments are relevant and applicable to understanding the effect of top management participation on employee attitudes, subjective norm, and perceived behavioral control in the context of information security policy compliance. For example, the legitimacy and justice mechanisms would be effective in influencing the attitudes and the subjective norm of employees toward information security policies when top management is perceived as actively participating in information security initiatives and programs. Similarly, the commitment mechanism would be effective on motivating and reassuring employees to commit to compliance behavior by participating in training to acquire necessary skills. Puhakainen and Siponen (2010) provided direct evidence of how top management actions in supporting the established information security policy observed by employees changed the attitudes of the employees and resulted in higher levels of compliance as well as discussions on new information security initiatives among the employees. However, their results are based on direct observations of a small number of employees and no theoretical hypotheses were tested. Thus, we propose:

H6a: Stronger perceived top management participation in information security initiatives leads to stronger positive attitude towards compliance with information security policies.

H6b: Stronger perceived top management participation in information security initiatives leads to stronger subjective norm about compliance with information security policies.

H6c: Stronger perceived top management participation in information security initiatives leads to stronger perceived behavioral control over compliance with information security policies.

One of the most important outcomes from top management participation is how the latter influences organizational culture (Bass & Avolio, 1993; Schein, 2004; Tsui et al., 2006; Ke & Wei, 2008). Schein (2004) argued that organizational culture springs from three sources: (i) the beliefs, values, and assumptions of the founders of an organization; (ii) the learning experiences of the members as their organization evolves; and (iii) new beliefs, values, and assumptions brought in by new members and leaders. He identified six primary embedding mechanisms through which organizational leaders can reinforce the adoption of their own beliefs, values, and assumption in organizations, in effect changing the organizational culture. These mechanisms include paying attention to, measuring, and controlling on a regular basis, reactions to critical incidents and crisis, allocating resources, role modeling, teaching, and coaching, allocating rewards and status, and recruiting, selecting, promoting, and excommunicating members (Schein, 2004). Ke and Wei (2008) argued that a more explicit one-to-one relationship between top management action and organizational culture dimensions, such as active top management participation leads to a participative decision making culture. Therefore, it is logical to infer that top management actions and engaging participation in information security initiatives and programs will directly influence relevant organizational culture values such as the goal and rule orientations, especially how these values are perceived at the individual level. Their demonstrated actions and expressed beliefs eventually are permeated into employee cognitive beliefs and attitudes and influence or change organizational culture via the embedded mechanisms identified above. It is logical to speculate that the mechanisms through which top management participation influences employee attitudes and beliefs as discussed above should have a similar effect on shaping organizational cultural values of goal orientation and rule orientation. Top management participation in establishing and enforcing information security policies will send strong signals to employees about the legitimacy of these policies and the organizational commitment toward the goal of a high level information security.

Again, the action research conducted by Puhakainen and Siponen (2010) provided some indirect evidence in support of these arguments. Thus, we posit that:

> *H7a: Stronger perceived top management participation in information security initiatives leads to stronger perceived goal orientation culture in the organization.*

> *H7b: Stronger perceived top management participation in information security initiatives leads to stronger perceived rule orientation culture in the organization.*

These research hypotheses are summarized in Figure 2. Prior research on behavioral and organizational studies suggests that a number of additional factors should be included as control variables because of their potential influence on the dependent variable of behavioral intention. In this study, we included job type, education, work experience, and dutifulness as control variables. While the first three are straightforward, the inclusion of dutifulness deserves a brief explanation. Dutifulness is a facet of "conscientiousness" - one of five factors in the five-factor-model (FFM) of personality (Costa & McCrae, 1995). Research in a variety of fields has shown significant relationships between conscientiousness and measures of compliance with rules, policies, or norms (Christensen & Smith, 1995; Stilley, Sereika, Muldoon, Ryna, & Dunbar-Jacob, 2004; Mount, Oh, & Burns, 2008). For example, conscientiousness was significantly correlated with rule compliance in Mount et al. (2008), and with adherence to a medication regimen in Stilley et al. (2004) and Christensen and Smith (1995). Thus, conscientiousness appears to correlate with measures of conformity behavior. Since our focus is not about personality in this study, we choose the most relevant facet of conscientiousness—dutifulness—as a control variable in the model to minimize its potential confounding effect on the model.

Insert Figure 2 Here

DATA AND ANALYSIS

Survey Development and Data Collection

The survey instrument was developed based on the research model as shown in Figure 2. Measurement items for each construct in the model are based on a 5-point Likert scale. All of the items were adapted from the extant literature in order to maximize the validity and reliability of the measurement model. Table 1 shows the constructs and the primary sources of the measurement items and Table A1 in the Appendix provides the full instrument.

Insert Table 1 Here

Data Collection

Measurement items for the survey instrument were refined through a pilot study using students enrolled in MIS courses at a large public university in the US. Minor changes were made to items that showed low loadings in initial analyses. The final version of the survey was published on a survey Web site. The intention was to distribute the link to potential respondents who were employed full or part time in various organizations. In doing so, we hoped to ensure maximum variance in the constructs. We sent out a total of 1089 emails to the alumni of the MIS and MBA programs of a large public university in the US and invited the recipients to participate in our study with a link to the online survey. Of these, 220 emails were returned as undeliverable by the email servers. From the remaining 869 emails, we received a total of 75 responses. In the course of the following month we performed a second round of requests for responses in an email campaign to the same email recipients. We obtained an additional 79 responses. From both campaigns, six responses were eliminated due to too many missing entries. This yielded a total of 148 responses, resulting in an effective response rate of approximately 17%, consistent with response rates reported in other IS studies. Descriptive statistics were run to reveal the demographic profiles of the respondents, followed by validity and reliability analyses of the instrument. The demographics of the respondents are shown in Table 2. Various industries—aerospace, military, financial, retail, services, education, high-tech, and healthcare—were represented in the study, with organizations ranging from small (3 employees) to very large (75,000 employees). We concluded that the respondents were a heterogeneous group that may approximate a random sample of organizational employees in the target population.

Structural Equation Modeling

To analyze the measurement quality as well as the path model for hypothesis testing, we used SmartPLS (Ringle, Wende, & Will, 2005) as the primary statistical tool. Following the widely adopted two-step approach to structural equation modeling (Anderson & Gerbing 1988; Hulland, 1999), we first assessed the quality of the measurement model to ensure the validity and reliability of the measurements. This was followed by the analysis of the structural model to test the research hypotheses and the overall quality of the proposed model.

------------------------

Insert Table 2 Here

----------------------

Quality of Measurement Model

Assessment of measurement quality is the first critical step in the structural equation modeling analysis. SmartPLS provides a rich set of indicators about reliability and convergent and discriminant validity of the measurement scale. Table 3 shows some of the quality indicators of our measurement model.

------------------------

Insert Table 3 Here

----------------------

The quality of the measurement model is usually assessed in terms of its content validity, construct validity, and reliability (Hulland 1999; Straub, Boudreau, & Gefen, 2004). Content validity is defined as the degree to which the items represent the construct being measured. Content validity is usually assessed by the domain experts and through literature review (Straub et al. 2004). In this case the content validity is primarily assured by adopting the previously published measurement items for the constructs and an item by item review by the research team.

Construct validity can be assessed using convergent validity and discriminant validity. Convergent validity is defined as the degree to which the measurement items are related to the construct they are theoretically predicted to be related. Convergent validity is shown when the t-values of the outer model loadings are statistically significant. Only one item, PGO1 showed low loading and low t-values and was subsequently removed from the model. As it can be seen from Table 3, all remaining item loadings for each construct are significant at $p < 0.01$ ($t > 2.576$), indicating good convergent validity. Hulland (1999) recommends that items with loading below 0.5 be dropped. All item loadings in our final measurement model are greater than this threshold.

Discriminant validity refers to the extent to which measures of the different model constructs are unique. There are a number of techniques that have been used for testing discriminant validity (Straub et al., 2004). In this study we assess the discriminant validity by comparing the correlations between constructs and the square root of the AVE of each construct. This is a widely used technique in the literature when component based methods such as PLS are used. Discriminant validity is supported if the square root of construct AVE is greater than the correlations of the construct with all other constructs (Fornell & Larcker, 1981; Hulland 1999). In our case, the diagonal values in Table 4 are AVEs of constructs, which show good discriminant validity for all constructs in the measurement model. Table 5 shows the cross loading of the items on all latent constructs used in the model, also indicating reasonable discriminant validity.

Insert Table 4 Here

The reliability of the measurement addresses the concern of how well the items for one construct correlate or move together (Straub et al. 2004). Reliability is usually assessed by two indicators: Cronbach’s alpha and composite reliability. Cronbach’s alpha is a measure of internal consistency among all items used for one construct. Composite reliability addresses a similar concept but is considered as a more rigorous reliability measure in the context of structural equation modeling (Raykov, 1998; Chin, 1998). The reliability indicators of the constructs in this study are shown in Table 4. The lowest composite reliability is .862 and the lowest Cronbach's alpha is 0.675, with most higher than the recommended minimum value of 0.7 (Bagozzi & Yi 1988; Gefen, Straub, & Boudreau, 2000), indicating acceptable reliability of the measurement for each construct.

Insert Table 5 Here

Finally, we addressed the threat of common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Straub et al., 2004). Whenever self-reported survey data are used, the threat of common method bias has to be checked to assure that the statistics in the data set are not confounded by respondents' social desirability, leniency, acquiescence, and other social, psychological, and measurement factors (Podsakoff et al., 2003). We reduced the likelihood of bias caused by social desirability or respondent acquiescence by ensuring anonymity to the respondents, assuring them that there were no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study. In addition to the precautions taken in the instrument design and data collection, we also performed two post-hoc tests to check for signs of method bias. First, following Podsakoff et al. (2003), we tested the common method variance using Harman's single-factor test by simultaneously loading all items from the combined dataset in factor analysis with no rotation. A total of 28 factors emerged, with 6 of them accounting for 69% of the total variance, and the largest component accounting for less than 31% of the sample variance, indicating that common method bias is not a significant concern. This result was confirmed when we conducted the second test based the method proposed by Liang et al. (2007) that showed the substantive variances are significantly larger than the method variances. This result is presented in Table A2 in the Appendix

Structural Path Analysis

The primary quality indicators for the structural model in component based PLS techniques are the R^2 values of the endogenous variables (Hulland, 1999) which measure how much of the variances in the endogenous constructs are explained by the exogenous constructs specified in the model. Figure 3 presents the results of the structural analysis using SmartPLS.

Insert Figure 3 Here

The R^2 value for the dependent variable of intention to comply with information security policies and practices is 0.548, indicating that the variables in the model explained about 55% of the variance in the dependent variable, which is high by the standard of structural equation modeling. And it is higher than comparable published studies using a similar dependent variable (e.g., 30% in D'Arcy et al., 2009; 42% in Herath &Rao, 2009a; 47% in Herath & Rao, 2009b; 35% in Bulgurcu et al., 2010; 47% in Siponen & Vance, 2010), with a relatively parsimonious model. The R^2 for the TPB constructs are in the reasonable range of 14%-19%. None of the control variables has a significant effect on the dependent variable. Overall, the structural model demonstrates a good fit to the underlying structure in the data set.

The Role of Individual Cognitive Beliefs

The test results show that the proposed model exhibited high R^2 (0.548) for the dependent variable, indicating strong explanatory power of the model. Indeed, only 5 out of the 16 hypotheses were not supported by the data, and most of the core hypotheses were strongly supported at level $p < .01$. Not surprisingly, the research hypotheses based on TPB (H1a, H1b, and H1c) are all strongly supported by the data at the $p < .01$ level, which once again confirms the resilience and reliability of the TPB in predicting individual behavior in various social and organizational contexts.

Interestingly, among the three determinants of compliance intention, attitudes show the smallest effect, with regression coefficient $\beta = .197$, on the intentions. In comparison, subjective norm is relatively strong, with regression coefficient $\beta = .366$, and perceived behavioral control is also strong, with regression coefficient $\beta = .360$. This pattern is consistent with the findings of Bulgurcu et al. (2010). These results indicate that in organizational settings, individual attitudes toward information security may not matter as much as the subjective norm within the organization.

This is in stark contrast with Dinev and Hu (2007) and Pavlou and Fygenson (2006) where the influence of subjective norm is found to be insignificant on individual behavior intentions. The difference may be explained by the different context where subjective norm was measured. The subjective norm in the Dinev and Hu (2007) and Pavlou and Fygenson (2006) studies was about voluntary and proactive behavior and was measured in terms of the influence from an individual's social circle (friends and relatives). In this study, the subjective norm is about compliance behavior in an organization. Since all the questions were framed in the organizational context, the respondents' understanding of "important and influential people that they respect" would be in their professional circles of colleagues, superiors, and subordinates within the organization, resulting in a stronger effect of subjective norm on individual behavioral intentions.

The effect of perceived behavioral control on compliance intention is also strong and consistent with the results of other studies based on the TPB framework (e.g., Dinev & Hu, 2007; Pavlou & Fygenson, 2006; Bulgurcu et al, 2010). Therefore, the more an employee feels in control and the compliance behavior is easy to enact, the more likely he or she will behave in accordance to the security policies. The most effective way to accomplish this is through extensive training, not only on the policies and procedures themselves, but also on the underlying technologies and skills to execute these policies and procedures.

The Role of Organizational Culture

The results indicate that organizational cultural orientations are important antecedents to employees' belief constructs in the context of information security, though with varying degree and significance. The relationship between perceived goal orientation and attitudes (H2a) is supported ($\beta = .193$, $p < .05$), but the relationship between goal orientation and subjective norm (H2b) and perceived behavioral control (H2c) are statistically insignificant. Interestingly, the rule orientation construct has a similar effect: the link between rule orientation and attitudes (H3a) is significant ($\beta = .194$, p

< .05), but the links to subjective norm (H3b) is insignificant, and the link to perceived behavior control (H3c) is only weakly supported (β = .145, p < .10).

Perhaps more interestingly, the two hypotheses directly linking organizational cultural values (PGO and PRO) to employee behavior intention (INT) are not supported. In fact, the path coefficients are virtually zero, a strong indication that cultural values do not have a direct impact on employee behavioral intentions, at least in the context of information security policy compliance. Rather, the effect of organizational culture on employee compliance behavior is fully mediated by cognitive beliefs—primarily attitudes. Since the extant literature on organizational culture and employee behavior usually articulate a direct relationship (e.g., Lund, 1986; Sheridan, 1992; Weaver & Treviño, 1999; Douglas et al., 2001; Tyler & Blader, 2005), our results suggest that the possibility that cognitive beliefs mediate the impact of culture on behavior is significant and deserves more attention in future research.

Since PLS does not offer direct testing of the mediating effect, we followed the Baron and Kenny (1986) procedure, which is by far the most widely used statistical method for testing mediating effect according to MacKinnon, Lockwood, Hoffman, West, and Sheets (2002). In a simple three variable causal model, X→M→Y, to support the mediation hypothesis that M mediates the effect of X on Y, the Baron and Kenny (1986) procedure requires testing three individual regression models: Model 1 to regress the mediator on the independent variable (X→M); Model 2 to regress the dependent variable on the independent variable (X→Y); and Model 3 to regress the dependent variable on both the independent variable and on the mediator (X, M→Y). The mediation hypothesis is supported if the following conditions hold: (i) the independent variable must affect the mediator in the first equation; (ii) the independent variable must be shown to affect the dependent variable in the second equation; and (iii) the mediator must affect the dependent variable in the third equation, and full mediation holds if the independent variable has no effect when the mediator is controlled (Baron & Kenny, 1986). Table 6 shows the regression results based on this procedure.

Insert Table 6 Here

As it can be seen, the results show that all three conditions for mediation are confirmed. In fact, the mediation of cognitive constructs (ATT, SN, and PBC) on the relationship between perceived cultural values (PGO and PRO) and employee behavioral intention (INT) meets the requirement of full mediation. In regression Model 3, when the mediators (ATT, SN, and PBC) are controlled, the independent variables (PGO and PRO) have no effect on the dependent variable (INT). However, we need to point out that Model 2 is weak, and only PRO has a significant impact on INT at the $p < 0.1$ level, indicating the direct effect of perceived cultural values on the behavior intention is not strong to begin with. Given the substantial literature on why organizational culture should affect employee behavior, we suspect that this weakness may be attributed to the measurement of organizational culture values rather than to substantive theoretical factors. Future research is required to gain a better understanding of this result, preferably with much larger sample size and refined measurement of organizational cultural values and employee intentions.

The Role of Top Management

The critical role of top management in information security cannot be over emphasized. Our results show that top management can significantly affect organizational culture as well as employee salient beliefs with regard to information security policies and procedures. Perceived top management participation (PMP) is fundamental to our theory. PMP strongly impacts subjective norm (H6b: $\beta = .289$, $p < .01$) and perceived behavior control (H6c: $\beta = .333$, $p < .01$), but interestingly, does not impact attitude (H6a: $\beta = .075$, $p > .10$). Since subjective norm and perceived behavioral control have the strongest influence on employee compliance intention, this result suggests that top management can have a significant impact on employee compliance behavior, supporting the main thesis of our study.

Moreover, another main thesis of this study—that top management can influence organizational culture—is also strongly supported by the data. The relationship between top management participation and goal orientation (H7a: $\beta = .291$, $p < .01$) and rule orientation (H7b: $\beta = .279$, $p < .01$) are both strong and statistically significant. Therefore, top management can influence the values, norms, and shared beliefs in their organization with regard to information security policies and procedures by actively participating in information security related initiatives, programs, and establishing and enforcing information security policies.

An interesting question could be raised here: Can top management participation directly influence employee compliance behavior? Though we did not hypothesize such a direct relationship, we found no explicit tests in the literature to determine whether the three mechanisms of top management participation (legitimacy, commitment, and fairness) discussed in the literature review section could have a direct influence on employee behavior. To answer this question, we conducted another mediation test using the Baron and Kenny (1986) procedure, as described in the previous section. The results are shown in Table 7.

Insert Table 7 Here

As it can be seen, full mediation of the influence of top management participation on employee compliance intention by the constructs of TPB (attitudes, subjective norm, and perceived behavioral control) is confirmed. While the direct regression of PMP on INT is significant (Model 2), when controlled for ATT, SN, and PBC (Model 3), PMP has no significant effect on INT, yet the influences of ATT, SN, and PBC on INT are all significant at the $p < 0.01$ level, a clear indication of full mediation. This was further confirmed when we tested a direct link between top management participation and employee compliance intention in addition to all other relationships depicted in the research model using SmartPLS, and found that this link is not only weak and insignificant (β=.048, t=.781, p>0.1) but also does not add much to the overall variance explained in INT (R^2 increased from .548 to .550).

The Total Effect of Constructs

Another interesting set of statistics provided by SmartPLS is the total effect of the exogenous variables on the endogenous variables in the model. The total effect reflects the cumulative influence of one construct on the other in the structural model. Table 8 shows the total effects of the constructs in the model, ordered by the magnitude of the effect, and grouped by the endogenous variables. It provides another perspective to see the causal effect of individual constructs on the focal variable of interest. For example, if our focus is to see which of the latent constructs has the most impact on the employee compliance intention (INT), we can see that the top three constructs are perceived behavioral control (PBC) (β=0.368), subjective norm (SN) (β=0.361), and perceived top management participation (PMP) (β=0.293). Similarly, we can see that while employee attitude can be influenced by both cultural values and top management participation, top management participation is the only significant source of influence in the model on subjective norm and perceived behavioral control.

Insert Table 8 Here

DISCUSSION

Some interesting relationships emerged from the empirical results. While the overall thesis of the study is supported by the empirical evidence, the significance and insignificance of individual hypotheses deserve further discussion. At the top of this list are the relationships between the perceived top management participation and employee attitude, subjective norm, and perceived behavioral control over compliance with information security policies. Although the other two relationships are supported as expected, the relationship between perceived top management participation and employee attitude is not statistically significant. In fact, the magnitude of the coefficient is very small (0.075) relative to the other two (0.285 and 0.333). The insignificant relationship may be explained by the relative hierarchical distance between the top management and the employees. Indeed, based on the attitude persuasion literature (Angst & Agarwal, 2009), common methods of affecting attitudes include direct psychological mechanisms such as appropriate message imparting to the recipients, convincing, personal persuasion with argument framing and issue involvement, and effectively conveying passion and beliefs. Thus, attitude is more likely to be affected by more personal and direct communications as compared to subjective norms and perceived behavioral control. This may be more realistic in smaller organizations than in larger ones. In fact, Puhakainen and Siponen (2010) noted that their observation that top management participation has a direct impact on employee compliance behavior contradicted the argument by Wylder (2003) that top management commitment to security policy has no bearing on ordinary employees' attitudes and commitment toward security policy since top management is more removed from day-to-day activities. Similarly, Liu, Feng, Hu, and Huang (2011) also found that in large organizations employees' attitudes toward using and learning ERP systems are more influenced by their peers and immediate supervisors than by more removed top executives. However, we should not conclude that top management participation does not directly influence employee attitudes toward information security policy compliance regardless of organizational sizes, structure, culture, and leadership styles. Future studies are clearly needed to further investigate this important relationship with varying organizational sizes, structures, culture, and leadership styles.

On the other hand, our results show that organizational culture, specifically the perceived goal orientation and perceived rule orientation values, does have a significant effect on employee attitudes, and that perceived top management participation strongly influences the perceived cultural values. Therefore, the data suggest that the impact of top management on employee attitude is mediated by organizational culture, consistent with the established literature on culture and leadership (Schein, 2004). This indirect effect on attitudes may be explained by the "trickle down" effect of the top management’s visions and actions. Their visions and actions permeate the organization, define and modify the organizational culture, and influence the employee beliefs and actions. After all, employees care about how they are evaluated in relation to the attainment of goals, objectives, and compliance with policies in an organization with a culture of strong goal and rule orientations.

We, however, do not have an adequate explanation as to why cultural orientations do not affect the employees’ subjective norm while perceived top management participation does. This may have something to do with how the subjective norm is defined and measured. In this study, like in many studies based on the TPB framework, the subjective norm primarily measures how strongly an individual perceives the influence by significant members in his or her social or professional circles. While culture may strongly affect attitudes and beliefs of individual members in the organization, it may not necessarily impact how an employee perceives the influence from his or her peers, supervisors, and subordinates. Top management can be considered as members of the influential social or professional circle and thus have a strong and direct influence on the subjective norm of the employees. The insignificance of goal orientation on perceived behavioral control raises interesting questions. It suggests that the desire for accomplishment, accountability, and contingent awards does not necessarily lead to perceived self-efficacy toward compliance. Other factors, such as resources and training, have to be in place as well. Evidently, further theoretical and empirical research is needed to address and test these important relationships.

Finally, the insignificance of the relationships between the two perceived cultural values and the employee compliance behavioral intention is intriguing but not surprising. While culture provides a normative framework for interpretation and sense-making and a general approach to problem solving for employees in organizational settings, strong organizational culture alone is not enough to change individual behavior toward specific policies or programs such as information security compliance. Our results clearly suggest that the effect of organizational culture, perhaps culture in general, on individual behavior is fully mediated by the internal cognitive processes of the individuals regarding specific tasks and contexts. This is consistent with Harris' (1994) theoretical argument that individuals formulate their responses to organizational stimuli based on internal mental schemas—cognitive structures in which an individual's knowledge is retained and organized. What organizational culture does, Harris argued, is to influence the saliency and activation of specific schemas from which individual responses are formulated, rather than the responses themselves. In addition, organizational culture has the function of making an individual's schemas resemble those of other organizational members, thus inducing similar responses from these members to the same organizational stimuli. This significant mediation function of internal cognition seems to have been overlooked in most organizational culture studies.

While not the focus of this study, one interesting observation is that the personality facet, dutifulness, as a control variable, is found to have a significantly positive impact on the intention to comply with information security polices ($\beta = .161$, $p < .05$). The path coefficient is of a similar magnitude to those of the organizational culture values, a strong indication that personality could play a significant role in shaping the compliance behavior. This is consistent with the normative literature on personality research, but is a factor that has not attracted much attention and has not been fully investigated in the information security research literature.

Contributions to Theory

Our research findings offer important theoretical contributions to information security research and management in organizational settings. First, this study is the only research on information security we are aware of that integrates three major theoretical frameworks about individual behavior in an organizational setting—top management, organizational culture, and theory of planned behavior—into one theoretical model. Our proposed theoretical model highlights the critical role that top management can play in managing information security and refines our understanding of the specific mechanisms via which top management and organizational culture work together in shaping employee attitudes, subjective norms, and perceived behavioral control over compliance with information security policies. Our model shows how top management, organizational culture, and employee cognitive beliefs are linked together on the nomological net of the theory of planned behavior, extending the individually grounded theory to the organizational context via links to the perceived organizational antecedents.

Second, to the best of our knowledge, this is the first study that has empirically shown that the effect of organizational culture on employee behavioral intention is fully mediated by the employee's internal cognition of the context specific behavior such as compliance with information security policies. That is, culture may alter the internal cognitive schema and variables, but does not directly lead to behavioral intention or actual behavior. While this logic has been theoretically argued in the literature (Harris, 1994), the majority of the empirical organizational culture studies tends to link cultural values directly to the focal behavioral variables. With this empirical evidence, we have refined our understanding of how culture works in organizational settings in terms of its impact on employee behavior. We call for explicit consideration of the mediation effect in future studies that connect organizational culture or culture in general, to individual behavior in broader organizational and social contexts.

Third, our results suggest a complementary relationship between top management and organizational culture in shaping employee compliance intention to information security policies. When top management participation fails to change the employees' attitudes towards information security compliance, the goal oriented cultural value is effective in that aspect. On the other hand, when both cultural values fail to influence the subjective norm about compliance with policies, top management participation comes to the rescue with its strong impact on this variable. Therefore, when top management and organizational culture work in tandem, better information security compliance can be reached in the organization. Interestingly, specific cultural values seem to affect only specific salient beliefs, that is, perceived goal orientation is effective only toward employees' attitudes, and perceived rule orientation is effective only toward employees' attitudes and perceived behavioral control. Without visible and active top management participation, organizational culture alone will not be effective in fostering employee compliance with information security policies. On the other hand, the impact of top management participation on employee compliance intention is partially mediated by organizational culture, and fully mediated by the individual cognitive process.

Last but not least, while the current mainstream literature on information security has put strong emphasis on individual cognitive processes (e.g., Boss et al., 2009; Bulgurcu et al., 2010; Johnston & Warkentin, 2010; Siponen & Vance, 2010; Hu et al., 2011), this study calls for attention to how organizational level factors influence the cognitive processes, thus complementing the extant literature by expanding the horizon for research and developing better theories. For instance, Bulgurcu et al. (2010) suggest that the individual awareness of information security policies and information security in general drive individual perceptions about the outcomes of compliance, which lead to individual assessments about the cost and benefits of compliance, which in turn leads to individual compliance intentions. However, it is not clear how such individual awareness can be acquired or enhanced in organizational settings. Siponen and Vance (2010) demonstrate that various neutralization mechanisms in individual cognitive processes, such as defense of necessity, denial of injury, appeal to higher loyalties, condemn the condemner, metaphor of the ledger, and denial of responsibility, lead to non-compliance intentions. But top management participation and strong rule and goal oriented organizational culture could neutralize some of the neutralizers identified. Johnston and Warkentin (2010) advocate constructing and communicating fear-inducing messages to strengthen individuals' response efficacy and self-efficacy to information security policy compliance. Yet, it is not clear how effectively fear appeals can work in organizations where top management actions are invisible and rules are routinely ignored. Therefore, a major contribution of this study is to reintroduce the two important organizational factors, top management and organizational culture, as perceived at the individual level, into the individual behavior centric empirical information security research and call for better integration of behavioral theories from different perspectives and inclusion of salient factors from different levels in the organization ecosystem.

Implications for Practice

Our findings also have important implications for information security management practices. First, not only it is shown that top management can make a difference with respect to security compliance behavior, the results also suggest that top management participation is the most important external factor among the constructs and variables included in the model that shapes employee behavior toward information security policy compliance, as it is clearly demonstrated in the total effect table. Similar findings have also been reported in Puhakainen and Siponen (2010). This is not a trivial argument to make. In some organizations, especially those for which IT is not their core business, top management often delegates decisions and responsibilities related to information security to lower level IT managers, with the belief that they have the best IT staff in their company to ensure the highest level of information security (Hu et al., 2007). What we found in this study calls for active and visible involvement of top management because it not only changes the relevant culture of the organization but also directly influence the cognitive beliefs of employees which then influence their compliance intentions.

Second, the significant influences of rule and goal oriented culture on employees' cognitive beliefs about information security offer another important opportunity for information security management practices. While prior studies have shown that deterrence factors may not be very effective in altering employee compliance behavior (Siponen & Vance, 2010; Hu et al., 2011), our results suggest that building an organizational culture, where goals are clearly articulated, rules and policies are well established and respected, employees are evaluated based on the attainment of goals and compliance with rules and policies, rule-abiding behaviors are rewarded, and rule-breaking behaviors are punished, will have a positive impact on employee intention and behavior toward compliance with information security policies.

Third, equally important is the role of top management in shaping organizational cultural values. Our results show that the perceived top management participation has direct and significant impact on the organizational culture of rule orientation and goal orientation. This result suggests that top management should be actively and visibly involved in the establishment, implementation, and enforcement of organizational information security policies and rules, perhaps by taking full advantage of the six embedding mechanisms identified by Schein (2004) and discussed in the hypothesis development section. Not only can visible and active participation have direct impact on employee cognitive beliefs, subjective norm in particular, it can also impact these beliefs indirectly via cultural values.

Fourth, our analyses and results suggest to managers that while it is certainly important to have information security training programs and to implement comprehensive information security policies, they are not enough and likely inadequate, as the security breach incidents reported in the media have demonstrated repeatedly. Given the finding that employee cognitive processes fully mediate the influences of top management participation and organizational culture, instituting programs that target the minds of the employees, focusing on how to change employees' attitudes, subjective norm, and perceive behavioral control over compliance, not only can be an important complement to the existing information security programs, but it is likely a necessary and more effective component to any comprehensive information security management program. Information security management initiatives, such as training programs that are designed based on such theoretical understanding, as shown in Puhakainen and Siponen (2010), are more likely to be effective than generic training programs on information security technology or policies.

Finally, this study and the numerous studies published in the past on information security have clearly shown that managing information security policy compliance in organizations is a complex task that requires comprehensive approaches. Any information security programs and initiatives that only emphasize certain aspects of the complex phenomenon are not likely to be effective. Higher levels of information security will demand higher degrees of comprehensive information security programs, including top management champions; information policy awareness education; constructing and communicating effective messages related to compliance; designing training programs based on learning theories; certain, severe, and swift deterrence against non-compliance; and building and fostering a strong rule and goal oriented organizational culture.

Limitations and Future Research

Our study inevitably has its limitations. For example, organizational culture is a multi-dimensional and complex concept (Denison, 1996), therefore selecting any one cultural value framework imposes certain limitations to what is included. We chose the Quinn (1988) competing value framework and the Van Muijen et al. (1999) operationalization because we believed those to be the most salient in the context of information security. However, given some of the inconclusive findings about the influence of culture on subjective norm and perceived behavioral control, using other schemes and operationalizations of organizational culture in future studies may shed some light on this important issue. When considering the role of top management, the nature and effectiveness of communication from top management to employees was not examined. An interesting path for future investigation would be testing the effectiveness of different styles and channels of communication utilized by top management in shaping employee beliefs and organizational culture and ultimately changing the level of compliance toward information security policies and procedures. Third, top management participation was measured in terms of employee perception. As we have noted before, the structural and physical distances between top management and employees may distort this measurement to an unknown degree, depending on the unique characteristics of each organization. It is entirely possible that in some organizations, especially large ones, active top management participation in information security initiatives may not be visible to lower level employees, thus may not be reflected in the variance of survey data analysis. Future studies could either group the data based on the size of the organizations or use multilevel analysis in which organizational level data (e.g., top management participation, organizational culture values, and organization structure) and individual level data (attitude, subjective norm, and perceived behavioral control) can be collected and tested with multilevel statistical tools. Finally, we would like to point out that not all of our respondents are strictly employees without management responsibility. A series of ANOVA tests were conducted to compare the responses of those who selected themselves as "employees" and the responses of those who selected one of the management titles on each and every construct used in the model. The results show that there is no statistical difference between these two groups. We also run a MANOVA test and got a similar result. Still, the mixing of two groups can cause some concerns about lost information. While the current sample size precluded us from testing the group effect on the relationships, future research could test the group differences with larger samples, which might reveal some interesting insight not shown in this study.

CONCLUSIONS

In this study, we developed an employee compliance model in the context of information security by integrating three well established frameworks relevant to employee behavior: top management, organizational culture, and the theory of planned behavior. We explicitly considered and tested the mediating effects of organizational culture on the influence of top management, and the mediating effects of individual cognitive process (as defined in the theory of planned behavior) on the influence of both top management and organizational culture. Using survey data and structural equation modeling, we tested the hypotheses on how top management participation could influence individual perceived organizational culture values and individual salient beliefs toward compliance with information security policies. The hypothesized relationships are generally supported by the data. We confirmed that the established behavioral determinants—attitudes, subjective norm, and perceived behavioral control—indeed significantly influence an individual's behavioral intention toward compliance with information security policies. More importantly, we showed how top management can influence employee behavior through active participation in information security related initiatives and through building rule and goal oriented organizational cultures. Moreover, our model suggests that the influences of organizational culture and top management participation on employee compliance behavior are complementary to each other and fully mediated by employee cognitive beliefs toward context specific behavior.

This study complements a long stream of research on individual information security compliance behavior and research on organizational information security based social, organizational, and criminological theories by including top management and organizational culture in the collection of significant factors in organizational settings. We believe that a higher level of information security can be achieved only if strong information security technology is implemented with comprehensive information security programs that are based on sound understanding of how organizational, cultural, and individual cognitive factors work together in shaping individual behavioral intentions and actual behavior. However, as the results suggest, there is still much to be learned about the complex inter-relationships among leadership, organizational culture, and employee cognitive process in the context of information security policy compliance. We hope this study will inspire a new stream of research that examines and tests the effectiveness of balanced and comprehensive information security management programs and theories.

REFERENCES

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

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339-370.

Ajzen, I. (2005) *Attitudes, personality, and behavior (2nd Edition)*. New York, NY: Open University Press.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289.

Armstrong, C., & Sambamurthy, V. (1999). Information technology assimilation in firms: The influence of senior leadership and IT infrastructures. *Information Systems Research, 10*(4), 304-327.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Baron, R.M., & Kenny, D.A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Bass, B. M. (1998). *Transformational leadership: Industrial, military, and educational impact.* Mahwah, NJ: Lawrence Erlbaum.

Bass, B. M., & Avolio, B. J. (1993). Transformational leadership and organizational culture. *Public Administration Quarterly*, *17*(1), 112–121.

Björck, F. (2004). Institutional theory: A new perspective for research into IS/IT security. *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37)*, Big Island, HI, USA: IEEE Computer Society, Los Alamitos, CA.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151-164.

Buenger, V., Daft, R. L., Conlon, E. J., & Austin, J. (1996). Competing values in organizations: Contextual influences and structural consequences. *Organization Science*, *7*(5), 557-576.

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

Button, S. B., Mathieu, J. E., & Zajac, D. M. (1996). Goal orientation in organizational research: A conceptual and empirical foundation. *Organizational Behavior and Human Decision Processes*, *67*(1), 26-48.

Cameron, K. S., & Quinn, R. E. (2005). *Diagnosing and changing organizational culture*. San Francisco, CA: Jossey-Bass.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research*. Hillsdale, NJ: Lawrence Erlbaum Associates, 295-336.

Christensen, A. J., & Smith, T. W. (1995). Personality and patient adherence: Correlated of the five-factor model in renal analysis. *Journal of Behavioral Medicine, 18*(3), 305-313.

Colquitt, J. A., & Simmering, M. J. (1998). Conscientiousness, goal orientation, and motivation to learn during the learning process: A longitudinal study. *Journal of Applied Psychology, 83*(4), 654-665.

Costa Jr., P., & McCrae, R. (1995). Domains and facets: Hierarchical personality assessment using the revised NEO personality inventory. *Journal of Personality Assessment*, *64*(1), 21-50.

D'Arcy, J., Havav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Denison, D. R. (1996). What is the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. *The Academy of Management Review*, *21*(3), 619-654.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intentions towards preventive technologies in the context of voluntary use. *Journal of the AIS, 8*(7), 386-408.

Douglas, P. C., Davidson, R. A., & Schwartz, B. N. (2001). The effect of organizational culture and ethical orientation on accountants' ethical judgments. *Journal of Business Ethics*, *34*(2), 101-121.

Dweck, C. S. (1986). Motivational processes affecting learning. *American Psychologist*, *41*(10), 1040-1048.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Gefen, D., Straub, D. W., & Boudreau, M.C. (2000). Structural equation modeling and regression: Guidelines for research practice. C*ommunications of the AIS*, *4*1,1-78

Harris, S. G. (1994). Organizational culture and individual sensemaking: A schema-based perspective. *Organization Science, 5*(3), 309-321.

Harrison, D. A., Mykytyn, P. P., & Riemenschneider, C. K. (1997). Executive decisions about adoption of information technology in small business: Theory and empirical tests. *Information Systems Research, 8*(2), 171-195.

Hartog, D. N. D., Muijen, J. J. V., & Koopman, P. L. (1996). Linking transformational leadership and organizational culture. *Journal of Leadership & Organizational Studies, 3*(4), 68-83.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

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

Heyman, G. D., & Dweck, C. S. (1992). Achievement goals and intrinsic motivation: Their relation and their role in adaptive motivation. *Motivation and Emotion*, *16*(3), 231-247.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative Science Quarterly*, *35*(2), 286-316.

Holmes, A. (2008). Malicious thumb drives in justice, accessed June 2, 2010, available at http://techinsider.nextgov.com/2008/08/malicious_thumb_drives_in_just.php.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external influences on organizational information security practices: An institutional perspective. *Journal of Strategic Information Systems*, *16*(2), 153-172.

Hu. Q., Xu, Z. C., Dinev, T., & Ling, H. (2011). Does deterrence really work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 34-40.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal*, *20*(2), 195–204.

Iivari, J., & Huisman, M. (2007). The relationship between organizational culture and the deployment of systems development methodologies. *MIS Quarterly*, *31*(1), 35-58.

James, H. S. (2000). Reinforcing ethical decision making through organizational structure. *Journal of Business Ethics*, *28*(1), 43-58.

Jarvenpaa, S. L. & Ives, B. (1991). Executive involvement and participation in management information technology. *MIS Quarterly*, *15*(2), 205-227.

Jaskyte, K. (2004). Transformational leadership, organizational culture, and innovativeness in nonprofit organizations. *Nonprofit Management & Leadership*, *15*(2), 153-168.

Johnston, A.C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *33*(4), 549-566.

Jones, R. A., Jimmieson, N. L., & Griffiths, A. (2005). The impact of organizational culture and reshaping capabilities on change implementation success: The mediating role of readiness for change. *Journal of Management Studies*, *42*(2), 361-386.

Ke, W., & Wei, K. K. (2008). Organizational culture and leadership in ERP implementation. *Decision Support Systems*, *45*(2), 208-218.

Kouzes, J.M., & Posner, B. Z. (1987). *The leadership challenge: How to get extraordinary things done in organizations*. San Francisco, CA: Jossey-Bass.

Leidner, D. E., & Kayworth, T. (2006). Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly*, *30*(2), 357-399.

Liang, H., Saraf, H., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59-87.

Lin, S.-C., & Chang, J.-N. (2005). Goal orientation and organizational commitment as explanatory factors of employees' mobility. *Personnel Review*, *34*(3), 331-353.

Liu, L. N., Feng, Y. Q., Hu, Q., & Huang, X. J. (2011). From transactional user to VIP: How organizational and cognitive factors affect ERP assimilation at individual level. *European Journal of Information Systems*, *20*(2), 186-200.

Lund, D. B. (1986). Organizational culture and job satisfaction. *Journal of Business & Industrial Marketing*, *18*(3), 219-236.

MacKinnon, D. P., Lockwood, C. M., Hoffman, J. M., West, S. G., & Sheets, V. (2002). A comparison of methods to test mediation and other intervening variable effects. *Psychological Methods*, *7*(1), 83-104.

Markoff, J. (2010). Cyberattack on Google said to hit password system, *New York Times*, April 20, p. A1.

Mills, E. (2010). IBM: We distributed malware-ridden USB drives, accessed June 2, 2010, available at http://news.cnet.com/security/?keyword=USB.

Mount, M. K., Oh, I., & Burns, M. (2008). Incremental validity of perceptual speed and accuracy over general mental ability. *Personnel Psychology*, *61*(1), 113-139.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Ouchi, W. G., & Wilkins, A. L. (1985). Organizational culture. *Annual Review of Sociology*, *11*, 457-483.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1), 115-143.

Payne, S. C., Youngcourt, S. S., & Beaubien, J. M. (2007). A meta-analytic examination of the goal orientation nomological net. *Journal of Applied Psychology*, *92*(1), 128-150.

Podsakoff, P. M., MacKenzie, S. B., Lee, J-Y., & Podsakoff, N.P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757-778.

Quinn, R.E. (1988). *Beyond Rational Management*. San Francisco, CA: Jossey-Bass.

Quinn, R. E., & Rohrbaugh, J. (1983). A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. *Management Science*, *29*(3), 363-377.

Quinn, R. E., & Spreitzer, G. M. (1991). The psychometrics of the competing values culture instrument and an analysis of the impact of organization culture on quality of life. In W. A. Pasmore, & R. W. Woodman (Eds.), Research in Organizational Change and Development, Volume 5. Greenwich, CT: JAI Press Inc., 115-142.

Raykov, T. (1998). Coefficient alpha and composite reliability with interrelated nonhomogeneous items. *Applied Psychological Measurement*, *22*(4), 375-385.

Richardson, R. (2008). CSI computer crime and security survey, accessed March 31, 2010, available at http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf.

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS, 2.0 (beta), University of Hamburg, Hamburg, Germany, accessed March 7, 2012, available at http://www.smartpls.de.

Schein, E. (2004). *Organizational culture and leadership*. (3rd ed.) San Francisco, CA: Jossey-Bass.

Schrodt, P. (2002). The relationship between organizational identification and organizational culture: Employee perceptions of culture and identification in a retail sales organization. *Communication Studies*, *53*(2), 189-202.

Sharma, R., & Yetton, P. (2003). The contingent effects of management support and task interdependence on successful information systems implementation. *MIS Quarterly*, *27*(4), 533-555.

Sheridan, J. E. (1992). Organizational culture and employee retention. *Academy of Management Journal*, *35*(5), 1036-1056.

Siponen, M., & Vance, A.O. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 87-502.

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, *28*(3), 339-358.

Smith, S., Winchester, D. W., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, *34*(3), 463-486.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, *30*(3), 679-704.

Stilley, C. S., Sereika, S., Muldoon, M. F., Ryan, C. M., & Dunbar-Jacob, J. (2004). Psychological and cognitive function: Predictors of adherence with cholesterol lowering treatment. *Annals of Behavioral Medicine*, *27*(2), 117-124.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. (2009). Your botnet is my botnet: Analysis of a botnet takeover. *Proceedings of the 16th ACM conference on computer and communications security (CCS'09)*, November 9–13, Chicago, Illinois, USA: ACM New York, NY, 635-647.

Straub, D. W. (1990) Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of AIS*, *13*1380-427. .

Symantec and Ponemon (2009). More than half of ex-employees admit to stealing company data according to new study. Press release by Symantec Corporation and Ponemon Institute, accessed March 7, 2012, available at http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144-176.

Trice, H. M., & Beyer, J. M. (1993). *The Culture of Work Organizations*. Englewood Cliff, NJ: Prentice Hall.

Tsui, A. S., Zhang, Z.-X., Wang, H., Xin, K. R., & Wu, J. B. (2006). Unpacking the relationship between CEO leadership behavior and organizational culture. *The Leadership Quarterly*, *17*(2), 113-137.

Tyler, T. R. & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143-1158.

Tyler, T. R., Callahan, P. E., & Frost, J. (2007). Armed, and dangerous (?): Motivating rule adherence among agents of social control. *Law & Society Review*, *41*(2), 457-492.

Van Kessel, P. (2008). Moving beyond compliance – Ernst & Yong 2008 global information security survey. Full report available by request at http://www.ey.com,

Van Muijen, J. J., Koopman, P., De Witte, K., De Cock, G., Susanj, Z., Lemoine, C., Bourantas, D., Papalexandris, N., Branyicski, I., Spaltro, E., Jesuino, J., Neves, J. G. D., Pitariu, H., Konrad, E., Peiró, J., González-Romá, V., & Turnipseed, D. (1999). Organizational culture: The focus questionnaire. *European Journal of Work and Organizational Psychology*, *8*(4), 551–568.

Vandenberghe, C., & Peiro, J. M. (1999). Organizational and individual values: Their main and combined effects on work attitudes and perceptions. *European Journal of Work & Organizational Psychology*, *8*(4), 569-581.

Von Solms, R., & Von Solms, B. (2004a). From policies to culture. *Computers & Security*, *23*(4), 275-279.

Von Solms, B., & Von Solms, R. (2004b). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Weaver, G. R., & Treviño, L. K. (1999). Compliance and values oriented ethics programs: Influences on employees' attitudes and behavior. *Business Ethics Quarterly*, *9*(2), 315-335.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403–414.

Wylder, J. O. (2003). Improving security from the ground up. *Information Systems Security*, *11*(6), 29-38.

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the AIS*, *26*, Article 13, 245-266.

APPENDIX

Table A1: Survey instrument**.**

Please indicate the extent to which you agree with the following statements: 1-Strongly Disagree 3-Neutral 5-Strongly Agree		
PMP	PMP1	Senior managers of our company have articulated a clear vision about information security.
	PMP2	Senior managers of our company have formulated a clear strategy for achieving a high degree of information security.
	PMP3	Senior managers of our company have established clear goals and objectives for achieving a high degree of information security.
ATT	ATT1	I believe that it is beneficial for an organization to establish clear information security policies, practices, and technologies.
	ATT2	I believe that it is useful to for an organization to enforce its information security policies, practices, and technologies.
	ATT3	I believe that it is a good idea for an organization to establish clear information security policies, practices, and technologies.
SN	SN1	People who are influential to me would think that I should follow the policies and procedures and use the security technologies.
	SN2	People who are important to me would think that I should follow the policies and procedures and use the security technologies.
	SN3	People whom I respect would think that I should follow the policies and procedures and use the security technologies.
PBC	PBC1	I am able to follow the policies and procedures and use the security technologies.
	PBC2	I have the resources and knowledge to follow the policies and procedures and use the security technologies.
	PBC3	I have adequate training and skills to follow the policies and procedures and use the security technologies.
INT	INT1	I intend to follow the information security policies and practices at work.
	INT2	I intend to use the information security technologies at work.
	INT3	I intend to use common sense on good information security practices at work.
DUT	DUT1	I try to perform all the tasks assigned to me conscientiously.
	DUT5	When I make a commitment, I can always be counted on to follow through.
	DUT7	I try to do jobs carefully, so they won't have to be done again.
Please answer the question based on your observation of the whole company: How often …. 1- Never 3 - Often 5- Always		
PRO	PRO1	Are instructions written down?
	PRO2	Are jobs performed according to defined procedures?
	PRO3	Do the management follow the rules themselves?
PGO	PGO1	Is competitiveness in relation to other companies measured?*
	PGO2	Do management specify the targets to be attained?
	PGO3	Is it clear how performance will be evaluated?

*Dropped from final data set due to low loading.

Testing for Common Method Bias

We conducted the test for common method bias following the approach as described in Liang et al. (2007). With this method, common method bias can be detected if: (i) an indicator's method factor loading (R2) is statistically significant; and (ii) an indicator's method variance ($R2^2$) is substantially greater than its substantive variance ($R1^2$). The results are shown in Table A2. We have a mixed result: while a large number of indicators' method factor loadings (R2) are significant, these indicators' method variances ($R2^2$, average = 0.511) are substantially smaller than their substantive variances ($R1^2$, average = 0.859). On the other hand, all t-values for the substantive variance R1 (average = 23.64) are significantly higher than the t-values for the method variance R2 (average = 5.57). Thus, coupled with the result of the Harmon one factor test, we conclude that the data may contain a small level of common method bias, but not to an extent that threatens the integrity of the statistical results.

Table A2: Common method bias indicators.

Construct	**Item**	**Substantive Factor Loading (R1)**	**R1^2**	**t-value**	**Method Factor Loading (R2)**	**R2^2**	**t-value**
ATT	ATT1	0.884	0.781	24.977	0.307	0.094	1.938
	ATT 2	0.856	0.733	23.816	0.356	0.127	2.716
	ATT 3	0.854	0.729	21.881	0.415	0.172	3.132
INT	BI1	0.854	0.729	19.545	0.438	0.192	3.524
	BI2	0.866	0.749	21.632	0.492	0.242	4.851
	BI3	0.813	0.661	22.518	0.512	0.262	5.236
DUT	DUT1	0.852	0.725	17.306	0.426	0.181	1.986
	DUT 5	0.834	0.695	11.807	0.298	0.089	1.798
	DUT 7	0.819	0.671	11.056	0.344	0.118	2.723
PGO	PGO2	0.898	0.806	29.445	0.404	0.164	3.364
	PGO 3	0.908	0.825	45.205	0.510	0.260	4.465
PMP	PMP1	0.895	0.801	32.281	0.558	0.312	6.210
	PMP 2	0.938	0.879	53.049	0.601	0.361	8.455
	PMP 3	0.857	0.734	11.413	0.533	0.284	6.188
PBC	PBC1	0.763	0.582	9.566	0.655	0.429	7.904
	PBC 2	0.865	0.748	19.530	0.505	0.255	4.952
	PBC 3	0.863	0.744	27.393	0.649	0.421	8.487
PRO	PRO1	0.834	0.695	24.229	0.486	0.236	4.490
	PRO 2	0.868	0.754	22.862	0.432	0.187	3.509
	PRO 3	0.847	0.718	28.530	0.452	0.204	3.668
SN	SN1	0.831	0.690	12.020	0.539	0.290	5.183
	SN2	0.909	0.826	39.879	0.700	0.489	9.262
	SN3	0.844	0.713	13.403	0.560	0.314	4.396

Average	**0.859**	**0.739**	**23.624**	**0.486**	**0.247**	**4.715**

TABLES AND FIGURES

Figure 1: Conceptual model of individual behavior in organizations.

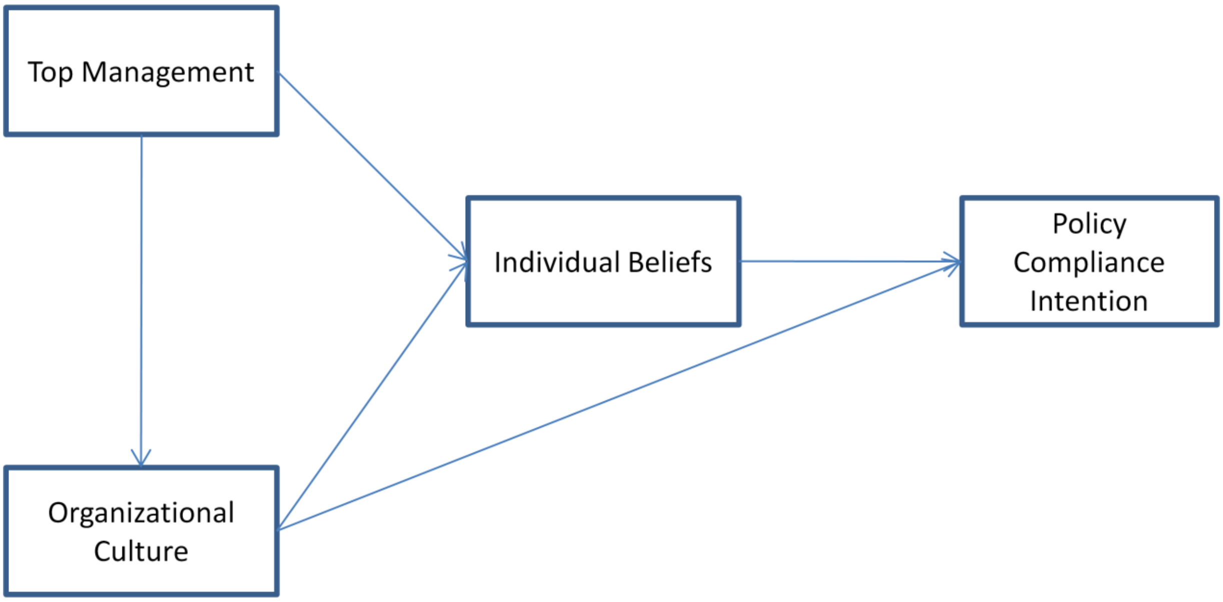


Figure 2: Research model.

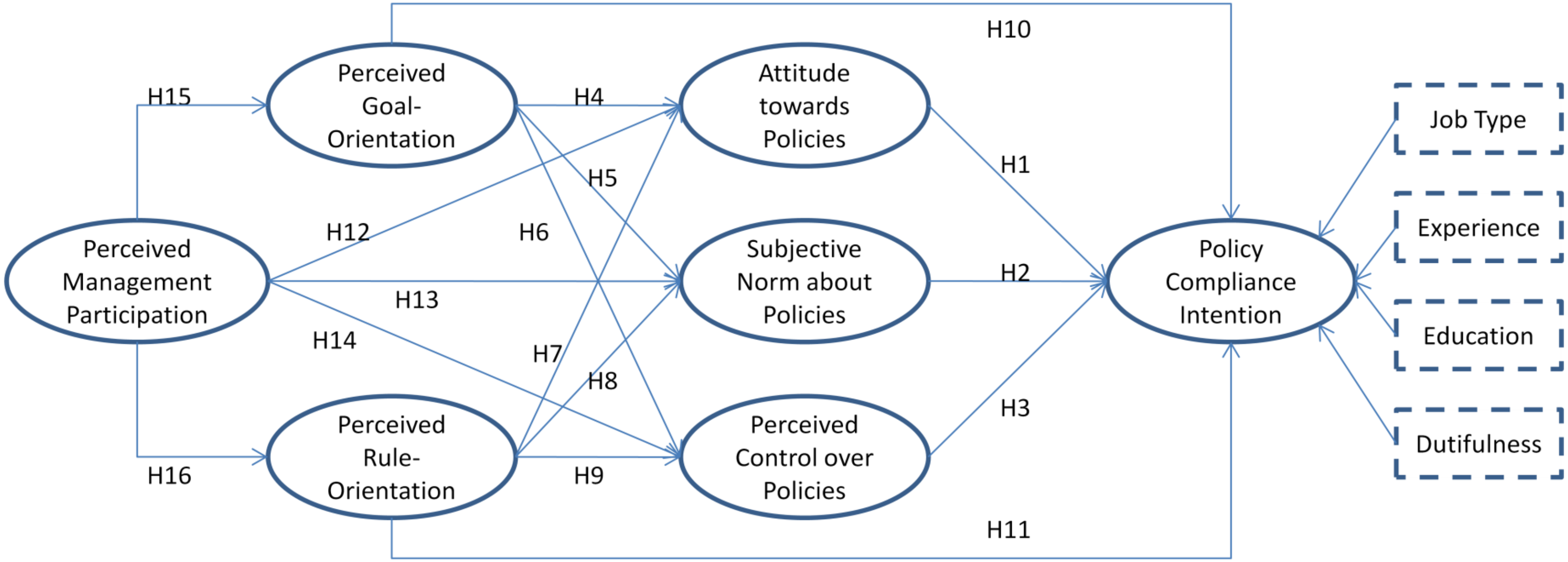
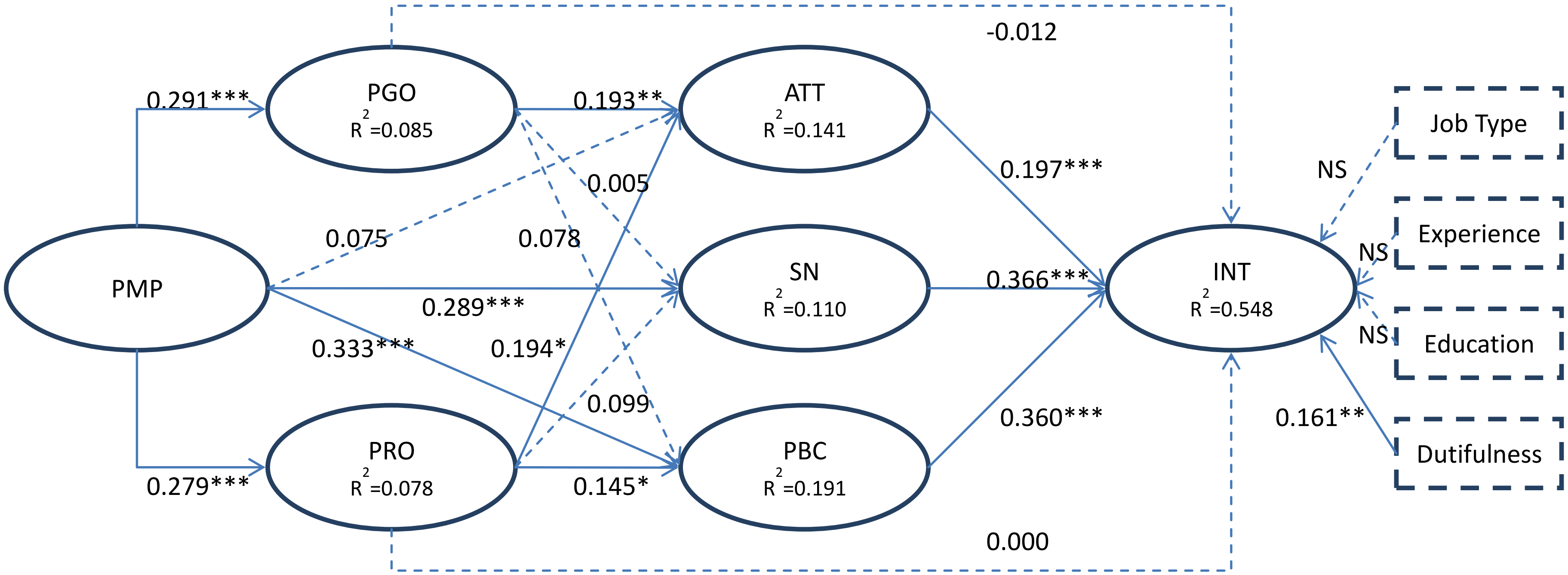

H10
Perceived Goal-Orientation
H15
H4
Attitude towards Policies
Job Type
H5
H1
Experience
H12
H6
Perceived Management Participation
Subjective Norm about Policies
H2
Policy Compliance Intention
H13
Education
H14
H7
H8
H3
Perceived Rule-Orientation
Perceived Control over Policies
Dutifulness
H16
H9
H11

Figure 3: Structural model.



Note: NS indicates statistically non-significant; * - at level p<.05; ** - at level p<.01. Dashed arrows indicate statistically insignificant relationships.

Table 1: Construct operationalization.

Latent Construct	Definition	Primary Sources
Behavioral intention (INT)	Employee's belief that he or she will perform the behavior sometime in the future.	Taylor and Todd (1995); Pavlou and Fygenson (2006)
Attitudes toward behavior (ATT)	Employee's judgment on whether it is good or bad to perform a behavior of interest.	Taylor and Todd (1995); Pavlou and Fygenson (2006)
Perceived subjective norm (SN)	Employee's perceptions of whether the behavior is accepted and encouraged by people who are important to him or her in the organization, such as colleagues, subordinates, or superiors.	Taylor and Todd (1995); Pavlou and Fygenson (2006)
Perceived behavioral control (PBC)	Employee's perceived ease or difficulty of performing a behavior and a personal sense of having the skills and control over performing it.	Taylor and Todd (1995); Pavlou and Fygenson (2006)
Perceived goal orientation (PGO)	Employee's beliefs that his or her performance and appraisal are directly related to attainment of clearly defined goals and objectives by the management.	Van Muijen et al. (1999)
Perceived rule orientation (PRO)	Employee's beliefs that jobs and tasks are performed according to clearly defined and written procedures followed by everybody in the organization.	Van Muijen et al. (1999)
Perceived top management participation (PMP)	Employee's perception of the top managers' behavior and actions in facilitating the organizational actions.	Liang et al. (2007)

Table 2: Respondent profiles.

Category	Sub-Category	Count	Percentage (%)
Sex	Male	96	65%
	Female	52	35%
Age	<30	39	26%
	30-50	96	65%
	>50	12	8%
Education	High School	4	3%
	Undergraduate	78	53%
	Graduate	64	43%
Job Title	Corporate executive	11	7%
	Business manager	22	15%
	IT manager	35	24%
	Employee	80	54%
Job Type	Administrative	26	18%
	Operational	40	27%
	IT	82	55%
Work Experience	<5 years	41	28%

	5-15 years	79	53%
	>15 years	26	18%

Note: Missing data accounts for the differences between sample size of 148 and actual total count in some categories.

Table 3: Measurement quality indicators.

Latent Construct	Item	Loading	*t*-value	AVE	Composite Reliability	Cronbach's Alpha
ATT	ATT1	0.851	17.411	0.743	0.896	0.743
	ATT2	0.851	27.737			
	ATT 3	0.883	37.162			
DUT	DUT1	0.856	16.092	0.702	0.876	0.702
	DUT5	0.789	12.095			
	DUT7	0.867	15.559			
PGO	PGO2	0.872	18.988	0.814	0.897	0.814
	PGO3	0.932	51.775			
INT	INT1	0.844	27.924	0.697	0.873	0.697
	INT2	0.851	29.004			
	INT3	0.808	29.558			
PBC	PBC1	0.791	17.685	0.675	0.862	0.675
	PBC2	0.814	16.211			
	PBC3	0.859	44.016			
PRO	PRO1	0.862	35.113	0.720	0.885	0.720
	PRO2	0.849	19.994			
	PRO3	0.835	24.024			
SN	SN1	0.812	13.995	0.725	0.888	0.725
	SN2	0.918	73.203			
	SN3	0.821	14.076			
PMP	PMP1	0.891	40.263	0.804	0.925	0.804
	PMP2	0.940	86.254			
	PMP3	0.857	17.637			

Table 4: Latent variable mean, standard deviation (SD), and correlations.

		Mean	SD	1	2	3	4	5	6	7	8
1	ATT	3.500	.940	**0.743**							
2	DUT	4.460	.503	0.055	**0.702**						
3	PGO	3.541	.930	0.329	0.198	**0.814**					
4	INT	4.411	.515	0.296	0.336	0.233	**0.697**				
5	PBC	4.079	.717	0.139	0.198	0.258	0.601	**0.675**			
6	PRO	3.492	.769	0.328	0.095	0.586	0.247	0.280	**0.720**		
7	SN	4.102	.682	0.116	0.281	0.147	0.600	0.516	0.182	**0.725**	
8	PMP	3.387	.930	0.186	0.151	0.291	0.357	0.395	0.279	0.318	**0.804**

Note: Values on the diagonal and bold are AVEs.

Table 5: Cross loadings of items.

Item	**ATT**	**DUT**	**PGO**	**INT**	**PBC**	**PRO**	**SN**	**PMP**
ATT1	**0.851**	0.046	0.264	0.179	0.082	0.234	0.068	0.087
ATT2	**0.851**	0.006	0.239	0.247	0.135	0.299	0.134	0.133
ATT 3	**0.883**	0.083	0.333	0.315	0.134	0.303	0.094	0.232
DUT1	0.019	**0.856**	0.181	0.290	0.248	0.105	0.251	0.173
DUT5	0.035	**0.789**	0.136	0.198	0.096	0.079	0.164	0.125
DUT7	0.078	**0.867**	0.174	0.331	0.138	0.060	0.270	0.089
PGO2	0.275	0.137	**0.872**	0.174	0.197	0.459	0.119	0.184
PGO3	0.314	0.211	**0.932**	0.239	0.261	0.584	0.143	0.323
INT1	0.195	0.406	0.239	**0.844**	0.440	0.181	0.560	0.273
INT2	0.311	0.189	0.219	**0.851**	0.585	0.325	0.451	0.392
INT3	0.235	0.245	0.121	**0.808**	0.479	0.106	0.491	0.224
PBC1	0.165	0.250	0.185	0.551	**0.791**	0.154	0.499	0.354
PBC2	0.096	0.068	0.137	0.365	**0.814**	0.202	0.312	0.231
PBC3	0.079	0.141	0.288	0.526	**0.859**	0.323	0.428	0.361
PRO1	0.317	0.015	0.506	0.179	0.280	**0.862**	0.161	0.337
PRO2	0.194	0.033	0.472	0.263	0.182	**0.849**	0.129	0.209
PRO3	0.309	0.205	0.511	0.199	0.238	**0.835**	0.169	0.143
SN1	0.223	0.100	0.145	0.440	0.313	0.220	**0.812**	0.197
SN2	0.116	0.328	0.148	0.621	0.503	0.202	**0.918**	0.327
SN3	-0.046	0.260	0.075	0.440	0.487	0.028	**0.821**	0.271
PMP1	0.240	0.193	0.276	0.327	0.319	0.253	0.221	**0.891**
PMP2	0.189	0.107	0.273	0.339	0.394	0.283	0.307	**0.940**
PMP3	0.065	0.109	0.234	0.293	0.346	0.211	0.327	**0.857**

Table 6: Testing mediating effect of TPB on the relationship between perceived cultural values and behavioral intention.

Category	Ind. Variables	Base Model			Model 1a: CUL→ATT			Model 1b: CUL→SN			Model 1c: CUL→PBC			Model 2: CUL→INT			Model 3: CUL+TPB→INT		
		β	t	p	β	t	p	β	t	p	β	t	p	β	t	p	β	t	p
Control Variables	DUT	.336	4.221	.000										.305	3.825	.000	**.161**	2.616	.010
	EDU	.018	.224	.823										.004	.051	.960	.073	1.214	.227
	EXP	.004	.055	.957										-.005	-.057	.954	-.022	-.358	.721
	JOB	-.047	-.594	.554										-.040	-.512	.610	-.083	-1.423	.157
TPB Variables	ATT																**.197**	3.161	.002
	SN																**.366**	5.236	.000
	PBC																**.360**	5.207	.000
Org. Culture	PGO				**.208**	2.181	.031	.061	.604	.547	.142	1.459	.147	.068	.701	.485	-.012	-.167	.868
	PRO				**.206**	2.162	.032	.146	1.454	.148	**.197**	2.013	.046	**.176**	1.833	.069	.000	.002	.999
Regress. Quality Indicator	R^2	.116			.136			.036			.092			.164			.548		
	R^2-adj.	.091			.124			.022			.079			.129			.519		
	F	4.677		.000	11.391		.000	2.671		.073	7.327		.001	4.618			18.604		.000

Table 7: Testing mediating effect of TPB on the relationship between perceived top management participation and behavioral intention.

Category	Ind. Variables	Base Model			Model 1a PMP→ATT			Model 1b PMP→SN			Model 1c PMP→PBC			Model 2 PMP→INT			Model 3 PMP+TPB→INT		
		Beta	t	Sig.	Beta	t	Sig.	Beta	t	Sig.	Beta	t	Sig.	Beta	t	Sig.	Beta	t	Sig.
Control Variables	DUT	.336	4.221	.000										.305	3.825	.000	**.156**	2.592	.011
	EDU	.018	.224	.823										.004	.051	.960	.068	1.135	.258
	EXP	.004	.055	.957										-.005	-.057	.954	-.018	-.307	.760
	JOB	-.047	-.594	.554										-.040	-.512	.610	-.082	-1.412	.160
TPB Variables	ATT																**.188**	3.195	.002
	SN																**.360**	5.145	.000
	PBC																**.345**	4.947	.000
Top Management	PMP				**.186**	2.284	.024	**.318**	4.050	.000	**.395**	5.200	.000	**.357**	4.620	.000	.043	.681	.497
Regress. Quality Indicator	R2	.116			.034			.101			.156			.164			.550		
	R2-adj.	.091			.028			.095			.150			.129			.524		
	F	4.677		.000	5.215		.024	16.404		.000	27.036		.000	4.618			21.199		.000

Table 8: Total effect of constructs on endogenous variables.

Causal Chain	**Coefficient**	**t-stat.**	**Significance**
Compliance Intention (INT)			
PBC → INT	0.368	4.389	***
SN → INT	0.361	5.192	***
PMP →INT	0.293	5.874	***
ATT → INT	0.189	3.189	***
DUT → INT	0.174	2.161	**
ROR → INT	0.120	1.562	
EDU → INT	0.071	1.365	
GOR → INT	0.047	0.666	
EXP → INT	-0.019	0.428	
JOB → INT	-0.079	1.720	*
Employee Attitude (ATT)			
ROR → ATT	0.201	2.038	**
GOR → ATT	0.191	2.037	**
PMP → ATT	0.185	2.311	**
Subjective Norm (SN)			
PMP → SN	0.321	5.106	***
ROR → SN	0.092	0.989	
GOR →SN	0.011	0.048	
Perceived Behavioral Control (PBC)			
PMP → PBC	0.401	6.772	***
ROR → PBC	0.131	1.697	*
GOR → PBC	0.080	0.928	
Perceived Cultural Orientation			
PMP → GOR	0.292	4.413	***
PMP → ROR	0.286	3.727	***

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$