Association for Information Systems

AIS Electronic Library (AISeL)

ACIS 2016 Proceedings

Australasian (ACIS)

2016

Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations

Ahmed Al-Kalbani
RMIT University, ahmed.al-kalbani@rmit.edu.au

Hepu Deng
RMIT University, hepu.deng@rmit.edu.au

Booi Kam
RMIT University, booi.kam@rmit.edu.au

Julia Zhang
School of Information Management, Wuhan University, xjz@whu.edu.cn

Follow this and additional works at: https://aisel.aisnet.org/acis2016

Recommended Citation

Al-Kalbani, Ahmed; Deng, Hepu; Kam, Booi; and Zhang, Julia, "Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations" (2016). *ACIS 2016 Proceedings*. 26.
https://aisel.aisnet.org/acis2016/26

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2016 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations

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

Xiaojuan(Julia) Zhang
School of Information Management
Wuhan University
Wuhan, China
Email: xjz@whu.edu.cn

Abstract

The increasing threat to information security has created institutional pressures on organizations to comply with information security policies and standards. This paper presents an empirical study to investigate the impact of institutional pressures (coercive, normative, and mimetic) on information security compliance in organizations. The results show that coercive pressures that are manifested by regulatory agencies, normative pressures that are exerted through social pressures, and mimetic pressures that are manifested by security benefits positively influence information security compliance in public organizations. Furthermore, the results reveal that regulation and security benefits generate pressures on management to strengthen their commitments towards information security compliance in organizations. It is, however, worthwhile to notice that social pressures do not have a significant impact on management commitments towards information security compliance. The implications of this study indicate the criticality of institutional pressures for enhancing information security compliance in public organizations both directly and indirectly.

Keywords
Institutional pressures, information security compliance, management commitment

1 Introduction

The increasing dependence on information systems in organizations has led their critical information exposed to the possibility of cyber-crime nowadays (Tassabehji et al. 2007). As a result, proactive approaches have to be adopted to safeguard organizational information. Enforcing information security compliance (Boss and Kirsch 2007; Siponen et al. 2007), which is referred to as the effective implementation of information security standards and policies for protecting information in organizations, is a proactive approach that is widely used (Von Solms 2005; Alkalbani et al. 2014; 2015a). A report of Gartner (2014), for example, demonstrates an accelerated demand of an information security compliance approach in organizations across the world. Two reports from the International Standards Certifications (ISC 2012 and 2013) point out that there is an increasing spending in organizations to ensure their compliance with existing standards and policies for information security.

Information security compliance ensures that information security mechanisms can work together effectively to protect the critical information in organizations (Wimmer and Von Bredow 2002; Tassabehji et al. 2007). Numerous studies have been conducted on information security compliance in organizations (Herath and Rao 2009; Bulgurcu et al. 2010; Ifinedo 2013). These studies have focused primarily on the factors related to users' attitudes, intentions, and behaviors to comply with information security standards and policies. There is, however, more on information security compliance with respect to understanding the complex socio-organizational dynamics in information security in organizations (Dhillon and Backhouse 2001; Vance et al. 2012). An investigation of such a dynamics leads to better understanding the interactions among various factors for shaping the use of information security compliance in organizations (Dhillon and Backhouse 2001; Bulgurcu et al. 2010).

This paper presents an empirical study to investigate the impact of institutional pressures on information security compliance in organizations. Theoretically the study contributes to the information security compliance research by better understanding how institutional pressures can be used as a baseline for enhancing information security compliance in organizations. Practically this study informs information security policy decision makers in organizations on the major institutional drivers for influencing information security compliance.

The rest of this paper is organized as follows. Section 2 presents a literature review of information security compliance. Section 3 presents an information security compliance model. Section 4 describes the research methodology. Section 5 presents the research findings based on the analysis of the survey data. Finally Section 6 presents the conclusion with the limitations of the study and future research.

2 Literature Review

The increasing reliance on information systems has created unprecedented challenges for organizations to protect their critical information from different threats (Knapp et al. 2006). As a result, the security of information has become critical in organizations. This has led organizations to continue to improve their security practices and solutions for establishing a proper use of their organizational information (Al-Kalbani et al. 2015b). Information security compliance is considered as an institutional yardstick for showing adequate steps taken to protect organizational information (Boss and Kirsch 2007; Siponen et al. 2010). It signifies that different information security aspects are working together for information security (Von Solms 2005; Neubauer et al. 2006). Non-compliance to information security policies in organizations can affect all workgroups and operations areas that have access to, or responsibility for, sensitive organizational information (Kankanhalli et al. 2003).

Several studies have investigated information security compliance in organizations using various theories (Pahnila et al. 2007; Herath and Rao 2009; Bulgurcu et al. 2010; Warkentin et al. 2011). Such theories include the social cognitive theory (Bandura, 1997), the social bond theory (Hirschi 1998), and the theory of social control (Wiatrowski et al. 1981). Bulgurcu et al. (2010), for example, find that having information security awareness programs highly affects employees' beliefs about the benefits of compliance and the cost of non-compliance. Shaw (2012) shows that having an organizational security culture improves employees' attitudes towards information security compliance. Kankanhalli et al. (2003) find that the fear of sanction of non-compliance with information security policies has a significant impact on employees' behavior towards information security compliance. These studies show a predominant focus on influencing employees' attitudes for improving information security compliance in organizations (Herath and Rao 2009).

There is, however, more on information security compliance with respect to a better understanding of other factors such as information security governance (Smith and Jamieson 2006) and legislative requirements (Benabdallah et al. 2002) that may influence information security compliance in organizations. Chan and Greenaway (2005) and Hovav and D'Arcy (2012), for example, advocate that using socio-organizational theories such as the institutional theory (DiMaggio and Powell, 1983) could leverage information security research. Bjorck (2004) argues that the institutional theory, as outlined in Meyer and Rowan (1977) and DiMaggio and Powell (1983), can be used to better explain how an organizational environment that consists of social and cultural forces can be used to influence the development of a formal security structure in organizations. The theoretical underpinning of this study is based on the use of institutional pressures for information security compliance in organizations.

3 Institutional Theory and Hypotheses Development

A main objective in organizational decisions is to gain legitimacy from all the stakeholders. This legitimacy can be gained by making strategic responses to external pressures (Cavusoglu et al. 2015). The basic notion of the institutional theory is that organizational structures and behaviours are based on the cultural and social pressures of their environments (Barley and Tolbert 1997). In the context of information security, it is these pressures that determine the ways organizations integrate their information security mechanisms in the process of complying with information security standards and policies (Khansa and Liginlal 2007). The presence of various laws and regulations on information security often forces organizations to act in compliance to receive legitimacy (Edwards et al. 2009).

The adoption of the institutional theory offers a new lens of rigor to examine the dynamics of information security practices in organizations (Bjorck 2004). It has been successfully used as a theoretical lens to (a) explain whether specific organizational behaviours are consistent with institutional forces, for example, determining the social behaviour of employees in terms of making choices with security implications (Liang et al. 2007; Delmas and Toffel 2008), and (b) understand the process of diffusion by the need to conform and imitate to institutional forces by which the actual security structure in organizations is developed (Khansa and Liginlal 2007; Appari et al. 2009; Cavusoglu et al. 2015). The institutional theory classifies pressures into three archetypes: coercive pressures, normative pressures, and mimetic pressures (Davidsson et al. 2006).

3.1 Coercive Pressure

Coercive pressures force organizations and decision makers to adopt certain institutionalized rules and practices in managing the organization (Hu et al. 2007). They stem from government mandates that force organizations to act in compliance to certain rules and practices to receive legitimacy (DiMaggio 1988; Edwards et al. 2009). Existing regulations (e.g., Sarbanes Oxley Act, and Privacy Act) are a source of coercive pressures (Hu et al. 2007; Khansa and Liginlal 2007). These regulations are made for the protection of organisational information to satisfy the requirements of various stakeholders for information security. This has made organizations to use information security practices such as the International Organization for Standardization (ISO 27001) to provide the foundation for building a robust response to regulatory requirements. Furthermore, regulations with enforcement provisions force organizations to incorporate the legal requirements in information security practices for meeting legal obligations (Khansa and Liginlal 2007). Organizations that have continually regulatory interventions may leads to significant structure changes such as the standardization of operational processes and practices to show conformity and gain legitimacy (Gunningham and Kagan 2005).

The formal pressure that is exerted on organizations to follow or adopt certain institutionalised rules and practices has an effect on the commitment of senior management towards information security compliance (Hu et al. 2006; Liang et al. 2007). The attitude and behaviours of managers towards information security in organizations are influenced by the regulatory requirements. Senior management is responsible for ensuring that their organizations comply with applicable laws and regulations because a failure to do so can result in stringent legal actions against them. This triggers them to review their current security practices. Hu et al. (2007) assert that regulatory pressure shapes and motivates managers in organizations to comply with information security requirements. The discussion above leads to the following hypothesis.

H1: Regulations have a positive impact on information security compliance in organizations.

H2: Regulations have a positive impact on management commitment towards information security compliance in organization.

3.2 Normative Pressure

Normative pressure stems from the cultural expectation that organizations are compelled to honour (Appari et al. 2009). A decision to adopt new practices is often influenced by how organizational stakeholders take actions with respect to the new practices (Cavusoglu et al. 2015). This type of pressures are raised from the values and norms that are embedded in the organization for information security compliance (Appari et al. 2009). There is abundant literature supporting the use of normative pressures for enhancing information security compliance (Kankanhalli et al. 2003; Appari et al. 2009). Organizations are likely to adjust their behaviour based on their beliefs about what is viewed as appropriate among members of their social networks and consequently adopt techniques and methods that reflect the current standards of those networks (Scott 2013). This implies that organizations are subjected to pressures exerted by their stakeholders' expectations (Kam et al. 2013).

The privacy, trust, and quality of services are social desirable needs that must be adequately addressed in organizations. These social desirable needs put organizations and their management in the spot light, making them conscious of the need to maintain the trust of stakeholders and preserve their reputation as a responsible public entity in protecting stockholders' information (Gunningham and Kagan 2005; Zhang et al. 2005). Kam et al. (2013), for instance, find that stakeholders' expectation of information security generates pressures in organizations to strengthen their information security practices. Delmas and Toffel (2008) explore the role of stakeholders in improving information security compliance. Alfawaz et al. (2008) investigate different cultural pressures that have an impact on information security compliance in public organizations in developing countries. Based on the above discussion, this study argues that normative pressures are exerted mainly through social pressures that influence both information security compliance in organizations and strengthen management commitments towards information security compliance. This leads the following hypothesis.

H3: Social pressures have a positive impact on information security compliance.

H4: Social pressures have a positive impact on management commitment towards information security compliance.

3.3 Mimetic Pressures

Mimetic pressures refer to the acquiescence by imitating peers to gain organizational legitimacy (DiMaggio and Powell 1983). They are present when an organization adopts the same actions, structure, and behaviours of similar organizations within their environments as a means of gaining legitimacy (DiMaggio and Powell, 1983). Mimetic pressures cause organizations to imitate success actions and practices taken by others, such as competitors within their industry (DiMaggio 1988). These successes serve as the basis of the desirable imitation, especially when organizations face similar needs and hoping for similar success (Haveman 1993; Bjorck 2004).

The perceived benefits of information security practices in terms of minimizing risks and threats, improving stakeholders' confidence and trust and employees' performance, and minimizing the impacts (Steinbart et al. 2012) in organizations serve as a basis for organizations to mimic each other. When organizations publicize their perceived benefits, they create pressures on other organizations to take actions with respect to their information security practices. That leads organizations to mimic each other. The perceived benefits may exhibit individual personality characteristics to imitate their successful peers to behave in a similar manner (Galaskiewicz 1985). Oliver (1991) argues, for example, that acquiescence by imitating successful peers to gain organizational legitimacy is a common strategic response to institutional pressures. Chan and Greenaway (2005) propose that organizations with effective information security practices influence employees' behaviour to conform to industry norms. The discussion above leads the following hypothesis.

H5: Security benefits have a positive impact on information security compliance.

H6: Security benefits have a positive impact on management commitment towards information security compliance.

3.4 Management Commitment

Management commitment centers on the efforts of senior management to promote information security compliance in organizations (Kajava et al. 2007; Karunasena andDeng 2013). It refers to the decisions, investments and actions taken for enforcing information security policies across the organization (Lee et al. 2004; Knapp et al. 2006). Commitment from top management is significant for information security in organizations, since their decisions usually drive the operational practices across the organisation. Failing to understand information security as a core competency in organizations could have a direct implications for business survivability (Kajava et al. 2007; Gupta 2008). Senior management should provide visible support and real commitment towards information security in their organizations.

Management commitment is an internalised organizational pressure that affects employees behaviours in complying with information security standards and policies (Dhillon and Backhouse 2001; Sasse et al. 2001). The visible participation, ongoing communication and championing of senior management stimulate employees' intentions towards information security compliance, and encourage the adherence to information security policies (Knapp et al. 2006; Kolkowska and Dhillon 2012). Management commitment has a persuasive effect on employees' information security compliance. Knapp et al. (2006) show that creation, training and enforcement of organization's security policies would not be taken seriously without top management support and involvement. This leads to the following hypothesis.

H7: Management commitment has a positive impact on information security compliance.

The above discussion suggests that institutional pressures influence information security compliance in organizations. This leads to the development of a conceptual model shown as in Figure 1 that hypotheses institutional pressures have a positive impact on information security compliance in organisations, and affect senior management commitments towards information security compliance. Figure 1 shows the conceptual model with the identified constructs and their associated attributes.

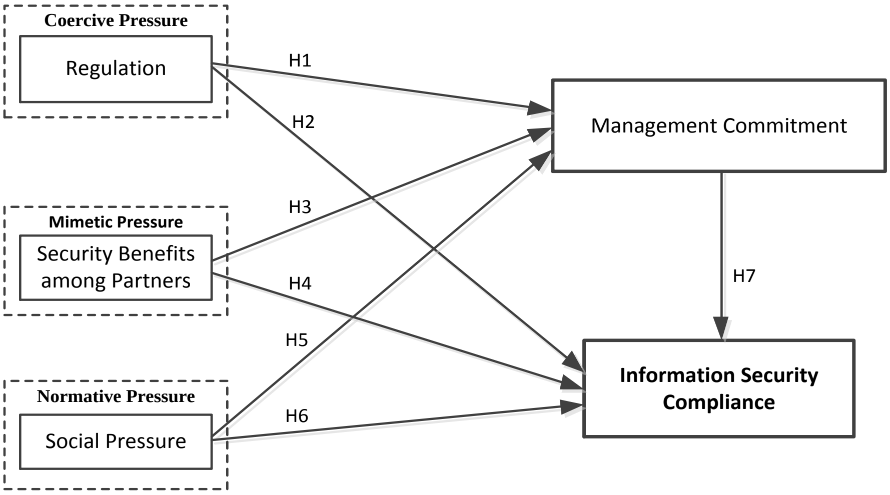

Figure 1. A Research Model

4 Research Methodology

This study aims to evaluate the impact of institutional pressures on information security compliance in organizations for better understanding the relationships between institutional pressures and information security compliance. To fulfil this objective, this study uses SEM for testing the relationships proposed in the theoretical model in Figure 1.

A web-based survey is used for data collection from public organisations in Oman. The survey questionnaire is tested for content and construct validity with experts in the field of information security and academics in information systems. The measurement items used in this research are adopted from previous studies in information security compliance shown as in Table 2. A seven point Likert scale is 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'. Overall, 326 responses are received, 32 responses with missing data and aberrant responses are excluded, yielding a total of 294 completed questionnaires for the analysis.

The consideration of the types of organisation and the role of participants ensures the robustness and generalizability of the research findings. The 294 responses represent the employees from different organisations. Most participants' ages below or equals to 40 years. 51% of participants hold a 'bachelor's degree' in their education background. 40% of the respondents were female, whereas 60% of the respondents were male. The responses indicate the diversification of the organisations in terms of sector type. Having 29% of the respondents from ICT sector, 18% from Education, 16% from Finance, 15% from Trading, 12% from Healthcare, 6% Agriculture, and 5% only from Travel and Tourism. In terms of size of the organisations, respondents reported 40% having more than 1000 employees at the time of study, and only 1% below 50 employees. As can be inferred from the above description of the respondents, the sample ensures the robustness and generalizability of the data collected for this research. The details of the sample demographics are reported in Table 1.

Profiles of Responding Participants	**Frequency**	**Percentage**
Gender		
- Male	175	60
- Female	119	40
Age		
- <=30	138	47
- 31 – 40	133	45
- 41 – 50	23	8
- 51 – 60	0	0
- > 60	0	0
Education Level		
- High School	36	12
- Diploma/Advanced Diploma	66	22
- Bachelor Degree	149	51
- Master Degree	38	13
- Doctoral Degree	5	2
Number of Years at current Role		
- 1 - 3	107	36.4
- 4 - 6	80	27.2
- >= 7	107	36.4
Organization Type		
- Education	52	18
- Health Care	34	12
- ICT	86	29
- Trading	43	15
- Travel/Tourism	15	5
- Finance	47	16
- Agriculture	17	6
Total Number of Employees		
- 1-50	3	1
- 51 – 100	9	3
- 101 – 250	31	11
- 251 – 500	72	24
- 501 – 1000	61	21
- >1001	118	40

Table 1. Summary of the participants' profiles

5 Data Analysis Results and Research Findings

This study uses SEM for testing the relationships proposed in the theoretical model as in Figure 1. The use of SEM is appropriate for this study due to its potential for extending the theory development (Gefen et al. 2000) and its capability of simultaneously assessing the multiple and interrelated dependence relationships. This study uses a two-step approach to SEM, namely a measurement model and a structural model (Hair, et al. 1998). The measurement model involves in conducting a confirmatory factor analysis (CFA) for assessing the contribution of each indicator variable and for measuring the adequacy of the measurement model. The structure model contains the path coefficients that indicate the strength and sign of the paths between variables (Hair 2010).

5.1 Measurement Model

To validate the measurement model, constructs are assessed based on (a) the reliability, (b) the discriminant validity, and (c) the adequacy of the model fit. To test the reliability of the constructs, Cronbach's alpha is used. Table 2 shows that all constructs have 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 the five factors have the AVE values exceeding the threshold value of 0.5. With the presence of these results, the reliability and validity of the constructs used in the model are supported (Hair 2010).

Constructs	α	AVE	Indicators	Variable	Factor Loading	Item Source
Regulation	0.76	0.52	Existence of regulations	R1	0.76	Mikko Siponen and Pahnila and Mahmood, 2010; Kam, Katerattanakul, Gogolin, Hong, 2013
			Governance of Law	R2	0.73	
			Severity of violation	R4	0.67	
Security Benefits among Partners	0.80	0.58	Perceived Benefits	B1	0.73	Kenneth and Knapp, 2006; Herath and Rao 2009;
			Responsiveness	B2	0.77	
			Appropriateness	B3	0.78	
Social Pressure	0.75	0.52	Citizen's trust	S1	0.69	Mikko Siponen and Pahnila and Mahmood, 2010; Kam, Katerattanakul, Gogolin, Hong, 2013
			Security commitment	S2	0.81	
			Social responsibility	S5	0.66	
Mang. Commit	0.77	0.52	Goals alignment	C1	0.73	Kenneth and Knapp 2006; Hayes et al. 1998
			Management support	C2	0.75	
			Management participation	C3	0.68	
InfoSecCom	0.73	0.50	Appropriateness of security Requirements	SecC1	0.73	Chan, Woon and Kankanhalli 2005; and Authors
			Perceived improvement	SecC2	0.68	
			Conformity with the expectations	SecC3	0.68	

Table 2. Reliability and validity measurement

Discriminant validity is assessed by comparing the square root of the AVE for each construct against the inter-construct correlation estimates (Fornell and Larcker 1981). Table 3 shows acceptable discriminant validity between each pair of constructs, with all AVE square roots greater than the correlation between the constructs. For example, security benefits showed highest discriminant validity among all other constructs. The square root of AVE for security benefits was 0.76 while the correlation between security benefits and other constructs ranged from 0.42 to 0.64. The results satisfy the discriminant validity (Fornell and Larcker 1981; Hair 2010).

Constructs	Regulation	Sec. Benefits	Social Pressure	Manag. Com.	InfoSecCom
Regulation	0.71				
Sec.Benefits	0.43	0.76			
Social Pressure	0.46	0.62	0.72		
Mang. Com.	0.62	0.64	0.50	0.72	
InfoSecCom	0.60	0.59	0.45	0.44	0.700

Table 3. The model constructs correlation

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 (χ2 /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 4 presents the final GOF results for both individual single-factor models and full measurement model within the acceptable range.

	x/df <2	**CFI>.95**	**GFI>.95**	**AGFI>.80**	**SRMR <.09**	**RMSEA <.05**	**PCLOS >.05**
Regulation	0.465	1	0.999	0.994	0.0094	0.00	0.631
Sec. Benefits	1.415	0.998	0.997	0.981	0.0135	0.038	0.390
Social Pressure	0.079	1	1	0.999	0.0029	0.00	0.845
Mang. Commit	0.286	1	0.999	0.996	0.0095	0.00	0.868
InfoSecCom	0.167	1	1	0.998	0.0077	0.00	0.928
Full Model	**1.650**	**0.972**	**0.932**	**0.911**	**0.0384**	**0.047**	**0.615**

Table 4. The GOF Results

5.2 A Structural Model

The significance of the structure model was tested using the paths coefficient and the explanatory power for each dependent variable (R^2) (Byrne 2013). The hypothesized model contains 5 constructs as shown in Figure 2. The hypothesized model with path coefficient and the explanatory power (R2) for each dependent construct is displayed in Figure 2. All coefficients on hypothesized paths except for the path coefficient from social pressure to management commitment are found to significantly differ from zero (p< 0.05 or p<0.01), as shown by dotted lines.

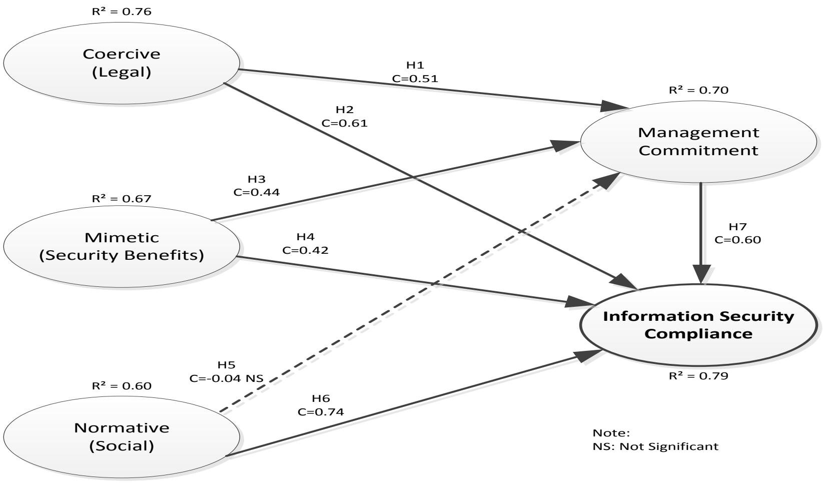

Figure 2: The hypothesised model results

The results of the model indicate a strong support for H1, H2, H3, H4, H6 and H7 with path coefficient values ranged from 0.42 to 0.74 respectively (p <0.05 or p <0.01). The results reject H5 implying that social factor has an insignificant effect on management commitment. In addition, in terms of the explanatory power, the model accounts for 76% of the variance in coercive pressure, 60% of the variance in normative pressure, 67% of the variance in mimetic pressure, and 70% of the variance in management commitment. With this result, it concluds that all hypotheses except H5 are supported.

The significance of institutional pressures on information security compliance is confirmed in the study. These pressures cause public organizations to put in extra efforts to maintain effective information security compliance. The study has also confirmed the significance of coercive pressures, and mimetic pressures for influencing management commitment towards information security compliance. It confirms the assumption that the higher impact of coercive pressures exerted by regulatory agencies and the mimetic pressures that are exerted through the influences of security benefits among partners the greater the commitment of senior management is towards information security compliance. On the other hand, the insignificant effect of social pressures on management commitment towards information security compliance suggests that management commitment towards information security compliance is not dependent on the presence of social pressures.

The study contributes by extending the current understanding of information security compliance in terms of the values of institutional pressures to foster information security compliance in public organizations. In practice, this study sheds lights on institutional pressures that offer suggestions on how public organizations may improve their information security compliance. It informs management and security practitioners to consider institutional pressures within their organizational environment for effective information security compliance.

6 Conclusion

In this study, SEM was used to test the hypothesized model in evaluating institutional pressures for information security compliance. The hypothesized model proposed various positive relationships between the institutional dimensions and the effectiveness of information security compliance in organizations. The research found strong support for six hypotheses and no support for one of the seven hypothesized relationships. This study has found that having institutional pressures could lead effective information security compliance in organizations. It, also, clearly indicates that regulation, and security benefits among partners have a direct effect on management commitments towards information security compliance. The findings underscore the importance of having institutional pressures for effective information security compliance.

Several limitations of this study can be addressed in future. First, some tangible measures of information security compliance could be considered. Second, the research findings remain limited, since these findings have been validated in a single country. As a result, replicating this study in other countries with different organizational and cultural settings would be a fruitful direction to assess and gauge the generalizability of the study. Third, further studies should consider incorporating technological and psychological factors that can help to enforce information security compliance.

References

Alfawaz, S., May, L. J., and Mohannak, K. 2008. "E-government security in developing countries: A managerial conceptual framework."

AlKalbani, A., Deng, H., and Kam, B. 2015a. "Investigating the Role of Socio-organizational Factors in the Information Security Compliance in Organizations," 26th Australasian Conference on Information Systems (ACIS 2015)2015, pp. 1-12.

AlKalbani, A., Deng, H., and Kam, B. 2015b. "Organizational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure," 19th Pacific Asia Conference on Information Systems (PACIS 2015) 2015. Singapore.

Alkalbani, A., Deng, H., and Kam, B. 2014. "A Conceptual Framework for Information Security in Public Organizations for E-Government Development," ACIS2014.

Appari, A., Johnson, M. E., and Anthony, D. L. 2009. "HIPAA Compliance: An Institutional Theory Perspective," AMCIS2009, p. 252.

Barley, S. R., and Tolbert, P. S. 1997. "Institutionalization and structuration: Studying the links between action and institution," *Organization studies* 18:1, pp. 93-117.

Benabdallah, S., Gueniara El Fatmi, S., and Oudriga, N. 2002. "Security issues in E-government models: what governments should do?," Systems, Man and Cybernetics, 2002 IEEE International Conference on, IEEE2002, pp. 398-403.

Bjorck, F. 2004. "Institutional theory: A new perspective for research into IS/IT security in organisations," System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, IEEE2004, p. 5 pp.

Boss, S. R., and Kirsch, L. 2007. "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.

Byrne, B. M. 2013. *Structural equation modeling with AMOS: Basic concepts, applications, and programming*, Routledge.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2015. "Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," *Information & Management* 52:4, pp. 385-400.

Chan, Y. E., and Greenaway, K. E. 2005. "Theoretical explanations for firms' information privacy behaviors," *Journal of the Association for Information Systems* 6:6, p. 7.

Davidsson, P., Hunter, E., and Klofsten, M. 2006. "Institutional Forces The Invisible Hand that Shapes Venture Ideas?," *International Small Business Journal* 24:2, pp. 115-131.

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., and Powell, W. W. 1983. "The iron cage revisited: Collective rationality and institutional isomorphism in organizational fields," *American Sociological Review* 48:2, pp. 147-160.

DiMaggio, P. J. 1988. "Interest and agency in institutional theory," *Institutional patterns and organizations: Culture and environment* 1, pp. 3-22.

Edwards, J. R., Mason, D. S., and Washington, M. 2009. "Institutional pressures, government funding and provincial sport organisations," *International Journal of Sport Management and Marketing* 6:2, pp. 128-149.

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

Galaskiewicz, J. 1985. "Interorganizational relations," *Annual review of sociology*, pp. 281-304.

Gartner, A. 2014. "Gartner Security & Risk Management."

Gefen, D., Straub, D., and Boudreau, M.-C. 2000. "Structural equation modeling and regression: Guidelines for research practice," *Communications of the association for information systems* 4:1, p. 7.

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

Gupta, J. N. 2008. *Handbook of research on information security and assurance*, IGI Global.

Hair, J. F. 2010. *Multivariate data analysis*, Perason.

Haveman, H. A. 1993. "Follow the leader: Mimetic isomorphism and entry into new markets," *Administrative science quarterly*, pp. 593-627.

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.

Hirschi, T. 1998. "Social bond theory," *Criminological theory: Past to present. Los Angeles: Roxbury*.

Hovav, A., and D'Arcy, J. 2012. "Does culture really matter? A cross-cultural analysis of security countermeasure effectiveness based on deterrence theory," *Information & Management* 49:2, pp. 99-110.

Hu, Q., Hart, P., and Cooke, D. 2006. "The role of external influences on organizational information security practices: An institutional perspective," Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), IEEE2006, pp. 127a-127a.

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.

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.

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.

Karunasena, K., andDeng, D. 2013. "A conceptual framework for evaluating the public value of e-government: a case study from Sri Lanka", 20th Australasian Conference on Information Systems (ACIS2013), Melbourne

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.

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

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.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS quarterly*, pp. 59-87.

Miller, D. 1987. "Strategy making and structure: Analysis and implications for performance," *Academy of management journal* 30:1, pp. 7-32.

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

Oliver, C. 1991. "Strategic responses to institutional processes," *Academy of management review* 16:1, pp. 145-179.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' behavior towards IS security policy compliance," System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, IEEE2007, pp. 156b-156b.

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.

Shaw, R. M. 2012. *The influence of organizational culture on employee attitudes towards information security policy*, Capella University.

Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' adherence to information security policies: an empirical study," in *New Approaches for Security, Privacy and Trust in Complex Environments*, Springer, pp. 133-144.

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

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.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from habit and protection motivation theory," *Information & Management* 49:3, pp. 190-198.

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

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

Warkentin, M., Johnston, A. C., and 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, pp. 267-284.

Wiatrowski, M. D., Griswold, D. B., and Roberts, M. K. 1981. "Social control theory and delinquency," *American Sociological Review*, pp. 525-541.

Wimmer, M., and Von Bredow, B. 2002. "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.

Acknowledgement

This work is supported by the Natural Science Foundation of China (Grant 71473182), and the Major Project of the Key Bases of Humanities and Social Science of the Ministry of Education, China (Grant 13JJD870004).

Copyright: © 2016 AlKalbani, Deng, Kam, and Zhang. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 3.0 Australia License, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and ACIS are credited.