ORGANISATIONAL SECURITY CULTURE AND INFORMATION SECURITY COMPLIANCE FOR E-GOVERNMENT DEVELOPMENT: THE MODERATING EFFECT OF SOCIAL PRESSURE

Ahmed AlKalbani, School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia, ahmed.al-kalbani@rmit.edu.au

Hepu Deng, School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia, hepu.deng@rmit.edu.au

Booi Kam, School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia, booi.kam@rmit.edu.au

Abstract

Rapid development of e-government has exposed critical public information to the possibility of cybercrime. Information security has become a critical issue that needs to be adequately addressed in e-government development. This paper develops an information security compliance model by drawing insights from organizational and institutional theory literature to examine how organizational security culture influences information security compliance in public organizations for e-government development. It also investigates the role of social pressure in moderating the relationship between information security culture and information security compliance. The study explores three specific dimensions of information security culture: management commitments, accountability and information security awareness. The result of a hierarchical regression analysis indicates that management commitments, accountability, information security awareness, and social pressure have a significant positive impact on information security compliance in public organizations. The moderating role of social pressure, however, is only significant in augmenting the relationship between accountability and information security compliance. This study contributes to the information security compliance research by highlighting the criticality of establishing an information security culture within public organisations to promote information security compliance.

Keywords: E-government, information security compliance, information security culture, social pressure

1. INTRODUCTION

Electronic government (e-government) is a way of delivering public services through the use of information and communication technologies (ICT) (Basu 2004; Deng 2008). While e-government has opened up new ways for governments to interact with their stakeholders, it has also exposed critical information in public service systems to the possibility of cybercrime (Tassabehji et al. 2007). Consequently, information security has emerged as a critical issue in e-government development.

There is an increasing focus on enforcing information security compliance for information security (Boss & Kirsch 2007; Siponen et al. 2007), which is referred to as the effective implementation of information security standards and policies for protecting information in public organizations (AlKalbani et al. 2014; Von Solms 2005). The adoption of information security compliance ensures that information security mechanisms can work together effectively to protect critical information in e-government systems (Tassabehji et al. 2007; Wimmer & Von Bredow 2002). It satisfies the security requirements for e-government services, thus improving users' confidence and trust. As a result, information security compliance is widely considered for ensuring information security in public organizations (Herath & Rao 2009).

Several studies have explored alternative approaches to improving information security compliance. Bulgurcu et al. (2010), for example, investigated the role of information security awareness to change users' attitudes towards complying with information security requirements. Sasse et al. (2001) analysed employees' interactions with security mechanisms to strengthen information security compliance. Lee et al. (2004) explored the use of sanctions to increase information security compliance in public organizations. Siponen et al. (2010) examined the factors relating to normative beliefs, threat appraisal, self-efficacy, and visibility that influence employees' intention to comply with information security standards and policies in organizations. These studies have focused primarily on the factors related to users' attitude, intentions, and behaviours to comply with information security standards and policies. There are, however, many other issues related to organizational security culture and external environment that need to be investigated for improving information security compliance within organisations (Warkentin et al. 2011). To extend the literature on information security compliance, this study aims to develop and validate a conceptual model for information security compliance based on organizational security culture and the moderating role of social pressure.

2. INFORMATION SECURITY FOR E-GOVERNMENT

Information security in e-government not only implies protecting information from unauthorized disclosure but also assuring the accuracy of the information, including maintaining its origin, completeness, and correctness (Benabdallah et al. 2002). It demands that access to information is limited to the right people at the right time (Karokola et al. 2012) and only legitimate data are used in transactions, communications, and documentation (Smith & Jamieson 2006). Information security requires that that all actions compromising information security can be traced back to the responsible party (Wimmer & Von Bredow 2002). In this study, information security is defined as protecting the confidentiality, integrity, availability, authenticity, and accountability of information in e-government systems (Karokola et al. 2012; Zissis & Lekkas 2011).

Many factors affect information security in e-government including the support of senior management (Smith & Jamieson 2006), legislative requirements (Benabdallah et al. 2002), security strategies and policies (Smith & Jamieson 2006), advanced security technologies (Lambrinoudakis et al. 2003), and potential breaches (Benabdallah et al. 2002). There was an average of 23,647 information security breaches in organizations in 2013 (PonemonInstitute 2013). Criminal attacks, human errors, system glitch, and business process failures are among some of the common causes. The existence of information sharing in public organizations raises further security concerns (Baskerville & Siponen 2002; Conklin 2007).

Managing information security in e-government remains a complex and challenging process (Karunasena & Deng 2012). It involves putting in place information security measures and mechanisms that can work together effectively (Neubauer et al. 2006). As public organizations are the host of e-government services, the process warrants adopting a compliance-based approach not only to satisfy the legal security requirements for e-government service offerings, but also to ensure public confidence and trust.

Several studies have examined information security compliance. Herath and Rao (2009), for example, empirically validated an integrated model to gain insights into behaviours, motivations, values and norms that affect employees' intentions to comply with information security policies. Ifinedo (2013) proposed a framework that focuses on changing individual's thoughts, actions, feelings, and attitudes towards information security compliance. Puhakainen and Siponen (2010) developed a training and education approach for improving employees' attitude and behaviour towards information security compliance. The majority of these studies, however, have focused primarily on the factors related to users' attitudes, intentions and behaviours in information security compliance. Other important factors such as organizational security culture and external pressures have not been given much attention (Warkentin et al. 2011).

3. THEORY AND HYPOTHESES DEVELOPMENT

Behavioural theories, such as planned behaviour (Ajzen 1991), deterrence theory (Straub Jr 1990), threat avoidance (Liang & Xue 2010; Warkentin et al. 2011), moral judgment (Myyry et al. 2009), and planned behaviour (Bulgurcu et al. 2010) have been commonly drawn on in information security research. This study aims to investigate the relationship between organizational security culture and information security compliance in public organisations and whether the strength of this relationship is moderated by social pressures. For this reason, this research draws on the technology-organization-environment (TOE) theory (Tornatzky et al. 1990) and the institutional theory (DiMaggio & Powell 1983). TOE argues that the process by which technological innovations are adopted in organizations is conspired by technological, organizational, and environmental contexts (Duan et al. 2012; Tornatzky et al. 1990).

This study focuses on the organization and environment aspects of the TOE theory for information security. Organizational factors such as the communication process and the top management championship affect employees' intentions and behaviours on information security compliance (Dhillon & Backhouse 2001; Sasse et al. 2001). Environmental factors force organizations to secure legitimacy from stakeholders by conforming to external expectations (DiMaggio & Powell 1983). These external expectations impose pressures on public organizations to initiate internal efforts to meet information security requirements.

A conceptual model is developed which hypotheses that organizational security culture will have a positive impact on information security compliance in public organizations for e-government development and that the strength of this relationship is moderated by the intensity of social pressures. Figure 1 shows the conceptual model with the identified constructs and their associated attributes.

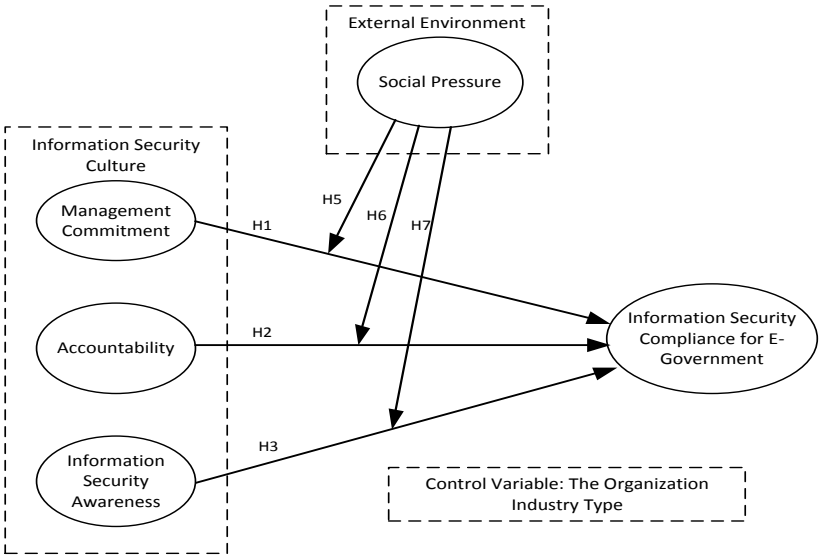

Figure 1. A model for Information Security Compliance for E-Government Development

An effective implementation of information security standards and policies in public organizations implies having an efficient system of executing information security controls (Knorr & Röhrig 2001). Vroom and Von Solms (2004), for example, asserted that the compliance with information security policies can be improved if employees integrate information security mechanisms in their daily work practices.

Beautement et al. (2009) developed a compliance based approach for improving organizational processes in managing information security. Backes et al. (2003) stated that integrating security requirements into the development of organizational processes can improve information security compliance. These studies have shown that security mechanisms must be designed and implemented to support the organizational objectives to promote information security compliance in public organizations. Information security compliance can be measured by employees' perception of the efficiency with which information security requirements are implemented (Chang & Ho 2006), productivity gained in operational processes and performance improvement attributable to the establishment of security mechanisms (Chan et al. 2005).

3.1 Organizational Security Culture

Organizational security culture refers to the belief of individual employees on the value of complying with information security standards and policies (McIlwraith 2006). A security culture could be engendered "by instilling the aspects of information security to every employee as a natural way of performing his or her daily job" (Oost & Chew 2007). There are three major factors that undergird the formation of the organizational security culture: management commitment, accountability, and information security awareness (Bulgurcu et al. 2010; Herath & Rao 2009; Kajava et al. 2007).

Management commitment centers on the efforts of senior management to promote information security compliance (Kajava et al. 2007). Management commitment could be measured by employees' perception of efforts made by management to attain information security compliance, as reflected by management support and involvement, goal alignment, and efficacy (Knapp et al. 2006; Lee et al. 2004). Management support refers to the decisions, investments and actions taken for enforcing information security policies across the organization (Knapp et al. 2006; Lee et al. 2004). Management involvement is exhibited by the extent to which senior management participates in dealing with organization's information security issues (Lee et al. 2004). Goal alignment is the degree of alignment between information security policies and organizational goals. Efficacy refers to the competency and capability of the organisation in managing information security activities, which include the contemporaneousness of information security policies and procedures as well as the communication of these policies and procedures to employees across the organization (Hayes 2004).

Management commitment influences the adoption of information security compliance in public organizations (Smith & Jamieson 2006). It requires visible participation, ongoing communication and championing to stimulate employees' intentions towards information security compliance (Kolkowska & Dhillon 2012). Knapp et al. (2006) showed that creation, training and enforcement of organization's security policies would not be taken seriously without top management support and involvement. The lack of management support has been singled out as a common reason for the weak implementation of information security policies in organization (Knapp et al. 2006; Kolkowska & Dhillon 2012). The discussion above leads this study to propose the following hypothesis.

H1: Management commitment has a positive impact on information security compliance.

Accountability is an important dimension of organizational security culture. It refers to the established measures for promoting individuals' responsibilities towards enforcing information security standards and polices in organizations (Herath & Rao 2009). Accountability can be measured by employees' perception of the level of comprehensiveness of the information security policy for guiding appropriate information security compliance behaviours (Chan et al. 2005; Taylor & Todd 1995), clarity and understandability of the roles and responsibilities (Bulgurcu et al. 2010), appropriateness of sanctions for violating information security policies (Herath & Rao 2009), and the enforcement of information security policies and procedures across the organization (Knapp et al. 2006; Straub Jr 1990).

Extant literature has shown that accountability is one of the most effective elements in building a strong organizational security culture to change employees' attitudes towards information security compliance (Posthumus & Von Solms 2004). If stipulated sanctions are not enforced accordingly, individuals would not expect any consequences when caught breaching information security policies (Adams & Sasse 1999). Ryan (2004) observed that individuals with well-defined roles and responsibilities are more proactive in undertaking higher information security precautions. This leads to the following hypothesis.

H2: Accountability has a positive impact on information security compliance.

Information security awareness stresses the importance of having information security programs in place to increase user's knowledge and understanding of security policies and mechanisms in organizations (Smith & Jamieson 2006). Bulgurcu et al. (2010), for example, pointed out that information security awareness greatly affects employees' beliefs about the benefit of compliance and the cost of non-compliance. Puhakainen and Siponen (2010) found out that employees who understand the benefits and value of information security in their organization have a higher sense of security awareness, which can lead to better compliance with information security policies. Many studies have shown that information security awareness and training could help develop an effective security culture in organizations with a corresponding reduction in misuse intentions and an increase in users' avoidance of information security risks and threats (Bulgurcu et al. 2010; Puhakainen & Siponen 2010; Tsohou et al. 2008).

The awareness of information security compliance can be assessed by employees' perceptions of the features of information security compliance training programs (Bulgurcu et al. 2010; Puhakainen & Siponen 2010; Taylor & Todd 1995). Employees' perception of the effectiveness of training programs reflects the impacts generated by the range and variety of training programs put in place to support organizations' information security goals (Bulgurcu et al. 2010; Eloff & von Solms 2000), while employees' views on program usefulness are the indications of how well such training programs have been structured and presented (Barling et al. 2002; Martins & Elofe 2002). Visibility refers to the clarity of information security activities promoted within organizations by the use of various business communications channels to increase security awareness and security compliance training (Puhakainen & Siponen 2010; Taylor & Todd 1995). This discussion above leads to the development of the following hypothesis.

H3: User's awareness has a positive impact on information security compliance.

3.2 The Moderating Role of Social Pressure

Environment or external pressures coerce public organizations to improve their information security compliance. Such pressures prompt internal organization efforts toward information security compliance (Chang & Ho 2006; Herath & Rao 2009; Karunasena & Deng 2012). Existing research on information security has identified social pressure as an environmental factor that could propel organizations to integrate information security mechanisms into their daily practices by motivating managers and employees to comply with information security practices(e.g., Khansa & Liginlal 2007).

Social pressure refers to protecting socially desirable information in e-government services. The privacy, trust, and quality of services, for example, are social desirable needs that must be adequately addressed in e-government services. It can be measured through employees' perception of the (a) consequences of failure to meet social obligations and commitments (Beautement et al. 2009; Kam et al. 2013; Puhakainen & Siponen 2010), (b) degree of citizen's reliance on technological services, and (c) degree of efforts put in by public organisations to fortify information in e-government systems to build citizens' confidence (Kam et al. 2013). These social pressures put public organizations in the spot light, making them conscious of the need to maintain the trust of citizens, and preserve their reputation as a responsible public entity in protecting citizen's information (Gunningham & Kagan 2005; Zhang et al. 2005). Kam et al. (2013), for instance, found that stakeholders' expectation of information security generates pressures in organizations to strengthen their information security practices. Many studies on information security conclude that stakeholders' demands play an important role in improving the compliance behaviour of employees in public organizations (Appari et al. 2009; Delmas & Toffel 2008). This leads to the following hypotheses.

H5: Social pressure positively moderates the relationship between management commitment and information security compliance: the higher the social pressure, the greater the management commitment towards information security compliance.

H6: Social pressure positively moderates the relationship between accountability and information security compliance: the higher the social pressure, the greater the accountability impact on information security compliance.

H7: Social pressure positively moderates the relationship between information security awareness and information security compliance: the higher the social pressure, the greater employees' awareness of information security.

4. RESEARCH METHODOLOGY

This study aims to validate the hypothesised model for information security compliance in public organizations for e-government development. To test the hypotheses, a web-based survey and a paper-based survey were used for data collection. The survey questionnaire was initially tested for content and construct validity with experts in the field of information security and academics in information systems. The identified constructs were measured using items from the related literature.

The survey questionnaire consists of two parts. The first part was to capture participants' background, such as years of working experience in public organisations, job function, educational background, gender, and other demographic information. The second part was to solicit the perception of respondents on the relative importance of identified information security compliance factors. A seven point Likert scale was used to obtaining respondents' assessments (Miller 1987) of a range of information security compliance items, with "7" denoting 'highly important' and "1" representing 'not important at all'. The sample population is comprised of the public organizations that had undertaken e-government projects in Oman.

The survey was conducted by hosting an online survey using the university Qualtrics application. Over a thousand invitations were sent to employees of public organisations offering e-government services in Oman via emails, messages in social media groups, and phone text messages with a link to the survey site. To boost response rate, about 300 paper-based survey questionnaires were also randomly distributed to employees in the targeted public organisations in Oman. 326 responses were received. 32 responses with missing data and aberrant responses were excluded, yielding a total of 294 completed questionnaires for the analysis.

5. RESULTS AND FINDINGS

To validate the measurement model, the constructs are assessed based on (a) the reliability of the construct used in the model, (b) the convergent validity, (c) the discriminant validity, and (d) the adequacy of the model fit. To test the reliability of the constructs, Cronbach's alpha was used. The results show that all constructs have α values exceeding 0.7, indicating high construct reliability. The convergent validity test for a single factor was confirmed by examining both the average variance extracted (AVE) and the factor loadings of the indicators associated with each construct. The results indicate that three of the five latent factors (Management Commitment, Information Security Awareness, and Social pressure) have AVE values equal to or exceeding the threshold value of 0.5, while two (Accountability and Information Security Compliance) just marginally miss the 0.5 threshold value. In a strict sense, these two factors do not achieve convergent validity (Fornell & Larcker 1981). However, the factor loadings of all five latent factors range from 0.59 to 0.86 and are all statistically significant at p = 0.05. We thus argue that the presence of convergent validity is supported (Bagozzi et al. 1991). Lastly, the discriminant validity test of single factor model is assessed by comparing the square root of the AVE for each construct against the inter-construct correlation estimates (Fornell & Larcker 1981). The result shows the square root of the AVE of each construct is higher than its correlation with other constructs (Management Commitment =0.711, Accountability =0.7, Information Security Awareness =0.707, Social Pressure =0.775, and Information Security Compliance =0.7), indicating the discriminant validity (Fornell & Larcker 1981).

The goodness-of-fit (GOF) measures is used to assess each single-factor model for their validity with various fitness indices, such as normed chi-square ($\chi 2$ /d.f.), normed fit index (NFI), non-normed fit index (NNFI), comparative fit index (CFI), goodness of fit index (GFI), standardized root mean square residual (SRMR), and root mean-square error of approximation (RMSEA). Table 1 presents the GOF strength for each single-factor model indicating a good fit with the collected data.

	No. of Items	**x/df <3**	**P >.05**	**CFI >.95**	**GFI >.95**	**AGFI >.80**	**SRMR <.09**	**RMSEA <.05**	**PCLOSE >.05**
MC	4	0.655	0.519	1	0.998	0.989	0.0108	0.00	0.716
Acc	4	1.992	0.136	0.994	0.993	0.966	0.0211	0.058	0.330
ISA	3	0.014	0.907	1	1	1	0.0015	0.00	0.936
SocPres	3	0.032	0.858	1	1	1	0.0016	0.00	0.901
InfoSecCom	3	0.287	0.592	1	0.999	0.996	0.0071	0	0.708

Table 1. The GOF Results

Following the reliability and validity assessment, the hypotheses were tested using the hierarchal regression technique. Hierarchical regression is used to understand the constructs associations and variation. It is used to examine specific theoretically based hypotheses (Petrocelli 2003). As shown in Table 2, four of six hypotheses indicated in the conceptual model are supported. Management commitment has a significant effect on information security compliance (standardized path coefficient = 0.18, $p < 0.01$), supporting H_1. Both accountability (standardized path coefficient = 0.24, $p < 0.01$) and information security awareness (standardized path coefficient = 0.18, $p < 0.01$) are also found to have a significant effect on information security compliance, thus supporting H_2 and H_3, respectively. The results also indicate that social pressure has a significant effect on information security compliance (standardized path coefficient = 0.25, $p < 0.01$).

Mixed findings are obtained on the moderating role of the social pressure. Of the three interaction effects tested, only that between social pressure and accountability was found to be statistically significant. This result supports H_6, which postulates that the higher the social pressure is, the greater the effect accountability has on information security compliance. Because the interaction effects of social pressures with management commitment and social pressures with awareness on information security compliance are not found to be statistically significant, hypotheses H_5 and H_7 cannot be supported. Overall, the model explained approximately 48 percent of the variance in information security compliance.

	Base Model	Model 1	Model 2	Model 3
Control Variables				
Medical and Health Care Organizations[1]	0.03	0.03	0.03	0.03
IT Organizations[1]	-0.07	0.00	-0.00	-0.01
Financial Organizations[1]	0.04	-0.03	-0.03	-0.03
Main Effects				
Management Commitment (MC)		0.21***	0.18***	0.20***
Accountability (ACC)		0.31***	0.24***	0.22***
Information Security Awareness (ISA)		0.22***	0.18***	0.18***
Social Pressures (SP)			0.25***	0.23***
Interaction Effects				
SP x MC				-0.09
SP x ACC				0.19***
SP x ISA				0.06
R^2	0.01	0.42	0.47	0.48
ΔR^2	0.01	0.41	0.06	0.01
F-value for ΔR^2	0.92	35.11	36.01	26.33

Note: 1. Dummy variable * $P<0.1$; ** $p< 0.05$; *** $P<0.01$ All regression coefficients indicated are standardized β values.

Table 2. Results of Hierarchical Regression

6. DISCUSSION

This study shows that organizational security culture, defined by management commitment, accountability, and information security awareness has a positive effect on information security compliance. Specifically, the results show that management commitment could increase information security compliance in public organizations. Management commitment could take the form of (a) providing active support through firmed decisions, investments and actions taken to enforce information security policy across the whole organization, (b) visible involvement in dealing with organization's information security issues through active participation, and (c) aligning the goals of information security policy with other organizational goals to increase employees' belief on the value of compliance with information security policies and procedures.

Accountability deals with the organizational security culture that inculcates individuals to take responsibility towards information security compliance. Existing research (Herath & Rao 2009; Posthumus & Von Solms 2004) considers accountability the most effective elements for building a strong organizational security culture that changes employees' attitudes towards information security compliance. The results of the study confirm that accountability has a significant impact on information security compliance. This suggests that less stringent enforcement may lead to insufficient security policies being designed for protecting information. In light of the findings, organizations should pay special attention to establishing a comprehensive set of rules and procedures in a sufficiently clear and detailed manner to

guide appropriate information security behaviour in organizations. This obligates individual employees to be more proactive in undertaking higher information security precautions and not inadvertently breaching security policies.

Raising employees' knowledge and understanding information security policies and mechanisms in organizations is critical for information security compliance (Smith & Jamieson 2006; Tsohou et al. 2015). The results indicate that the awareness of information security has a significant effect on information security compliance. This result and the supporting literature confirm the importance of awareness of security issues in influencing and shaping the attitudes and behaviour of employees towards information security compliance. This suggests that employees in public organizations should be aware of (a) the security risks and cyber threats faced, (b) the responsibilities associated with having security policies and practices put in place to address these risks, and (c) the costs and consequences of information security breaches. The findings also hint at the design of an organisation's security awareness programs should be tailored to reflect the organisation's circumstances and commensurate with the nature of the organisation's operations.

The significance of social pressure on information security compliance is also confirmed in the study. Social pressures can motivate public organizations to put in extra efforts to maintain citizens' trust, and preserve public organization's reputation in protecting citizen information (Gunningham & Kagan 2005; Zhang et al. 2005). The significance of social pressure in moderating the strength of the relationship between accountability and information security compliance confirms the assumption that the higher the social pressure, the greater is the effect of accountability on information security compliance. The insignificant moderating effects of social pressure on the relationships between management commitment and information security compliance as well as between information security awareness and information security compliance, on the other hand, suggest that the effects of management commitment and employees' information security awareness are not dependent on the presence (or absence) of social pressures. Strong management commitment in enforcing information security measures would lead to a greater level of information security compliance within public organisations, regardless of the prevalence of social pressures. The same is true of the impact employees' information security awareness has on information security compliance.

Overall, the results of the study are in line with those of existing research on information security compliance. The findings underscore the importance of building an information security culture within organisations to promote information security compliance. The contributing role of social pressures in moderating the relationships between the three latent constructs representing information security culture and information security compliance is limited: social pressures only have an influence in boasting the effect of accountability on information security compliance.

7. CONCLUSION

Effectively information security management in public organizations is important to the success of e-government development because it directly increases the confidence and trust of e-government stakeholders (Ebrahim & Irani 2005). Such confidence and trust could help improve the quality of e-government services and facilitate further development of e-government (Karokola et al. 2012). This study has found that having an effective information security culture within public organizations could lead to higher levels of information security compliance. The findings based on the context of e-government development in Oman offer valuable insights on how information security compliance could be achieved.

Several limitations of our study can be addressed in future work. First, some other tangible measures of information security compliance could be considered. For instance, physical monitoring of employee information security behaviour at work over a period of time could be used as an assessment of the effectiveness of an information security mechanism put in place to improve information security compliance in public organizations. Second, this study only collected data from employees in public organizations. It had not survey other e-government stakeholders, such as private citizens and businesses. Third, additional factors could be included to further explore the antecedents of information security compliance in public organizations. In particular, further studies should consider incorporating technological factors that can help to enforce information security policies toward information security compliance (Venter & Eloff 2003).

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

AlKalbani, A., Deng, H., & Kam, B. (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development.

Appari, A., Johnson, M. E., & Anthony, D. L. (2009). HIPAA Compliance: An Institutional Theory Perspective. Paper presented at the AMCIS.

Backes, M., Pfitzmann, B., & Waidner, M. (2003). Security in business process engineering *Business Process Management* (pp. 168-183): Springer.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. Administrative science quarterly, 421-458.

Barling, J., Loughlin, C., & Kelloway, E. K. (2002). Development and test of a model linking safety-specific transformational leadership and occupational safety. Journal of Applied Psychology, 87(3), 488.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. Logistics Information Management, 15(5/6), 337-346.

Basu, S. (2004). E‐government and developing countries: an overview. International Review of Law, Computers & Technology, 18(1), 109-132.

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. Paper presented at the Proceedings of the 2008 workshop on New security paradigms.

Benabdallah, S., Gueniara El Fatmi, S., & Oudriga, N. (2002). Security issues in E-government models: what governments should do? Paper presented at the Systems, Man and Cybernetics, 2002 IEEE International Conference on.

Boss, S., & Kirsch, L. (2007). The last line of defense: motivating employees to follow corporate security guidelines. Paper presented at the Proceedings of the 28th International Conference on Information Systems.

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.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3), 18-41.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361.

Conklin. (2007). Barriers to Adoption of e-Government. Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Delmas, M. A., & Toffel, M. W. (2008). Organizational responses to environmental demands: Opening the black box. Strategic Management Journal, 29(10), 1027-1055.

Deng, H. (2008). Towards objective benchmarking of electronic government: an inter-country analysis. Transforming Government: People, Process and Policy, 2(3), 162-176.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio‐organizational perspectives. Information Systems Journal, 11(2), 127-153.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American sociological review, 147-160.

Duan, X., Deng, H., & Corbitt, B. (2012). Evaluating the critical determinants for adopting e-market in Australian small-and-medium sized enterprises. Management Research Review, 35(3/4), 289-308.

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. Business Process Management Journal, 11(5), 589-611.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. Computers & Security, 19(3), 243-256.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research, 382-388.

Gunningham, N., & Kagan, R. A. (2005). Regulation and business behavior*. Law & Policy, 27(2), 213-218.

Hayes, S. C. (2004). Acceptance and commitment therapy, relational frame theory, and the third wave of behavioral and cognitive therapies. Behavior therapy, 35(4), 639-665.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.
Ifinedo, P. (2013). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information & Management(0).
Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2007). Senior executives commitment to information security–from motivation to responsibility *Computational Intelligence and Security* (pp. 833-838): Springer.
Kam, H.-J., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective. PACIS 2013 Proceedings.
Karokola, G., Yngstrom, L., & Kowalski, S. (2012). Secure e-government services: a comparative analysis of e-government maturity models for the developing regions-the need for security services. International Journal of Electronic Government Research, 8(1), 1(25).
Karunasena, K., & Deng, H. (2012). Critical factors for evaluating the public value of e-government in Sri Lanka. Government information quarterly, 29(1), 76-84.
Khansa, L., & Liginlal, D. (2007). The Influence of regulations on innovation in information security.
Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.
Knorr, K., & Röhrig, S. (2001). Security requirements of e-business processes.
Kolkowska, E., & Dhillon, G. (2012). Organizational power and information security rule compliance. Computers & Security.
Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. Computer Communications, 26(16), 1873-1883.
Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413.
Martins, A., & Elofe, J. (2002). Information security culture: Springer.
McIlwraith, A. (2006). Information security and employee behaviour: how to reduce risk through employee education, training and awareness: Gower Publishing, Ltd.
Miller, D. (1987). Strategy making and structure: Analysis and implications for performance. Academy of management journal, 30(1), 7-32.
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.
Neubauer, T., Klemen, M., & Biffl, S. (2006). Secure business process management: A roadmap. Paper presented at the Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on.
Oost, D., & Chew, E. (2007). Investigating the Concept of Information Security Culture. University of Technology, Sydney School of Management Working Paper Series}, 1, 12.
Petrocelli, J. V. (2003). Hierarchical multiple regression in counseling research: Common problems and possible remedies. Measurement and evaluation in counseling and development, 36(1), 9-22.
PonemonInstitute. (2013). Cost of Data Breach Study: Global Analysis.
Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646.
Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 34(4), 757-778.
Ryan. (2004). Information security tools and practices: what works? Computers, IEEE Transactions on, 53(8), 1060-1063.
Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 19(3), 122-131.
Siponen, Pahnila, & Mahmood. (2007). Employees' adherence to information security policies: an empirical study *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 133-144): Springer.
Siponen, Pahnila, & Mahmood. (2010). Compliance with information security policies: An empirical investigation. Computer, 43(2), 64-71.

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. Information Systems Management, 23(2), 23-32. doi: 10.1201/1078.10580530/45925.23.2.20060301/92671.4
Straub Jr, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.
Tassabehji, R., Elliman, T., & Mellor, J. (2007). Generating Citizen Trust in E-Government Security: Challenging Perceptions. International Journal of Cases on Electronic Commerce (IJCEC), 3(3), 1-17.
Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: a test of competing models. Information Systems Research, 6(2), 144-176.
Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). The processes of technological innovation (Vol. 273): Lexington Books Lexington, MA.
Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58.
Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. Information Security Journal: A Global Perspective, 17(5-6), 207-227.
Venter, H., & Eloff, J. H. (2003). A taxonomy for information security technologies. Computers & Security, 22(4), 299-307.
Von Solms. (2005). Information security governance–compliance management vs operational management. Computers & Security, 24(6), 443-447.
Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.
Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 20(3), 267-284.
Wimmer, M., & Von Bredow, B. (2002). A holistic approach for providing security solutions in e-government. Paper presented at the System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on.
Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing. Journal of Enterprise Information Management, 18(5), 548-567.
Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. Government information quarterly, 28(2), 239-251.