A Conceptual Framework for Information Security in Public Organizations for E-Government Development

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

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

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

Abstract

The rapid development of e-government across the world has exposed critical information in public organizations to the possibility of cybercrime. Information security has become a critical issue that needs to be adequately addressed in e-government development. This paper proposes a conceptual framework for information security compliance. The proposed framework, consisting of four dimensions - organizational security culture, operational process, technology, and environment - was validated using semi-structured interviews with security managers in public organizations involved in e-government development in Oman. This paper contributes to information security research by identifying the critical factors for adopting an information security compliance approach to increase information security for e-government development in public organizations.

Keywords

E-government, information security, information security compliance, critical factors

INTRODUCTION

Despite rapid advances in information and communication technologies (ICTs), information security remains one of the most vexing issues confronting ICT professionals. As greater attempts are made to leverage the prowess of ICTs to transform government services to make them more accessible, effective and accountable (Karunasena and Deng 2012), protecting the confidentiality, integrity, availability, authenticity, and accountability of information has become a critical issue in electronic government (or e-government) development (Karokola et al. 2012). The many unprecedented opportunities e-government development have created for governments to interact with its stakeholders have, at the same time, exposed critical information in e-government systems to the possibility of cybercrime (Tassabehji et al. 2007), which directly affects the confidence and trust of e-government users (Ebrahim and Irani 2005). Such confidence and trust are important to the continued improvement of e-government service quality and the evolvement of new forms of e-government services (Karokola et al. 2012).

Enforcing information security compliance, i.e., implementing information security standards and policies, to adequately protect organizational information has been on the rise in recent years (Boss and Kirsch 2007; Siponen et al. 2010). Information security compliance ensures that information security mechanisms can work together effectively (Neubauer et al. 2006). Adopting a compliance approach not only satisfies the security requirements of public organizations for e-government services, but also increases user confidence and trust. Information security compliance is widely acknowledged as an effective means to ensure information security in public organizations (Herath and Rao 2009).

Many studies have examined issues relating to information security compliance. Bulgurcu et al. (2010), for example, investigate the role of information security awareness on users' attitudes towards complying with information security requirements. Hazari et al. (2008) explore behavioural issues on information security compliance in organizations. Sasse et al. (2001) analyze employees' interactions with information security mechanisms to achieve information security compliance. These studies, however, tended to focus primarily on factors related to users' attitudes and behaviours in information security compliance in public organizations. Little attempt has been made to develop a comprehensive framework to address information security compliance in public organizations.

This paper proposes a conceptual framework for adopting information security compliance in public organizations for e-government development. Four dimensions of information security compliance are considered: organizational security culture, operational process, technology, and environment. The proposed framework highlights the critical factors for adopting an information security compliance framework in public organizations for e-government development. It is validated using semi-structured interviews with security managers in public organizations involved e-government development in Oman.

INFORMATION SECURITY FOR E-GOVERNMENT DEVELOPMENT

E-government has created new ways of interactions between government organizations and citizens in the delivery of public services. These interactions have necessitated the need for maximum information protection. In general there are five broad requirements of information security in e-government: confidentiality, integrity, availability, authenticity, and accountability (Zissis and Lekkas 2011). Confidentiality means protecting information from unauthorized disclosure by assuring that information is shared only among authorized users. Integrity concerns the accuracy of the information, including maintaining its origin, completeness, and correctness. Availability implies allowing information to be accessed by the right people at the right time. Authenticity refers to the legitimacy of data involved in transactions, communications, and documentation. Accountability suggests that all actions compromising e-government security can be traced back to the responsible party.

Developing effective information security practices requires an adequate consideration of both the technological perspective and the socio-organizational perspective (Bulgurcu et al. 2010; Dhillon and Backhouse 2001). McIlwraith (2006), for example, considers three main aspects for effective information security in organizations. The first aspect is having a trusted technical infrastructure system that can secure transactions, protect access to information, and fence off hacker attacks. The second aspect is establishing reliable internal processes to efficiently execute information security controls. The third aspect is developing a good corporate security culture that promotes positive individual attitude and behaviour towards information security controls.

Considerable efforts have been made to design and develop frameworks for ensuring information security in organizations. Da Veiga and Eloff (2010), for example, propose an information security culture framework to heighten information security awareness in organizations. Posthumus and Von Solms (2004) develop an information security governance framework. Martin et al. (2011) recommend a total quality management based framework to manage information security in organizations. These studies have shown the merits of individual frameworks for maintaining information security in organizations from different perspectives. They, however, have not investigated the critical factors affecting information security compliance. To address this gap, this study seeks to develop, and empirically validate, a compliance-based conceptual framework to manage information security in public organizations for e-government development.

INFORMATION SECURITY COMPLIANCE

Information security compliance refers to the effective implementation of information security standards and policies for protecting information in public organizations (Von Solms 2005). It is fast becoming an institutional yardstick, signalling adequate steps have been taken to protect organizational information (Boss and Kirsch 2007; Siponen et al. 2010). Information security compliance signifies that different information security aspects are working together effectively (Neubauer et al. 2006; Von Solms 2005), and information security mechanisms are operating (Siponen et al. 2010). Information security compliance is evidence of meeting security and privacy requirements in organizations, and non-compliance to information security standards and policies has been a main reason for security breaches (Herath and Rao 2009; Ullah et al. 2013).

There are several recent important developments in the literature of information security compliance in public organizations. Lee et al. (2004), for example, investigate the use of sanctions to increase information security compliance. Siponen et al. (2010) identify factors, including normative beliefs, threat appraisal, self-efficacy, and visibility, that influence employees' intention to comply with information security policies. Ifinedo (2013) proposes a framework for complying with information security policy in organizations from the perspective of (a) socialization, (b) social influence, and (c) cognition. Majority of these studies have focused primarily on factors related to users' attitudes and behaviours in information security compliance. Few have explored factors contributing to promoting information security compliance in public organizations relating to e-government development. This paper proposes a conceptual framework for the adoption of information security compliance in public organizations on e-government development.

THE INFORMATION SECURITY COMPLIANCE FRAMEWORK

This study draws on two established theories - Technology-Organization-Environment (TOE) theory (Tornatzky et al. 1990), and institutional theory (DiMaggio and Powell 1983) – to examine information security compliance. TOE argues that the process by which technological innovations are adopted and implemented in organizations is conspired by the technological, organizational, and environmental contexts surrounding their operations (Tornatzky and Fleisher 1990). These three sets of factors present "both constraints and opportunities for technological innovation" (Tornatzky and Fleisher 1990, p. 154), shaping the manner in which a firm appraises its need for, explores the options for, and embraces new technology.

In the context of information security compliance, the technological context refers to the reliability of existing and new security technologies capable in satisfying the requirements of information security policies and standards to improve information security compliance by cementing user trust and confidence in using e-government (Wimmer and Von Bredow 2002). The organization aspect describes the characteristics, such as communication process and top management championship for promoting organizational security culture that steer employees' intentions and behaviours towards information security compliance. A well-developed organization culture on information security directly affects the behaviours of employees in complying with information security standards and policies in public organizations (Dhillon and Backhouse 2001; Sasse et al. 2001). As for the environmental context, institutional theory has been applied to study environmental pressure on adoption of innovation in e-commerce (Gibbs and Kraemer 2004; Kankanhalli et al. 2003).

Institutional theory posits that organizations must secure legitimacy from stakeholders by conforming to external expectations (DiMaggio and Powell 1983). These external expectations are classified into three archetypes: regulative expectation, normative expectation, and cognitive expectation (Scott 2013). For information security compliance, these external expectations impose pressures on public organizations to initiate internal organizational efforts to meet information security requirements. Operational process is a distinctive aspect considered in this research, it refers to the reliable internal processes that influence the acceptance of information security mechanisms in organizations. Information security processes and the way in which they are presented, integrated, and enforced are a fundamental leverage point for effective information security compliance. Figure 1 shows the research framework with the identified aspects and their associated attributes.

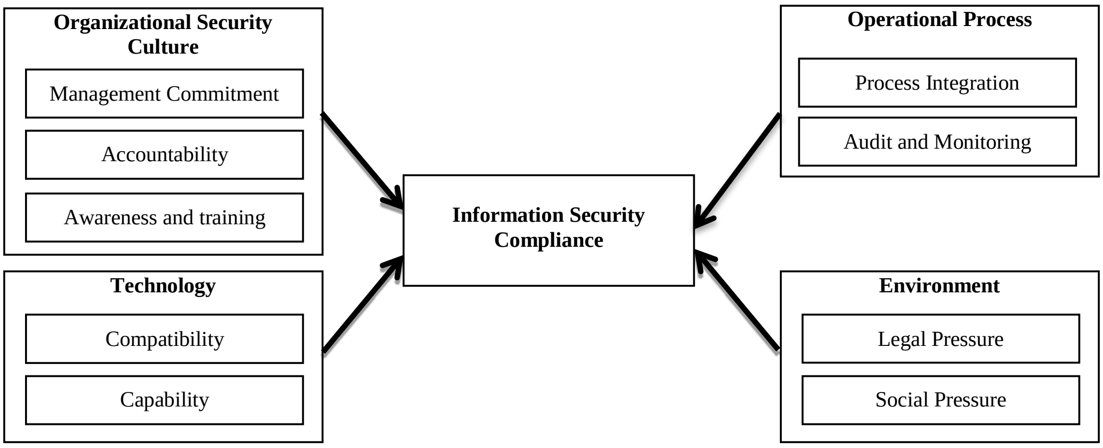

Figure 1: An Information Security Compliance Framework

Organizational Security Culture

Organizational security culture refers to the belief of individual employees on the value of compliance with information security standards and policies (McIlwraith 2006). According to Von Solms (2000) security culture is "to be created in a company by instilling the aspects of information security to every employee as a natural way of performing his or her daily job" (p618) (Oost and Chew 2007). Extant literature on information security suggests that there are three major factors affecting the establishment of an adequate organizational security culture for information security compliance: management commitment, accountability, and awareness and training (Bulgurcu et al. 2010; Herath and Rao 2009; Kajava et al. 2007).

Management commitment centers on the efforts of senior management to promote information security compliance (Kajava et al. 2007). It is a key driver that influences the adoption of information security compliance in public organizations (Smith and Jamieson (2006) and requires visible participation, ongoing communication and championing to stimulate employees' intentions towards information security compliance (Kolkowska and Dhillon 2012). Knapp et al. (2006) show that without top management support and involvement, the creation, training and enforcement of organization's security policies would not be taken seriously. In fact, a common reason cited for the weak implementation of information security policies in organization is the lack of management support to encourage adherence to information security policies (Knapp et al. 2006; Kolkowska and Dhillon 2012).

Accountability deals with organizational security culture that promotes individuals' responsibility towards enforcing information security in organizations (Herath and Rao 2009). It is one of the most effective elements for building a strong organizational security culture to change employees' attitudes towards information security compliance (Posthumus and Von Solms (2004). If stipulated sanctions are not enforced accordingly, individuals would not expect any consequences when caught breaching information security policies (Adams and Sasse (1999). Individuals with well-defined roles and responsibilities are more proactive in terms of undertaking higher information security precautions (Ryan 2004). Awareness and training stresses the importance of having information security programs in place to raise user's knowledge and understanding of security policies and mechanisms in organizations. Awareness is a critical factor for information security compliance (Smith and Jamieson 2006). Bulgurcu et al. (2010) for example, point out that information security awareness highly affects employee's beliefs about the benefit of compliance and the cost of non-compliance. According to Puhakainen and Siponen (2010), employees' security awareness can lead to a better compliance with information security policies after understanding the benefits and the value of information security in their organization. Many studies use information security awareness and training to develop effective security culture in organizations to reduce the misuse intentions and to increase users' avoidance of information security risks and threats (Bulgurcu et al. 2010; Puhakainen and Siponen 2010; Tsohou et al. 2008).

Operational Process

Developing appropriate processes to enhance information security in organizations could result in efficient execution of information security controls (Knorr and Röhrig 2001). Vroom and Von Solms (2004), for example, assert that compliance with information security policies can be improved if employees integrate information security mechanisms in their daily work practices. Kong et al. (2012) state that information security mechanisms can increase business performance in organizations, leading to the acceptance of these mechanisms. Extant literature indicates that process integration as well as auditing and monitoring are two of the most important factors affecting information security compliance.

Process integration implies mapping information security mechanisms into business processes (Backes et al. 2003) to support business objectives. Backes et al. (2003) have shown that integrating security requirements into the development of organizational processes can improve information security. Knorr and Röhrig (2001) provide a framework that uses business processes for facilitating the implementation of information security mechanisms. Beautement et al. (2009) provide a compliance based approach for improving the organizational process for information security. These studies have shown that security mechanisms must be designed as an integral part of the operation processes in order to be effective and efficient.

Auditing and monitoring processes deals with visibility of information security compliance in organizations (Neubauer et al. 2006). These processes, when appropriately enforced, could raise the speed of business operational execution and improve the overall effectiveness of information security mechanisms (Neubauer et al. 2006; Ransbotham and Mitra 2009). Steinbart et al. (2012), for instance, find that auditing and monitoring processes improve users' performance that leads to increased acceptance of information security mechanisms. Kolkowska and Dhillon (2012) assert that auditing and monitoring processes could push employees toward information security compliance.

Technology

Technologies provide the technical means that can be adopted to strengthen information security. It always play a critical role by providing organizations with secured transactions, protected access to information, and defence against hacker attacks (Venter and Eloff 2003). Effective information security in organizations mandates a reliable and secure technology infrastructure that conform to information security policies requirements (Huang and Bwoma 2003). Venter and Eloff (2003) point out that adopting adequate security technologies can help enforce policies, monitor and alert violations, and strengthen information protection. From existing literature, two technology factors influencing information security compliance were identified: technological compatibility and technological capability.

Technology compatibility is the ability of the security technologies to enforce the security requirements over operational technologies (Smetters and Grinter 2002). It is an essential element influencing the adoption of technical information security mechanisms (Smetters and Grinter 2002). Kaliontzoglou et al. (2005), for example, assess the effectiveness of different security technologies, such as digital signature, in enforcing security requirements over the Web portal technology. Wimmer and Von Bredow (2002) emphasise the need of technical information security standards to avoid e-government incompatibility, such as misfit between current work practices and security mechanisms and misalignment with individual's values and experience in using security technologies.

Technology capability refers to the ability to fulfil technical security requirements (Tudor 2001). It has an effect in increasing user trust and confidence, leading to greater information security compliance (Moynihan 2004; Wimmer and Von Bredow 2002). Technology capability also assists organizations to fulfil information security policy requirements, such as capabilities and usability of specific security technology, and reliability to detect and prevent information security threats and vulnerabilities. Lambrinoudakis et al. (2003), for example, utilize the Public Key Infrastructure technology services to satisfy most of e-government platform security requirements, such as authentication, authorization and integrity. Other studies assert that technology capability could improve the normal functioning of e-government systems by reducing security risks (Ebrahim and Irani 2005; Lambrinoudakis et al. 2003).

Environment

Environment relates to external pressures that force public organizations to attain information security compliance. Such pressures initiate internal organization efforts toward information security (Chang and Ho 2006; Herath and Rao 2009; Karunasena and Deng 2012). Existing research (e.g., Khansa and Liginlal 2007) on information security has shown that environmental pressures could propel organizations to integrate information security mechanisms into their daily practices by motivating managers and employees to comply with information security practices. In general, two environmental factors affecting information security compliance are identified: legal pressure and social pressure.

Legal pressure is the coercive pressure from the governments' regulatory agency that compels public organizations to comply with information security policies and standards. This pressure forces public organizations to incorporate legal requirements in information security practices for meeting any legal obligations (Khansa and Liginlal 2007). Hu et al. (2007) assert that regulatory pressure shapes and motivates managers and employees in organizations to comply with information security requirements. Other studies also conclude that regulative pressure is a critical environmental factor that has an immense influence on information security compliance in public organizations (Guarda and Zannone 2009; Torres et al. 2006).

Social pressure refers to protecting socially desirable information in e-government services. The need to protect desirable information coerces public organizations to strive to maintain the trust of citizens, and preserve public organization's reputation as a responsible entity in guarding citizen information (Gunningham and Kagan 2005; Zhang et al. 2005). Kam et al. (2013) assert that the stakeholders' expectation of information security generates pressures in organizations to strengthen their information security compliance. Many studies on information security compliance conclude that stakeholders' demands play an important role in improving the compliance behavior of employees in public organizations (Appari et al. 2009; Delmas and Toffel 2008).

RESEARCH METHODOLOGY

This study uses a qualitative approach to demonstrate the validity of the proposed conceptual framework in ensuring information security compliance in public organizations for e-government development. It explores the questions of how information security compliance can be ensured in public organizations and how the existing practices of information security can be improved in public organizations. The interview questions were developed based on a comprehensive review of the related literature and are divided into three parts. The first part focuses on the demographic information of the interviewees. The second part comprises general questions on the practices for ensuring information security in public organizations. The third part contains specific questions on factors influencing information security compliance in public organizations. The interview questions were pretested with the help of academics, higher degree research scholars, and information security practitioners. Nine semi-structured interviews were conducted with information security managers from different Omani public organizations to confirm the validity of the proposed conceptual framework. Interviewees were selected based on their knowledge, experience and roles in information security.

Thematic analysis technique was used to analyze the interview data. Specifically, this study employed the theory-driven thematic analysis by deriving deriving themes based on pre-existing theoretical concerns (Howitt 2010) summarized in Figure 1. Following (Howitt 2010), underlying dominant themes, i.e., information which repeatedly appears within the data set, were identified to generate insights, and reveal similarities and differences between the responses of the interviewees.

RESEARCH FINDINGS

Table 1 summarizes the research findings around the four dimensions identified in the proposed framework, namely, organizational security culture, operational process, technology, and environment. Each dimension consists of factors that have been identified in the semi-structured interviews.

Table 1. Information security compliance factors

Dimension	Factors	Sub-Factors	Corroborative Evidence
Organizational Security Culture	Management Commitment	Active support, Involvement, Goals alignment, Ongoing communication, raising loyalty	*"A robust, comprehensive documented security policy does not guarantee enforcement without executive commitment"* *"if senior management makes information security a known priority, government agencies can then reap the benefits of information security activities"*
	Accountability	Policies in place, Defined roles and responsibilities, Appropriateness of sanctions	*"the more the employee information security tasks are defined, the easier it is to determine inappropriate behaviour"*
	Awareness and training	Effectiveness, Usefulness, Visibility	*"it is important for information security to be communicated in an educated way that enables employees to understand and follow its requirements. One way to do this is by setting up an ongoing awareness campaigns across the organization"*
Operational Process	Process Integration	Design and implementation of the security controls, Improvement of performance and productivity, Conformity with users	*"the security controls must demonstrate its efficiency in integrating with users daily operational tasks"*
	Audit and monitoring	Appropriateness of auditing and monitoring activities, Perceived benefits, Responsiveness	*"Auditing tasks guide your information security in organizations. Having well designed auditing processes in place would improve the overall security"*
Technology	Compatibility	Appropriateness, Interoperability, Perceived impact	*"Three important issues when it comes to security technology compatibility, compatibility with preferred work, compatibility with existing work practices, and compatibilities with values"*
	Capability	Reliability, Ease of use, Easy to setup, Availability	*"the more flexible the security technology, the more it is accepted, particularly amongst the technical support team"*
Environment Pressure	Legal pressure	Laws and regulation, Severity of violation, Governance of Law	*"the increased intervention of regulatory agencies can force organizations to comply with information security"* *"Currently, we hear of many cases in courts that are related to information security. This has created huge pressure on organizations to take precautions' with their information"*
	Social pressure	Security and privacy commitment, Knowledge and understanding, Trust	*"most citizens in Oman are using social media to drive their requirements over public organizations"* *"The government has considered security as an integrated part of the e-service quality. Consequently, this obligation has created enormous social pressures on public organizations to secure citizen's information"*

Organizational Security culture

The nine interview transcripts unanimously confirm that building positive and strong security culture motivates individual employees towards information security compliance. They also indicate that the more security minded an organization is, the less friction compliance with information security policies would create. The results of the thematic analysis further suggest that organizational security culture is underscored by three factors - management commitment, accountability, and awareness and training. Each factor also extends further into a number of sub-factors that influence information security compliance in public organizations.

Management commitment refers to the efforts of senior management in supporting information security compliance. Interviewees concurred that senior management commitment can influence individual employees to comply with information security policies in their organizations. Having senior management's (a) active support in decisions making, investments and action taken for enforcing the information security policy across the organization, (b) involvement in maintaining organization's information security issues, (c) push to align the goals of information security policy with the organizational goals, (d) raising employees' loyalty using pride, respect, gratitude, and ownership strategies, and (e) ongoing communication of information security policies and procedures across the organization are prime motivations which could increase the belief, and value of individual employees' on compliance with information security policies and procedures. A majority of the interviewees stressed that employees' behaviour in the organization can be influenced by their superior because people tend to follow what other people do or what they have been told, either positively or negatively. An interviewee explained:

> *"… active support of senior management is vital for information security, as employees within that organization generally live by example.."*

Another factor unearthed under the organizational security culture is accountability. This factor creates an organizational environment that inculcates individuals to take responsibility towards information security compliance. Imposing accountability for information security practices in organizations was widely believed by interviewees that it could change employees' behaviour to comply with information security policy. Participants fully agreed that individuals with well-defined roles and responsibilities are more proactive in terms of undertaking higher information security precautions. The clarity of roles and responsibilities and the appropriateness of sanctions are highlighted as important factors that could generate an impact on changing employees' intentions to comply with information security policy. Interviewees added that employees' must believe their noncompliance with information security policies would be detected and sanctions would be applied. As the following interview transcript suggets, due to the missing accountability, some employees' violated existing information security policies.

> *"...If we want to minimize employees' omissive behaviour and policy violation, we have to CLEARLY clarify roles and responsibilities towards information security in organizations and then we can enforce sanctions across the organization..."*

Awareness and training is another important factor identified as an integral part of organizational security culture. Participants believed that it is important for organizations to maintain a functional pool of knowledge for employees to protect government information, especially when regular changes in the workforce are common. The interviewees also believed that raising awareness of risks and vulnerabilities faced by organizations increases the perceived benefits of employees' compliance. The interviews revealed that the effectiveness, usefulness, and visibility are desirable outcomes when conducting awareness and training programs in public organizations for e-government development. A majority of the interviewees stressed that if employees perceived usefulness in the design and implementation of awareness and training programs, they would exhibit compliance behavior and would attempt to avoid any deviant behavior that could harm their organization.

Operational process

Explicit alignment of information security controls with business processes was found to be a crucial element in reducing incidents and severity of security breaches, confirming that operational process is an important dimension influencing information security compliance in public organizations .Operational process was also found to be undergirded by two factors: efficient integration process, and audit and monitoring process. Each factor also includes a number of sub-themes that affect information security compliance in public organizations.

Interviewees indicated that misalignment of security controls with business processes introduces friction in organizations, which strikes at the heart of individual compliance issues. The most effective way to avoid this friction is to improve the design and integration of security controls. A majority of the interviewees further stressed that security control integration could provide employees and the organizations the benefits of improved performance and productivity. In the opinion of one interviewee:

> *"…in integrating efficiently the security controls with the business processes, organizations can move from a reactive mode of security management to proactive mode that can influence information security compliance through the operational processes…"*

Effectiveness of auditing and monitoring is another important element identified as having significant impact on information security compliance in public organizations. Interviewees stated that constant auditing and monitoring can be employed to compel employees to comply with information security policy, and to ensure the effectiveness of information security controls in public organizations. Most participants acknowledged that the appropriateness of the auditing and monitoring activities, and the perceived benefits of audit and monitoring processes increase its acceptance in organizations. They also mentioned that to increase the effectiveness of auditing and monitoring activities, management has to maintain a continuous responsive attitude towards the execution of auditing and monitoring requirements.

Technology

Technology is also confirmed as one of the four dimensions having a significant influence on information security compliance in public organizations. Interviewees identified two factors that reflect the influence of security technologies - technology compatibility, and technology capability - each of which also includes a number of sub-factors that influence information security compliance in public organizations.

Technology compatibility allows security technology to enforce security requirements across operational technologies. Interviewees believed that technologies that are very different in type, and sometimes very old, increase the complexity of information security controls in organizations. Interviewees pointed out that different information security compliance issues need to be addressed differently from the perspective of technology compatibility. These include the appropriateness of the security requirements, the interoperability of security technologies with the operational technologies, and the perceived impact in terms of technical cost. An interviewee, for example, stated that:

> *"….more technology compatibility is more reduction of technical burdens and cost that leads to information security acceptance"*

Another technology factor is the capability of the security technology. Interviewees held the view that technology capability increases employees' confidence and performance, which could lead to greater acceptance of security controls. Interviewees also confirmed that having diverse security technology capabilities could increase the flexibility of implementing information security controls in public organizations. All participants agreed that the reliability of the technology in detecting and preventing information security threats, the extent of ease-to-use and ease-to-setup, and the availability of technical support need to be met in order to increase the acceptance of technical security controls in organizations.

External environment

The interviews also established external environment as one of the four dimension influencing information security compliance. External environment was seen to comprise two factors that exert pressure on public organizations to comply with information security policy: legal pressure, and social pressure.

Legal pressure is a prime example of institutional pressure where law may place legal obligations on public organizations to satisfy information security requirements. Interviewees indicated that regulating agencies play a major role in enforcing regulations. The interviewees were also of the opinion that there should be an appropriate methodology for auditing information security compliance in public organizations to detect any legal violation.

Social pressure is another form of institutional pressure widely believed by interviewees to have a strong influence on information security compliance. The privacy, trust, and quality of services, for example, are a social desirable need that must be adequately addressed in e-government services. In this regard, a majority of the interviewees recognized that the current citizens' knowledge, understanding, and perception of information security issues, and social obligations create high pressure on public organizations to comply with information security standards and policies.

CONCLUSION

Effectively managing information security in public organizations is important to the success of e-government development. It increases the confidence and trust of e-government stakeholders. This paper has presented a conceptual framework for information security compliance consisting of four dimensions - organizational security culture, process, technology, and environment. These dimensions were investigated and validated using nine semi-structured interviews with officials knowledgeable about e-government development in different public organizations in Oman.

Rather than focusing predominantly on users' attitude and behaviours, the proposed framework extends current understanding of information security compliance in terms of the values of organizational security culture, operational process, technology, and environment to foster information security compliance in public organizations. It shed lights on aspects that have actually influenced information security compliance in public organizations. This framework is, to our best of knowledge, the first to investigate the role of organizational security culture, operational process, technology, and environment in influencing information security compliance in public organizations.

This study contributes to advancing current understanding of the critical factors influencing information security compliance in public organizations for e-government development. It suggests that to maintain information security compliance in public organizations, it is necessary to go beyond users' attitude and behaviour. This paper also contributes to e-government research both in theory and in practice. In theory, it has added a compliance-based framework to information security research. In practice, the proposed framework can be used as a guide to direct information security practitioners to focus on the tested dimensions of information security compliance. Since the framework was validated by nine in-depth interviews, its generalizability remains limited. A fruitful avenue for future research would be to test the proposed conceptual framework within the e-government context based on a large-scale quantitative survey.

REFERENCES

Adams, A., and Sasse, M. A. 1999. "Users are not the enemy," *Communications of the ACM* (42:12), pp 40-46.

Appari, A., Johnson, M. E., and Anthony, D. L. Year. "HIPAA Compliance: An Institutional Theory Perspective," AMCIS2009, p. 252.

Backes, M., Pfitzmann, B., and Waidner, M. 2003. "Security in business process engineering," in *Business Process Management*, Springer, pp. 168-183.

Beautement, A., Sasse, M. A., and Wonham, M. Year. "The compliance budget: managing security behaviour in organisations," Proceedings of the 2008 workshop on New security paradigms, ACM2009, pp. 47-58.

Boss, S., and Kirsch, L. Year. "The last line of defense: motivating employees to follow corporate security guidelines," Proceedings of the 28th International Conference on Information Systems2007, pp. 9-12.

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

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

Da Veiga, A., and Eloff, J. H. P. 2010. "A framework and assessment instrument for information security culture," *Computers & Security* (29:2) 3//, pp 196-207.

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

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

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

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

Gibbs, J. L., and Kraemer, K. L. 2004. "A Cross-Country Investigation of the Determinants of Scope of E-commerce Use: An Institutional Approach," *Electronic Markets* (14:2), pp 124-137.

Guarda, P., and Zannone, N. 2009. "Towards the development of privacy-aware systems," *Information and Software Technology* (51:2), pp 337-350.

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

Hazari, S., Hargrave, W., and Clenney, B. 2008. "An empirical investigation of factors influencing information security behavior," *Journal of Information Privacy & Security* (4:4), pp 3-20.

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

Howitt, D. 2010. *Introduction to qualitative methods in psychology*, (Prentice Hall New Jersey NJ.

Hu, Q., Hart, P., and Cooke, D. 2007. "The role of external and internal influences on information systems security–a neo-institutional perspective," *The Journal of Strategic Information Systems* (16:2), pp 153-172.

Huang, Z., and Bwoma, P. O. 2003. "An overview of critical issues of e-government," *Issues of Information Systems* (4:1), pp 164-170.

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., and Röning, J. 2007. "Senior executives commitment to information security–from motivation to responsibility," in *Computational Intelligence and Security*, Springer, pp. 833-838.

Kaliontzoglou, A., Sklavos, P., Karantjias, T., and Polemi, D. 2005. "A secure e-Government platform architecture for small to medium sized public organizations," *Electronic Commerce Research and Applications* (4:2), pp 174-186.

Kam, H.-J., Katerattanakul, P., Gogolin, G., and Hong, S. 2013. "Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective," *PACIS 2013 Proceedings*).

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An integrative study of information systems security effectiveness," *International Journal of Information Management* (23:2), pp 139-154.

Karokola, G., Yngstrom, L., and 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), p 1(25).

Karunasena, K., and Deng, H. 2012. "Critical factors for evaluating the public value of e-government in Sri Lanka," *Government Information Quarterly* (29:1), pp 76-84.

Khansa, L., and Liginlal, D. 2007. "The Influence of regulations on innovation in information security,").

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N. 2006. "Information security: management's effect on culture and policy," *Information Management & Computer Security* (14:1), pp 24-36.

Knorr, K., and Röhrig, S. 2001. "Security requirements of e-business processes,").

Kolkowska, E., and Dhillon, G. 2012. "Organizational power and information security rule compliance," *Computers & Security*).

Kong, H.-K., Kim, T.-S., and Kim, J. 2012. "An analysis on effects of information security investments: a BSC perspective," *Journal of Intelligent Manufacturing* (23:4) 2012/08/01, pp 941-953.

Lambrinoudakis, C., Gritzalis, S., Dridi, F., and Pernul, G. 2003. "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy," *Computer Communications* (26:16), pp 1873-1883.

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

Martin, C., Bulkan, A., and Klempt, P. 2011. "Security excellence from a total quality management approach," *Total Quality Management & Business Excellence* (22:3) 2011/03/01, pp 345-371.

McIlwraith, A. 2006. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*, (Gower Publishing, Ltd.

Moynihan, D. P. 2004. "Building Secure Elections: E-Voting, Security, and Systems Theory," *Public administration review* (64:5), pp 515-528.

Neubauer, T., Klemen, M., and Biffl, S. Year. "Secure business process management: A roadmap," Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, IEEE2006, p. 8.

Oost, D., and Chew, E. 2007. "Investigating the Concept of Information Security Culture," *University of Technology, Sydney School of Management Working Paper Series}* (1), p 12.

Posthumus, S., and Von Solms, R. 2004. "A framework for the governance of information security," *Computers & Security* (23:8), pp 638-646.

Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: an action research study," *Mis Quarterly* (34:4), pp 757-778.

Ransbotham, S., and Mitra, S. 2009. "Choice and chance: A conceptual model of paths to information security compromise," *Information Systems Research* (20:1), pp 121-139.

Ryan 2004. "Information security tools and practices: what works?," *Computers, IEEE Transactions on* (53:8), pp 1060-1063.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security," *BT technology journal* (19:3), pp 122-131.

Scott, W. W. R. 2013. *Institutions and organizations: Ideas, interests, and identities*, (Sage Publications.

Siponen, Pahnila, and Mahmood 2010. "Compliance with information security policies: An empirical investigation," *Computer* (43:2), pp 64-71.

Smetters, D. K., and Grinter, R. E. Year. "Moving from the design of usable security technologies to the design of useful secure applications," Proceedings of the 2002 workshop on New security paradigms, ACM2002, pp. 82-89.

Smith, S., and Jamieson, R. 2006. "Determining Key Factors in E-Government Information System Security," *Information Systems Management* (23:2) 2006/03/01, pp 23-32.

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. 2012. "The relationship between internal audit and information security: An exploratory investigation," *International Journal of Accounting Information Systems*).

Tassabehji, R., Elliman, T., and Mellor, J. 2007. "Generating Citizen Trust in E-Government Security: Challenging Perceptions," *International Journal of Cases on Electronic Commerce (IJCEC)* (3:3), pp 1-17.

Tornatzky, L. G., Fleischer, M., and Chakrabarti, A. K. 1990. *The processes of technological innovation*, (Lexington Books Lexington, MA.

Torres, J., Sarriegi, J., Santos, J., and Serrano, N. 2006. "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness," in *Information Security,* S. Katsikas, J. López, M. Backes, S. Gritzalis and B. Preneel (eds.), Springer Berlin Heidelberg, pp. 530-545.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008. "Investigating information security awareness: research and practice gaps," *Information Security Journal: A Global Perspective* (17:5-6), pp 207-227.

Tudor, J. K. 2001. *Information security architecture: an integrated approach to security in the organization,* (Auerbach.

Ullah, K. W., Ahmed, A. S., and Ylitalo, J. Year. "Towards Building an Automated Security Compliance Tool for the Cloud," Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, IEEE2013, pp. 1587-1593.

Venter, H., and Eloff, J. H. 2003. "A taxonomy for information security technologies," *Computers & Security* (22:4), pp 299-307.

Von Solms 2005. "Information security governance–compliance management vs operational management," *Computers & Security* (24:6), pp 443-447.

Von Solms, B. 2000. "Information security—the third wave?," *Computers & Security* (19:7), pp 615-620.

Vroom, C., and Von Solms, R. 2004. "Towards information security behavioural compliance," *Computers & Security* (23:3), pp 191-198.

Wimmer, M., and Von Bredow, B. Year. "A holistic approach for providing security solutions in e-government," System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on, IEEE2002, pp. 1715-1724.

Zhang, J., Dawes, S. S., and Sarkis, J. 2005. "Exploring stakeholders' expectations of the benefits and barriers of e-government knowledge sharing," *Journal of Enterprise Information Management* (18:5), pp 548-567.

Zissis, D., and Lekkas, D. 2011. "Securing e-Government and e-Voting with an open cloud computing architecture," *Government Information Quarterly* (28:2), pp 239-251.