Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2008 Proceedings

European Conference on Information Systems (ECIS)

2008

Top Management Championship and Individual Behaviour Towards Information Security: An Integrative Model

Qing Hu
Florida Atlantic University, qhu@fau.edu

Tamara Dinev
Florida Atlantic University, tdinev@fau.edu

Paul Hart
Florida Atlantic University, hart@fau.edu

Donna Cooke
Florida Atlantic University, cooke@fau.edu

TOP MANAGEMENT CHAMPIONSHIP AND INDIVIDUAL BEHAVIOUR TOWARDS INFORMATION SECURITY: AN INTEGRATIVE MODEL

Hu, Qing, Florida Atlantic University, Boca Raton, FL 33431, qhu@fau.edu

Dinev, Tamara, Florida Atlantic University, Boca Raton, FL 33431, tdinev@fau.edu

Hart, Paul, Florida Atlantic University, Boca Raton, FL 33431, hart@fau.edu

Cooke, Donna, Florida Atlantic University, Boca Raton, FL 33431, cooke@fau.edu

Abstract

We develop an individual behavioural model in the context of information security in organizational settings. This model integrates the top management championship theory and the theory of planned behaviour in conjunction with organizational culture and personality traits. Using structural equation modelling techniques and survey data, we test hypotheses on how top management beliefs and participation influence key individual behavioural determinants as well as the role of organizational culture and personality traits in moderating the relationships among key constructs. We find that the influence of top management on employee behaviour is mostly through the top management participation in information security-related initiatives and activities. More importantly, we find that a rules-oriented organizational culture enhances the effect of top management participation on employee behaviour. However, the hypothesized moderating effect of personality trait (dutifulness) on the relationships between attitudes, subjective norm, perceived behavioural control and behavioural intention are not supported.

Keywords: *Information Security, Top Management Championship, Organizational Culture, Personality Traits.*

1 INTRODUCTION

While the ongoing ICT driven globalization has brought unprecedented prosperity to individuals and businesses across the world, the high level of connectivity has also created new opportunities for the dark side of the technological world. Computer viruses, spyware, cyber attacks, and computer system security breaches are almost daily occurrences. These attacks have resulted in financial losses amounting to hundreds of millions of dollars to companies and organizations in the US (Gordon et al., 2005) and possibly billions of dollars around the world (Mercuri, 2003). The significant advances in communications and networking technologies, epitomized by the explosive growth of the Internet, have only exacerbated the complexity and vulnerability of organizational information systems. It is well-understood in the information security research and practices that having air-tight security technology in all organizational systems is neither attainable nor effective. Recent studies argue that securing organizational systems is only attainable with solutions based on sound understanding of the underlying socio-organizational phenomena (Dhillon and Backhouse, 2001; Hu et al., 2007).

One of the key aspects of the socio-organizational perspective of information security is to understand how the interactions among organizational, individual, and technical factors shape the final outcomes of information security of an organization. This is because organizational systems are complex systems created by humans to facilitate the collaborations among individuals and groups, to support information sharing and work processes, and to conduct business transactions among business partners and customers. The security of an organizational system can only be as good as the weakest link in

the entire system. While a considerable amount of resources have been devoted to developing increasingly sophisticated security technologies, it is often the organizational factors, including people, policies, processes, and culture, that create the most significant threat to the integrity and security of the systems. In this study, we set out to address two central research questions related to the role of organizational factors in information security: what factors make an employee follow the rules and practices of an organization's information security policies? and how do organizational culture and individual personality interact with these factors in shaping the behavioural outcome of an employee? We submit that individual behaviour toward information security can be shaped and influenced by the actions of top management, individual cognitive beliefs about information security, the organizational culture, and personality. By testing an integrated behavioural model that combines the theoretical frameworks of top management championship and planned behaviour, with considerations for organizational culture and personality traits, we hope to shed some light on these questions.

2 THEORY AND HYPOTHESES DEVELOPMENT

2.1 Conceptual Model

In order to understand the issues in managing individual behaviour towards information security in the context of organizations, this study intends to integrate relatively independent theoretical paradigms into one integrated model. In the extant literature on individual behaviour, the focus is on behavioural constructs believed to influence individual conduct, as typified by the theory of planned behaviour (Ajzen, 1988). On the other hand, literature on organizational behaviour is largely focused on how the institutional environment influences the behaviour of top managers whose actions usually determine organizational behaviour, as widely described in various branches of institutional theory (Powell and DiMaggio, 1991). However, the linkage between top management and individual employee behaviour is often missing from much of the literature. Liang et al. (2007) argue that, as the interface between the external institutional environment and internal organizational structure and culture, top management mediates the interaction between institutional forces and individual employees. This mediating effect must be accounted for in order to fully understand the behaviour of individuals in organizations.

We need to understand why an individual behaves in certain ways in the context of an organization, such as why certain security rules and policies are followed and others are ignored, and why in some organizations employees have a stronger sense of responsibility and accountability towards information security than in others. In order to accomplish that, we draw on the findings of prior literature and argue that it is necessary to integrate the two theoretical paradigms and analyze the roles of influential and moderating factors. The fundamental thesis of this study is that for any organization, the beliefs and actions of the top managers strongly affect employees' beliefs and attitudes toward information security, which in turn determine the employees' behaviour toward information security, while this causal chain of relationships is moderated by the organizational culture and employee personality traits. This logic is depicted in Figure 1.

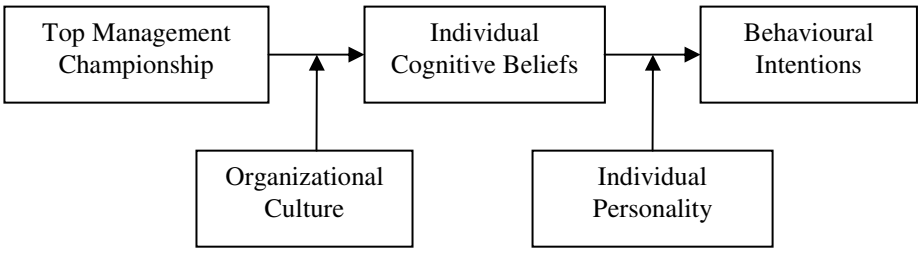

Figure 1: Conceptual Model of Individual Behaviour in Organizations

2.2 The Role of Individual Cognitive Beliefs

One of the main objectives of this study is to understand the factors that influence employee security behaviour in organizational settings. Fortunately, a rich body of literature exists on individual behavioural models and theories. For our purpose, we draw on the well-established theory of planned behaviour (TPB) by Ajzen (1988). TPB contends that a person's behaviour is determined by his or her intention to perform the behaviour of interest. This behavioural intention is, in turn, determined by three factors: attitude toward the behaviour (ATB), subjective norm (SN), and perceived behavioural control (PBC). Extensive extant literature on individual behaviour in a variety of organizational and social settings has rendered strong support for the fundamental propositions of this theory. Adapting the propositions of the theory of planned behaviour to the context of information security, we get the following hypotheses:

Hypothesis 1: Stronger positive attitude toward information security leads to stronger behaviour intentions to conform to organizational security policies.

Hypothesis 2: Stronger organizational norm about information security leads to stronger behaviour intentions to conform to organizational security policies.

Hypothesis 3: Stronger perceived control over information security leads to stronger behaviour intentions to conform to organizational security policies.

2.3 The Role of Top Management

In organizational settings, the cognitive beliefs of employees, including attitudinal, normative, and control beliefs, are inevitably influenced by the top management team (Jarvenpaa and Ives, 1991; Armstrong and Sambamurthy, 1999; Sharma and Yetton, 2003). To develop a refined understanding of the role of top management in shaping the behaviour of employees, following Jarvenpaa and Ives (1991) and Liang et al. (2007), we operationalize the concept of top management championship based on its two dimensions: top management beliefs (TMB) and top management participation (TMP). TMB refers to a subjective psychological state of the manager regarding the potential and benefits of certain organizational actions, while TMP refers to the behaviour and actions of the manager performed in facilitating the organizational actions (Liang et al., 2007).

2.3.1 Top Management Beliefs

The basic thesis in TPB is that an individual's beliefs about behaviour determine the individual's intention to conduct this behaviour (Ajzen, 1988). There is no exception when top management team members themselves are concerned. Strong evidence in the literature supports the notion that top management beliefs guide their actions. For example, Srivastava (1983) argues that top managers' mental image of a desired future organizational state often guides the formation of organizational strategies, decisions, and behaviour. Liang et al. (2007) find that top management belief about the benefits of ERP systems is a strong predictor of their participation in ERP assimilation related activities. Therefore, we propose that:

Hypothesis 4: Stronger top management beliefs about the benefits of information systems security lead to higher levels of top management participation in the information systems security initiatives.

In addition, top management beliefs about information security are likely to be perceived by employees as positive cues for the significance of information security in their organization. Because they are from the top management, such external stimuli are likely to have a stronger influence on the formation of the employee attitude toward information security and the subjective norm of the social groups within the organization. Thus, we propose that:

Hypothesis 5: Stronger top management beliefs about the benefits of information systems security lead to stronger positive attitudes of employees toward information security initiatives.

Hypothesis 6: Stronger top management beliefs about the benefits of information systems security lead to stronger subjective norm about information security initiatives in an organization.

2.3.2 Top Management Participation

The critical role of top management participation in IT systems implementation and assimilation in organizations has been clearly established in the literature (Armstrong and Sambamurthy 1999; Purvis et al. 2001; Sharma and Yetton 2003; Liang et al., 2007). Following the findings of this line of research, we argue that top management team participation in information security related activities could take many shapes and forms. For instance, top management can create organizational structures that facilitate the implementation of information systems security initiatives. Top management can also champion the new initiatives by allocating resources, participating in meetings, and helping resolve conflicts. Such top management actions often lend legitimacy in the mind of employees and other managers to the security initiative. Legitimacy of security initiatives is especially important since information security initiatives are often considered as an "extra burden" to routine work and "other people's job" (Hu et al., 2007). Top management participation in security initiatives could also send a strong signal to other managers and employees about how much they value the security initiatives. These mechanisms have a meta-structuring effect by providing a vision as to what the initiative is supposed to achieve and by encouraging employees to adapt the new artefacts towards specific goals (Chatterjee et al., 2002). Thus, we propose:

Hypothesis 7: Stronger top management participation in information security initiatives lead to stronger positive attitudes of employees toward information security activities.

Hypothesis 8: Stronger top management participation in information security initiatives lead to the stronger subjective norm about information systems security in organizations.

Hypothesis 9: Stronger top management participation in information security initiatives lead to the stronger perceived behavioural control over information security activities.

2.4 The Role of Organizational Culture

In this study, our focus is on whether and how organizational culture influences the employee behaviour toward information security. For this purpose, we use the value aspects of culture and 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 and Kayworth, 2006, p. 359). In organizational settings, these values form the foundation of organizational culture and define the norms of individual behaviour (Leidner and Kayworth, 2006). In the value models of culture proposed by Quinn (1988), organizational cultures are described in terms of two orthogonal dimensions: internal vs. external, and flexibility vs. control. These two dimensions form four quadrants of competing values: support orientation, innovation orientation, goal orientation, and rules orientation (Quinn, 1988). In supportive organizations, organizational culture can be characterized as participative, cooperative, team-spirit, trust, and individual growth; in innovative orientation, organizational culture can be characterized as creative, open-to-change, anticipative, and experimental; in goal-oriented, organizational culture is more toward rationality, accomplishment, accountability, and contingent awards; and finally, in rules-oriented organizations, organizational culture can be characterized as respect for authority, rationality for procedures, hierarchical structure, and formal communications (Van Muijen et al., 1999).

In this study, we submit that organizational culture moderates the relationship between top management championship and individual cognitive beliefs. Given the fact that conforming security behaviour, such as following the rules and practices specified in organizational security policies, is

usually not seen as a performance indicator and is rarely rewarded like other achievements in organizational settings, a rules-oriented culture is perhaps the most important factor that influences how top management beliefs and actions are translated into employee behaviour. To most individuals in an organization, from managers to workers, security is often considered as something extra to their main job and a burden to their performance (Hu et al, 2007). In such environment, we believe, it is the actual top management efforts (i.e. top management participation), facilitated by a strong rules-oriented culture, that will make a difference in shaping employees' security behaviour. Therefore, it is not difficult to infer that strong rules-orientation will likely enhance the relationship between top management participation and employee beliefs about the importance and consequences of information security. Thus, we posit that:

Hypothesis 10: The relationship between top management participation in information security and attitudes of employees toward information security is strengthened in organizations with a strong rules-oriented culture.

Hypothesis 11: The relationship between top management participation in information security and the subjective norm about information security is strengthened in organizations with a strong rules-oriented culture.

Hypothesis 12: The relationship between top management participation in information security and the perceived behavioural control over information security is strengthened in organizations with a strong rules-oriented culture.

On the other hand, a stronger rules-oriented culture will likely weaken the effect of top management beliefs on employees' behaviour. This is because beliefs may not necessarily be manifested in behaviour and individual beliefs may be suppressed by strong rules in organization about certain behaviour. Therefore, what top management believes would matter less in affecting employees' attitudes and subjective norm in a strong rules-oriented culture. Thus, we propose that:

Hypothesis 13: The relationship between top management belief in information security and attitudes of employees toward information security is weakened in organizations with a strong rules-oriented culture.

Hypothesis 14: The relationship between top management belief in information security and the subjective norm about information security is weakened in organizations with a strong rules-oriented culture.

2.5 The Role of Personality Traits

According to trait theorists in the personality field, personality traits are useful for explaining the behaviour of individuals (Allport, 1937). Traits are particularly appealing in the study of behaviour because they are relatively stable characteristics of individuals and not expected to vary with external stimuli. Traits are manifested in consistent patterns of thoughts, feelings, and actions. Recent research on personality has centered on the Five-Factor Model (FFM) that lists Neuroticism (N), Extraversion (E), Openness (O), Agreeableness (A), and Conscientiousness (C) as the domains which comprehensively represent all traits (Costa & McCrae, 1995). Based on the literature, we submit that Conscientiousness and its facets are the most relevant as antecedents or moderator variables to be introduced into the study of information security behaviours. Of its facets, dutifulness seems more closely related to the quality of conforming behaviours we seek to predict. Dutiful individuals abide by rules, adhere to the status quo and are unlikely to be creative (Feist, 1998). We expect that for dutiful employees, the relationship between beliefs constructs (attitudes towards security, subjective norm, and perceived control) and intent to conform to security policies and practices will be stronger than for less dutiful employees. This is because conscientious employees "may have a stronger desire to follow rules more than others" (Tyler & Blader, 2005, p. 1145). Therefore, dutiful employees have stronger intentions to follow policies since they have an intrinsic desire to abide by rules and procedures. Thus a moderating effect is hypothesized.

Hypothesis 15: Dutifulness of employees positively moderates the relationship between attitudes toward information systems security and behavioural intention to conform to security policies and practices.

In addition, dutiful employees, being more rule-bound, are likely to follow security policies when influential others think the same as they do, that is. Hence we hypothesize that dutifulness moderates the relationship between subjective norm and the intention to conform. In a similar vein, we expect dutifulness to play a moderating role in the relationship between perceived control and intent to conform. When dutiful employees believe that they have the resources, training, and ability to follow security rules and procedures, the strength of the relationship between perceived control and intent to conform will be greater than it is for less dutiful employees. Following this, we hypothesize that dutifulness will moderate the relationship between perceived control and intent to conform. Thus,

Hypothesis 16: Dutifulness of employees positively moderates the relationship between organizational norm about information systems security and individual behavioural intention to conform to security policies and practices.

Hypothesis 17: Dutifulness of employees positively moderates the relationship between perceived control over information systems security and behavioural intention to conform to security policies and practices.

These research hypotheses are summarized in Figure 2. The main constructs are depicted in solid boxes and the two moderating constructs, organizational culture and personality trait, are depicted in dashed boxes. In the following section, we describe how we developed our measurement instrument for this model and collected survey data in order to test the hypothesized relationships.

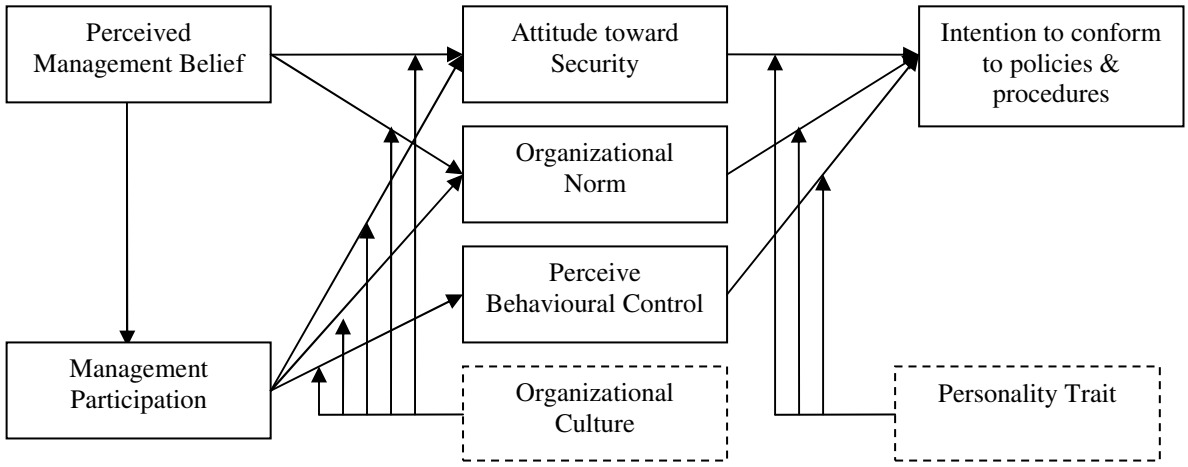

Figure 2: Research Model

3 DATA AND ANALYSIS

3.1 Data Collection

Measurement items of a survey instrument were adapted from extant instruments in the literature and refined through a pilot study. The final version of the survey was published on a survey web site. The intention was to distribute the link to potential respondents who are employed full or part time in various organizations for maximum efficiency and accuracy. We sent a total of 1089 emails to the alumni of the MIS program in the authors' university and invited the recipients to participate in our study with the link to the online survey. Of these, 220 emails returned as undeliverable by the email servers at the destinations. From the remaining 869 emails, we received total of 75 responses. In the

course of the following month we performed a second round of request for responses in an email campaign to the same email recipients. We obtained additional 79 responses. From both campaigns, six responses were eliminated due to many null entries. This yielded a total response rate of approximately 17%, consistent with the response rate reported in many IS studies.

3.2 Confirmatory Factor Analysis

The research model was tested through Structural Equation Modeling (SEM) using LISREL. The covariance structure model consists of two parts: the measurement model (sometimes referred as CFA stage), and the structural model (also known as SEM stage) (Joreskog and Sorbom 1989). We used the two-stage approach, as recommended by Gerbing and Anderson (1988) to first assess the quality of our measures through CFA and then test the hypotheses through the structural model. All the necessary steps in the measurement model validation and reliability assessment were conducted following the widely used validation heuristics by Byrne (1998) and Gefen et al. (2000). The analysis resulted in a converged, proper solution with a low $\chi 2$ per degree of freedom and a good fit as indicated by all the listed fit indices. Collectively, the data from the model fit indices (Table 3), factor loadings, and t-values (Table 1) suggest that the indicators account for a large portion of the variance of the corresponding latent constructs and therefore provide support for the convergent validity of the measures (Gefen et al., 2000).

Latent Variable	**Item**	**Latent Construct Loadings and error terms in ()**								**t-values**	**Reliability**
		ATT	**SN**	**PBC**	**BI**	**DUT**	**MB**	**MP**	**RO**		
		α =.94	α =.90	α =.84	α =.75	α =.76	α =.83	α =.92	α = .81		
Attitude towards Behaviour ATT	1	.73(.04)								11.07	.88
	2	.97(.04)								10.25	
	3	.82(.06)								13.61	
Subjective Norm SN	1		.89(.05)							12.34	.87
	2		.86(.05)							11.97	
Perceived Behaviour Control PBC	1			.84(.05)						8.86	.86
	2			.89(.04)						9.34	
Behaviour Attention BI	1				.83(.06)					12.41	.84
	2				.84(.05)					11.09	
	3				.71(.07)					6.23	
Dutifulness DUT	1					.92(.04)				6.54	.88
	2					.66(.08)				3.60	
	3					.94(.04)				10.45	
Management Belief MB	1						.92(.04)			10.23	.84
	2						.75(.07)			9.71	
	3						.71(.08)			9.22	
Management Participation MP	1							.70(.06)		7.40	.85
	2							.80(.05)		8.12	
	3							.74(.05)		7.15	
Rule Orientation RO	1								.67(.08)	7.58	.86
	2								.86 .05)	8.23	
	3								.74(.06)	8.16	

Table 1: Confirmatory Factor Analysis

Discriminant validity is assessed by testing whether the correlations between pairs of dimensions are not equal or close to 1.00 within 95% confidence intervals (Bagozzi 1991). The highest value of the correlations in our study (Table 2) is .77 between BI and SN with error term .06. Thus, with 95%

confidence, the correlation is in the interval between .72 and .82. Additionally, discriminant validity can be tested through evaluating pair-wise χ^2 difference tests between the constrained and unconstrained covariance structures (Gefen et al., 2000). In order to establish discriminant validity, the χ^2 value of the unconstrained model must be significantly lower than that of the constrained model. For each model run, the difference in χ^2 was considerably greater than the cut-off value of 3.84. Third, the squared correlations between all latent constructs were significantly less than the corresponding AVE (Fornell and Larcker 1981). All the criteria adequately demonstrated discriminant validity of the model.

A measure of the internal consistency of the scales is the composite reliability (sometimes called reliability coefficient) computed in conformance with the formula prescribed by Werts et al. (1974). Compared to Cronbach's alpha which provides a lower bound estimate of the internal consistency, the composite reliability is a more rigorous estimate for the reliability (Chin and Gopal 1995). A composite reliability greater than .5 would indicate that at least 50% of the variance in a measurement is captured by the trait variance and that the variance captured by the measures is greater than the one captured by the errors (Bagozzi 1991). The recommended values for establishing a tolerable reliability are above .70 (Werts et al. 1974; Gefen et al., 2000) and for strong reliability are above .80 (Koufteros 1999). The reliability coefficients of the constructs in this study are given in Table 1. Their high values provide further evidence of the reliability of the scales.

Finally, the threat of the common methods bias (Podsakoff et al. 2003) was addressed. By ensuring anonymity to the respondents, assuring them that there are no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study, we reduced the likelihood of bias caused by social desirability or respondent acquiescence (Podsakoff et al. 2003). Also, following Podsakoff et al. (2003), we empirically determined the common method variance using Harman's single-factor test by simultaneously loading all items in factor analysis using Varimax rotation. All indicators showed high factor loadings and low cross-loadings, indicating that our data do not suffer from common method bias.

	Mean	**Std. Dev.**	**ATT**	**SN**	**PBC**	**BI**	**DUT**	**MB**	**MP**	**RO**
ATT	4.47	.73	**.72**							
SN	4.09	.75	.57 (.06)	**.77**						
PBC	3.99	.84	.32 (.05)	.44 (.05)	**.75**					
BI	4.29	.57	.59 (.07)	.77 (.06)	.63(.07)	**.63**				
DUT	4.63	.50	.28 (.7)	.36 (.07)	.29(.04)	.47(.05)	**.72**			
MB	3.77	.82	.10 (.03)	.36 (.06)	.24(.05)	.29(.0)	.14(.04)	**.64**		
MP	2.57	.93	.38 (.08)	.41 (.05)	.36(.05)	.41(.06)	.19(.04)	.48 (.06)	**.57**	
RO	3.50	.76	.10 (.06)	.23 (.04)	.27(.04)	.19(.05)	.18(.04)	.40 (.05)	.17 (.05)	**.59**

Table 2. Latent Variable Statistics

* The diagonal terms indicate the AVE for each construct.

3.3 Structural Equation Modelling

Upon successful validation of the instrument, we proceeded with testing the hypothesized relationships of the model. The SEM stage specifies the direct and indirect causal relationships among the constructs and the amount of unexplained variance (Anderson and Gerbing 1988). The goodness-of-fit indices are reported in Table 3. All the values are within the acceptable range for a good model fit and thus indicate a good empirical support of the theoretical framework. Additionally, the moderating effects of the personality trait (DUT) and rules-orientation (RO) were tested. According to

the classical definition of moderation effect, the latter occurs when a variable (in our case DUT and RO) changes the strength of the causal relationship between two other variables. In order to rigorously test the moderating effect of the personality traits on the research model, the moderators were included in the model as product (interaction) terms of the relevant latent variables.

Goodness of Fit Measures	**χ^2(d.f.)**	**χ^2/d.f**	**NNFI**	**CFI**	**IFI**	**GFI**	**AGFI**	**RMSEA**
Good Model Fit Ranges	Non-sign.	<2.00	>.90	>.90	>.90	≈.90	>.80	<.800
SEM Model	413.44 (300)	1.38	.92	.93	.93	.85	.79	.048

Table 3. Goodness of Fit Indices

Table 4 provides a summary of the test results of research hypotheses. The results provided strong support for the majority of the hypotheses of the study, with most of the path coefficients statistically significant at $p < .01$ level.

Dependent Var.	**Dependent Var.**	**Hypothesis**	**Path Coefficient**
BI	ATT	H1	.19*
	SN	H2	.51**
	PBC	H3	.34**
	DUT*ATT	H15	-.20*
	DUT*SN	H16	NS
	DUT*PBC	H17	NS
ATT	MB	H5	NS
	MP	H7	.43**
	MB*RO	H13	-.62**
	MP*RO	H10	.70**
SN	MB	H6	NS
	MP	H8	.31**
	MB*RO	H14	-.69*
	MP*RO	H11	.83**
PBC	MP	H9	.33*
	MP*RO	H12	.38*
MP	MB	H4	.54**

Table 4. Summary of Model Relationships and Moderating Effects

4 DISCUSSION AND IMPLICATIONS

4.1 The Role of Individual Cognitive Beliefs

The research hypotheses, H1, H2, and H3, are supported by the data, which once again confirms the resilience and reliability of the TPB model in predicting individual behaviour in various social

contexts. Interestingly, among the three determinants of behavioural intention, subjective norm is the most significant with the highest path coefficient. On the other hand, the role of attitude is relatively weak, significant only at the $p < .05$ level. This is a strong indication that in organizational settings, individual attitudes toward information security may not matter as much as the subjective norm of the social groups within the organization. This result is in stark contrast with those of Dinev and Hu (2007) where the influence of subjective norm is found to be insignificant in the settings of individual voluntary use of anti-spyware. The effect of perceived behavioural control on behavioural intention is strong and consistent with the results of Dinev and Hu (2007). Therefore, the more an employee feels she is in control, the more likely she will behave in accordance to the security policies and practices, and less likely to make careless mistakes that often are the sources of security breaches.

4.2 The Role of Top Management

The critical role of top management in information security cannot be over emphasized. Our results clearly show that top management can significantly affect employee behaviour toward information security. However, while we hypothesized that top management beliefs and participation are antecedents to the employee behavioural constructs, only H7, H8, and H9, which are related to the effect of top management participation, are shown to be significant; H5 and H6, which are related to the effect of perceived top management beliefs, are insignificant. Thus, our results suggest that actions speak louder than words when it comes down to influencing employee security behaviour by the top management team. Top management must actively participate in information security initiatives which help create strong and positive attitudes and subjective norm towards information security in the organization. On the other hand, top management beliefs are shown to have a strong and significant impact on top management participation (H4), suggesting that the influence of top management beliefs on employee behaviour is mediated through top management actions. This result is consistent with the results of Liang et al. (2007), which further demonstrates the value of decomposing the concept of top management championship into two first-order constructs of belief and participation.

4.3 The Role of Organizational Culture

The results about the moderating role of organizational culture, operationalized as rules orientation, on the relationship between top management and behavioural constructs of employees are in agreement with our theoretical arguments. In our empirical model, the relationships between top management beliefs and the attitude of the employees and the subjective norm of the organization (H5 and H6) are statistically insignificant. This is likely due to the strong moderating effect of the rules orientation in the hypothesized direction (H13 and H14). That is, in an organization with strong rules-oriented culture, the perceived top management beliefs have insignificant influence on the attitudes of employees and subjective norm of the organization about information security. On the other hand, the moderating effects of rules-oriented culture on the relationships between top management participation and attitudes, subjective norm, and perceived behavioural control are all found to be significant and in the same direction as hypothesized (H10, H11, and H12). That is, in an organization with strong rules-oriented culture, the influence of top management participation is enhanced on the areas of employee attitudes, subjective norm, and perceived behavioural control regarding information security practices and rules.

4.4 The Role of Personality

Our results on the moderating role of dutifulness are rather surprising and need to be examined with caution. Of the three hypotheses, only H15 is significant, but it is in the opposite direction to what is hypothesized. We argued that employees with higher scores on dutifulness should exhibit a stronger relationship between attitudes toward security and behavioural intention to conform to security

practices and rules. However, the data suggest otherwise. Our results show that dutifulness of an employee has little to do with the degree to which subjective norm or perceived behavioural control may influence his or her behavioural intention. On the other hand, a higher degree of dutifulness may actually interfere negatively the degree to which attitudes influences behavioural intention. This result is also difficult to explain in the context of information security and needs further investigation.

5 CONCLUSION

In this study, we developed an integrated behavioural model in the context of information security by combining two well-established theories: the top management championship and the theory of planned behaviour, while considering the moderating effects of organizational culture and personality traits. Using structural equation modelling techniques and survey data, we tested the basic hypotheses on how top management beliefs and participation could influence the key individual behavioural modifiers and the role of organizational culture and personality traits in moderating the relationships among these key constructs.

The hypothesized relationships are generally supported by the data. We confirmed that the established behavioural modifiers – attitudes, subjective norm, and perceived behavioural control – indeed significantly influence an individual's behavioural intention to conform to organizational security practices and policies. We also confirmed the influence of top management on employee behaviour is mostly through top management participation in information security related initiatives and activities: actions are louder than words. More importantly, we find that rules-oriented culture indeed enhances the effect of top management participation on employee behaviour. However, we were unable to confirm the hypothesized effect of dutifulness on the relationships between the behavioural antecedents and the behavioural intention.

Our study inevitably has its limitations and calls for further research. For example, both organizational culture and personality traits are multi-dimensional and multi-faceted complex concepts, but we were able to test only one personality trait (dutifulness) and one cultural dimension (rules-orientated). Given the inconclusive findings about the role of dutifulness, testing the moderating effects of other facets of personality traits may shed some light on this important aspect of information security. Investigating the effects of the other cultural dimensions would be another interesting future project, given the fact that we were unable to explain the significant but negative effect of rules orientation on certain relationships in our model.

References

Ajzen, I. (1988) *Attitudes, Personality, and Behavior*, Dorsey Press, Chicago, IL.

Allport, G. W. (1937) *Personality: A psychological interpretation*. Holt, Rinehart and Winston, New York, NY.

Armstrong, C., and 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. (1991) Structural Equation Models in Marketing Research, 1*st Annual Advanced Research Techniques Forum,* W. Neil(ed.), American Marketing Association, Chicago, IL.

Byrne, B. (1998) *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*, Lawrence Erlbaum Associates, N.J.

Chatterjee, D., Grewal, R., and Sambamurthy, V. (2002) Shaping up for E-commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies. *MIS Quarterly,* 26(2), 65-89.

Chin, W. and Gopal, A. (1995) Adoption intention in GSS: Importance of beliefs, *Data Base Adv.* 26, 42-64.

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

Dhillon, G. and Backhouse, J. (2001) Current Direction in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 11, 127-153.

Dinev, T. and 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.

Feist, G.J. (1998) A meta-analysis of the impact of personality on scientific and artistic Creativity. *Personality and Social Psychological Review*, 2, 290-309.

Gefen, D., Straub, D. W., Boudreau, M.C. (2000) Structural Equation Modeling And Regression: Guidelines For Research Practice, C*ommunications of the AIS*, 4, Article 7.

Gorden, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2005) 2005 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. Available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf, accessed on July 25, 2006.

Hu, Q., Hart, P., and Cooke, D. (2006) The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective. *Journal of Strategic Information Systems*, 16(2), 153-172.

Jarvenpaa, S. L. and Ives, B. (1991) Executive Involvement and Participation in Management Information Technology. *MIS Quarterly*, 15(2), 205-227.

Jöreskog, K.G., and Sörbom, D. (1989) *LISREL7:* A Guide to the Program and Applications, SPSS Inc., Chicago, IL.

Koufteros, X. A. (1999) Testing a Model of Full Production: A Paradigm for Manufacturing Research Using Structural Equation Modeling. *Journal of Operations Management* 17, 467-488.

Leidner, D. E. and Kayworth, T. (2006) Review: A Review of Culture In Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS Quarterly*, 30(2), 357-399.

Liang, H., Saraf, H., Hu, Q., and 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.

Mercuri, R. T. (2003) Analyzing Security Costs. *Communications of the ACM*, 46(6), 15-18.

Nunnally, J.C. (1967) *Psychometric Theory*, McGraw-Hill, New York, NY.

Podsakoff, P. M., MacKenzie, S. B., Lee, J-Y., and 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.

Powell, W. W. and DiMaggio, P. J. (1991) The New Institutionalism in Organizational Analysis. The University of Chicago Press, Chicago. IL.

Purvis, R.L., Sambamurthy, V., and Zmud, R.W. (2001) The assimilation of knowledge platforms in organizations: An empirical investigation. *Organization Science*, 12(2), 117-135.

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

Sharma, R., and Yetton, P. (2003) The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation. *MIS Quarterly* , 27(4), 533-555.

Srivastava, S. (1983) *The executive mind*. Jossey-Bass, San Francisco, CA.

Tyler, T. R., and 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.

Van Muijen, J. J., Koopman, P., De Witte, K., De Cock, G., Susanj, Z., Claude 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., and Turnipseed, D. (1999) Organizational Culture: The Focus Questionnaire, *European Journal of Work and Organizational Psychology*, 8 (4), 551–568.

Werts, C.E., Linn, R.L. and Joreskog, K.G. (1974) Interclass Reliability Estimates: Testing Structural Assumptions, *Education and Psychological Measurement,* 34, 25-33.