Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2017 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

Summer 7-19-2017

Exploring the Factors influencing Top Management Involvement and Participation in Information Security

Rufizah Abdul Munir
International Islamic University - Malaysia, rufizah.munir@live.iium.edu.my

Nurul Nuha Abdul Molok
International Islamic University Malaysia, nurulnuha@iium.edu.my

Shuhaili Talib
International Islamic University - Malaysia, shuhaili@iium.edu.my

Follow this and additional works at: http://aisel.aisnet.org/pacis2017

Recommended Citation
Munir, Rufizah Abdul; Abdul Molok, Nurul Nuha; and Talib, Shuhaili, "Exploring the Factors influencing Top Management Involvement and Participation in Information Security" (2017). *PACIS 2017 Proceedings*. 65.
http://aisel.aisnet.org/pacis2017/65

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2017 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Exploring the Factors influencing Top Management Involvement and Participation in Information Security

Research-in-Progress

Rufizah Abdul Munir
Department of Information Systems
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia, Kuala Lumpur
rufizah.munir@live.iium.edu.my

Nurul Nuha Abdul Molok
Department of Information Systems
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia, Kuala Lumpur
nurulnuha@iium.edu.my

Shuhaili Talib
Department of Information Systems
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia, Kuala Lumpur
shuhaili@iium.edu.my

Abstract

Organizations that rely heavily on ICT face bigger challenges to safeguard their information assets. Organizations need to be vigilant to cope with ever growing information security risks and threats due to technological advancement. All employees, from the senior management to the junior subordinate, have the responsibility to protect organizational information from such threats. Top management members are accountable to play imperative roles in steering information security programs to ensure the confidentiality, integrity and availability (CIA) of organizational valuable assets are protected. They should be more involved to allow information security to become an intrinsic part of corporate governance. However, information security is often viewed as technical and operational issues rather than business issues, thus it is delegated to IT and security team. This conceptual study aims to explore this current phenomenon by investigating the factors influencing top management in governing information security implementation in organizations. Qualitative research approach is proposed for this study by interviewing the members of top management in the Malaysian public sector organizations. The understanding of the influencing factors would assist in formulating a dedicated information security training and awareness framework tailored for the top management. Since most information security awareness programs are designed for lower and middle level employees, this study aims to fulfil this gap by focusing on specific training guidelines for the top management. The proposed framework will help public sector organizations to produce, or improve existing, competency development programs. It will help the members of top management to exercise due diligence and understand their roles and responsibilities as the key driver in governing information security implementation in their organizations.

Keywords: information security, top management, information security governance, information security management

Introduction

In today's world, computers are more interconnected than ever before and are being used extensively in organizations. The dependency on computers and information and communication technology (ICT) in running overall business operations through technology, people and process elements, could expose organizations to information security risks (Razali & Said, 2015; Posthumus & von Solms, 2004). Despite efforts that have been done to mitigate information security risks and threats, substantial volumes of computer breaches and cybercrimes remain significantly high (Ula, Ismail, & Sidek, 2011). Recently, Ernst & Young (2014) reported annual increment of 50% of information security breaches. For this reason, organizations which rely heavily on ICT to operate business have taken information security seriously and have started to invest more money to produce secure virtual business environment.

According to von Solms (2006), up until early 1980s, solutions to information security primarily focused on technical issues. However, experts have now realized that technological solutions alone could not guarantee secure mechanisms for organizational information (Safa et al., 2015). In fact, 100% security is impossible because all possible risks, threats and vulnerabilities are never known (Singh, Picot, Kranz, Gupta, & Ojha, 2013). Risks, threats and vulnerabilities are growing and changing over time due to the technological advancement in the ICT world. Information security issues need to be tackled from a broader, holistic approach to preserve the CIA of the information. For that reason, in recent years, many studies in information security have started to incorporate the human aspects as well as managerial aspects, and no longer limited to technology issues. This include the governance component where the top management has a very important role in establishing and managing information security in organizations (Soomro, Shah, & Ahmed, 2016; von Solms, 2001) to handle business and IT risks (Singh et al., 2013).

Commitment from the top management is crucial not only to guarantee security initiatives can be implemented throughout the organizations, but also to ensure sustainability and continuous maintenance of information security activities within the organizations. However, preliminary observation shows that the involvement and participation of the top management in governing security implementation in Malaysian public sector organizations is still lacking. Therefore, it motivates this study to investigate the influencing factors that contribute to the involvement and participation issue among top management.

This study employs Multiple Perspectives Theory (MPT) as underlying framework. MPT is chosen because it proposes a solution to be viewed from multiple aspects rather than from a single point of view. The initial factors are extracted from implicit and explicit findings from Neo-Institutional Theory (NIT) (for external factors) and from academic literature in information security.

The Key Concepts of the Top Management Involvement and Participation

The terms "involvement" and "participation" are used extensively within the field of information systems (IS). Although the words are used interchangeably and suggest the same meaning, there is a slight different between the two according to researchers in psychology, marketing and organizational behavior disciplines (Barki & Hartwick; 1989). "Involvement" generally refers to subjective psychological state reflecting the importance and personal relevance of a system to a user, while "participation" refers to behaviors and activities performed by users. These two definitions are then argued by Jarvenpaa & Ives (1991), where "executive participation" refers to Chief Executive Officer (CEO) activities and personal interventions in information technology (IT) management, or in other words, the CEO spend his/her time and energy to do hands-on role in managing IT. On the other hand, "executive involvement" is more on the psychological state concerning with CEO's perception and attitudes about IT-related matters. The involvement of CEO does not require him/her to know "how" but the view of IT as a contributing factor to organization's success is all needed. Throughout the article, Jarvenpaa & Ives (1991) used "executive support" referring to involvement and participation of CEOs.

This study applied both words as in the IS field. The term top management "involvement"; or "participation"; or "commitment" used interchangeably as this study attempts to explore the influential factors pertaining both involvement (psychological state) as well as participation (hands-on). As for the "top management" that involved in this research, they are based on the roles mapping with the Information Security Governance (ISG) framework which developed by Posthumus & von Solms (2004) as below:

MAPPING OF TOP MANAGEMENT ROLES	
Information Security Governance Framework	**Designation in Malaysian Public Sector Organizations**
Board of Directors	Secretary General (KSU), Deputy Secretary General
Board Committees	Undersecretary and above
Chief Executive Officer (CEO)	Secretary General (KSU)
Chief Information Officer	Chief Information Officer (CIO)
Chief Information Security Officer (CISO)	Information and Communication Technology Security Officer (ICTSO)
Data Owners	Undersecretary

Table 1. Mapping of roles between the designations of top management in Malaysian public sector organizations and ISG Framework

Research Questions

This research is designed to understand the arising issues related to top management in information security. Below are the research questions (RQ) that this research seeks to answer:

- *How information security is being practiced in Malaysian public sector organizations?*
- *What are the factors influencing the top management involvement and participation information security initiatives in public sector organizations?*
- *How the influencing factors can be used to contribute to the awareness and competency development for the top management in order to govern information security implementation?*

These research questions attempt to investigate the current involvement and participation shown by the top management in several public sector organizations. As argued by extant studies, activities related to information security management are usually put on the shoulder of the operational level in IT-related unit (Williams, 2001). To address this issue, this study also investigates the extent of top management commitment. From this understanding, the factors that influence top management commitment in information security implementation will be proposed. These factors will be used in developing a framework for information security training and awareness programs tailored to the needs of the top management as one of the recommended solutions to the problem.

Background Study

Information as a valuable assets are the data which is recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium (Williams, 2001). The definition also extends the meaning of security which relates to the protection of information against loss, improper disclosure or damage. To sum up, information security is the discipline used to ensure protection of electronic information against possible risks to preserve confidentiality, integrity and availability of the information (von Solms & von Solms, 2009).

Information security back then was focused on the technical solutions, then moving to the management dimension and slowly shifted to institutional aspects. Many current studies are now exploring on the aspect of information and cyber security governance (von Solms, 2010). It is interesting to see the fact that management and governance of information security has gained a lot of interests from the experts and researchers.

ISM is about managing and configuring resources (Singh et al., 2013). For the organization to meet information security needs, critical business assets, risks and threats, and countermeasures need to be identified in producing a balanced mix of technical, management and human to form an overall ISM systems. Taking the management component into account, various management activities had a significant impact in producing a quality ISM (Soomro et al., 2016). There are six major activities involved in ISM which comprise of policy development, roles and responsibilities, design, implementation, monitoring, and awareness, training and education (Williams, 2001).

All employees – from the senior management to the junior subordinate, have information security responsibility (Johnson & Goetz, 2007; von Solms & von Solms, 2009). However, the accountability and responsibility to manage information security risks and its countermeasures lies on the shoulder of the organization's top management (Khoo, Harris, & Hartman, 2010; Razali & Said, 2015). Top

management need to be forced to accept the ultimate responsibility to ensure information security is aligned with the overall business objectives and mission (von Solms, 2001).

Information security initiatives require direction, goal and aim which developed by the top management of the organization which then escalated down and shared by the whole member of the organization. When the required activities are implemented in achieving the needs, the top management will receive feedback from all level of organization that basically becomes part of the monitoring process. This cycle – Direct-Implement-Check is basically form a formal structure known as Information Security Governance (ISG) (von Solms & von Solms, 2009). ISG must be integral but transparent in Corporate Governance and aligned with Information Technology Governance (ITG) framework (IT Governance Institute, 2006). This means, Corporate Governance driven by top management govern overall business functions and risks. ITG as one of Corporate Governance components appear as a result of expanding traditional business into information and communication technology (ICT) for daily business operations (von Solms & von Solms, 2009; Williams, 2001). ITG ensures IT related risks are properly managed and the reliance of ICT in daily business operations are maintained at all times. As a subset of ITG, ISG becomes a focused activity which revolves around information protection to produce a secure environment.

Every component in ISG (policies, processes, personnel, products, etc.) needs direct commitment from the top management. This is why top management need to understand their responsibility and accountability in ITG and ISG, and also realize the importance of their role for each and every governance (Williams, 2001).

The main objective of governance is to ensure every level of employees know their roles – know what to do, how it should be done, who should do it (Whitman & Mattord, 2012). Apart from knowing their roles and responsibilities, top management also need to know what do the security components need to be governed, so that they can actively involve and participate in information security initiatives in their organization.

Theoretical Foundations

The foundation of this study started with identifying several theories related to managerial and behavior in organizations. Information Systems (IS), psychology, marketing and organizational behavior are among significant fields which provide in-depth understanding about the concept and the definition of involvement and participation in the context of managerial in organizations. Since we want to study about the influential factors contribute to the involvement and participation of top management in information security initiatives from every aspects, The Multiple Perspectives Concept (MPC) proposes a problem-solving concept or way of thinking through multiple or different lens, value and assumption (Linstone, 1989; Mitroff & Linstone, 1993). Single point of view is not sufficient to solve complex issue of top management commitment in organization (Rahim, 2009). Understanding the issue from different perspectives allow researchers to propose more balance solutions. MPC highlights there (3) perspectives namely as *Technical* (T), *Organizational/Societal* (O) and *Personal/Individual* (P) (T.O.P perspective) and this seems fit to be the fundamental framework for this research model. Each factor is assessed and then is grouped under the most suitable perspective which later to be studied empirically.

The second construct of this research comes from Neo-Institutional Theory (NIT) by DiMaggio & Powell (2000); Meyer & Rowan (1977). NIT appears suitable to explain how external (institutional) forces able to shape the behavior of the organization actors (managers) thus determine the behavior of the organization (Hu, Hart, & Cooke, 2007) through three (3) important forces. The forces are: *Coercive* (actors are forced by the external regulation pressure e.g. government directives, laws, acts, standards, etc), *Mimetic* (actors are forced to remain similar/follow the success of the competitors/peer organizations) and *Normative* (actors are forced because the key persons in managerial or the actor himself learned (from academic background or professional training) that something is a good thing or need to do (Bjorck, 2004). These external forces would not have strong impact directly to the organization as it is first affecting the actors within the organizations (Liang, Saraf, Hu, & Xue, 2007). From their study, it is argued that the institutional forces have direct impact to the top management. Thus, it is suitable to be applied in managerial of IS/IT security research (Bjorck, 2004). For this study, NIT provides additional perspective – External (E) factor that seems significant and may potentially influence the involvement and participation of top management in governing information security implementation. For that reason, we modify the T.O.P perspective by adding "E" perspective to the "T" perspective of MPC which broaden the lens of solving the involvement issue.

We have the ground of conceptual model from MPC and external factor derived from NIT, the rest of the factors are extracted from implicit and explicit findings from literature reviews. Below is the summary of the factors which is categorized under each perspective adapted from MPC:

	TECHNICAL/ EXTERNAL FACTOR		**ORGANIZATIONAL/ SOCIETAL FACTOR**		**PERSONAL/INDIVIDUAL FACTOR**			
SUMMARY	1) Regulatory Forces *(Coercive)* 2) Peer Organizations Achievements *(Mimetic)*		1) Organizational Conditions 2) Organizational Size 3) Work Patterns/Practices		1) Age 2) Education Background *(Normative)* 3) Functional Background/ICT Knowledge/Perception/Competency *(Normative)* 4) Tenure in Company			
Barki & Hartwick (1989)			Organizational Conditions					
Jarvenpaa & Ives (1991)			Organizational Conditions	Organizational Size	Age	Education background	Functional background	Tenure in company
DiMaggio & Powell, 2000; Meyer & Rowan (1977)	Coercive	Mimetic			Normative			
Hu et al. (2007)	Coercive		Work Patterns		Normative			
Liang et al. (2007)	Coercive	Mimetic						
Barton (2014)		Mimetic						
von Solms (2001)					Perception			
Williams (2001)					Perception			
Lankton (2016)			Work Practices		ICT Knowledge & Expertise	Competency		
Horne (2016)					Competency			

Table 2. The Summary

Conceptual Model of the Factors influencing Top Management Involvement and Participation

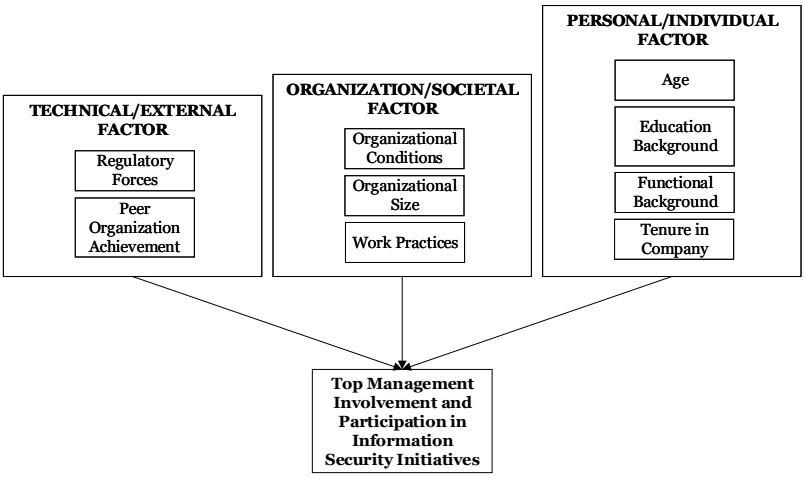

Figure 1. The Conceptual Model

Figure 1 illustrates plausible factors that may influence top management involvement and participation in governing information security initiatives. The baseline of this model is adapted from MPC where each factor is selected and grouped into T.O.P perspectives. Since the external factors (Coercive, Mimetic, Normative) from NIT have the potential to be the influential factor, therefore the MPC theoretical model is modified and External Factor is added into the "T" perspective.

Under the "T/E" perspective, there are two (2) possible factors to be studied – Regulatory Forces and Peer Organization Achievement. Both factors are extracted from NIT which represent Coercive and Mimetic force respectively. On the other hand, the factors from "O" and "P" perspective is extracted from the literature of involvement studies. Education and Functional Background under the "P" perspective represent Normative force in MPC.

This conceptual model shows that there are several factors from various aspects that may influence the top management involvement and participation in information security initiatives. This model is used to give the fundamental idea of involvement issue and the factors depicted from this model require an empirical study where this research intend to achieve.

Upon completion of this study, the actual factors that contribute to the involvement among top management will materialize. The reasons are expected to revolve around the factors depicted from this research model. We propose that the involvement and participation issue among top management can be addressed by setting up a training and awareness guideline that is able to contribute to the competency development program in Malaysian public sector organizations.

Proposed Research Design

This study will adopt qualitative research approach. Table 3 shows the proposed research design to answer research questions specified earlier and divided into four (4) phases as depicted below:

RESEARCH PHASE	RESEARCH PROCESS	METHOD	ACTIVITY	DELIVERABLE
Phase I: Background Study	Contextual Definition & Concept → Literature Review	-	▪ To seek definition of research context. ▪ To understand the concept and do literature review on topic.	▪ Understanding of the definition, concept and topic under study. ▪ Gathered plausible factors.
Phase II: Empirical Study (RQ1)	Multiple Case Studies → Data Analysis	Observations, document reviews	▪ To investigate the current practice of information security implementation in the organizations including the extent of top management commitment. ▪ To observe and to review information security activities and documents.	▪ Understanding of the current information security practices of the organizations and top management roles.
Phase III: Empirical Study (RQ2)	Multiple Case Studies → Data Analysis	Interviews (approximately 90-minute long), observations, document reviews	▪ To interview at least 2 top management from each ministry, followed by observations and document reviews. ▪ 4 Ministries involved: Public Services Commission of Malaysia (SPA), Ministry of Defense (MinDef), Ministry of Finance (MOF) and Malaysian Administrative Modernization and Management Planning Unit (MAMPU).	▪ Analyzed data. ▪ Factors identification and mapping.
Phase IV: Development and Findings Validation (RQ3)	Final Results → Conclusion	Focus Groups	▪ To validate findings by comparing and mapping the findings from Phase II and Phase III. ▪ To propose a framework for training and awareness program.	▪ All RQs are answered. ▪ Developed training guideline. ▪ Validated framework by the focus group and final confirmation.

Table 3. The Research Design

Expected Contribution

Studies concerning the influencing factors of top management involvement and participation in information security implementation are scant. Therefore, this study aims to complete this gap and contribute not only to IS research but also to the industry. Many existing security programs are designed for lower and middle level employees, so the proposed framework for training and awareness programs can be used by organizations to establish a dedicated program tailored for the top management. It would be able to contribute to competency development of the top management in driving information security implementation through a comprehensive and well-designed training and awareness program.

Acknowledgement

We would like to express our sincere gratitude to the Public Service Department of Malaysia for the sponsorship of this study under the Federal Training Award (HLP). We gratefully appreciate the constructive comments by the reviewers and all related parties who have helped improve the quality of this paper throughout the review process.

References

Barki, H., & Hartwick, J. 1989. "Rethinking the Concept of User Involvement," *MIS Quarterly* (13:1), pp. 53-63.

Barton, K. A. 2014. *Information System Security Commitment: A Study of External Influences of Senior Management*. Nova Southeastern University.

Bjorck, F. 2004. "Institutional theory: A new perspective for research into IS/IT security in organisations," in *Proceedings of the 37th Annual Hawaii International Conference,* pp. 1–5.

DiMaggio, P. J., & Powell, W. W. 2000. "The Iron Cage Revisited Institutional Isomorphism and Collective Rationality in Organizational Fields," in *Advances in Strategic Management*, Bingley: Emerald (MCB UP), pp. 143–166.

Ernst & Young. 2014. *Cyber Program Management - Identifying Ways to Get Ahead of Cybercrime*. Ernst & Young.

Horne, C. 2016. *Lack of Cyber Security Knowledge Leads to Lazy Decisions from Executives*. Retrieved November 23, 2016.

Hu, Q., Hart, P., & 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.

IT Governance Institute. 2006. *Information security governance: guidance for boards of directors and executive management*, IT Governance Institute.

Jarvenpaa, S. L., & Ives, B. 1991. "Executive Involvement and Participation in the Management of Information Technology," *MIS Quarterly,* pp. 205-227.

Johnson, M. E., & Goetz, E. 2007. "Embedding information security into the organization," *IEEE Security & Privacy* (*5:*3), pp. 16-24.

Khoo, B., Harris, P., & Hartman, S. 2010. "Information Security Governance of Enterprise Information Systems: An Approach to Legislative Compliant," in *International Journal of Management and Information Systems* (14:3), pp. 49-56.

Lankton, N. 2016. *Board Involvement with IT Governance - Practically Speaking Blog*. Retrieved October 7, 2016.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp. 59–87.

Linstone, H. A. 1989. "Multiple Perspectives: Concept, Applications, and User Guidelines," *Systems Practice* (2:3), pp. 307–331.

Meyer, J. W., & Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), pp. 340–363.

Mitroff, I. I., & Linstone, H. A. 1993. *The Unbounded Mind: Breaking the Chains of Traditional Business Thinking,* New York: Oxford University Press.

Posthumus, S., & von Solms, R. 2004. "A Framework for the Governance of Information Security. *Computers & Security* (23:8), pp. 638–646.

Rahim, N. Z. A. 2009. *Multiple Perspectives of Open Source Software Appropriation in Malaysian Public Sector*. Universiti Teknologi Malaysia.

Razali, F. M., & Said, J. 2015. "Information Security: Risk, Governance and Implementation Setback," in *Procedia Economics and Finance* (28), pp. 243–248.

Safa, N. S., Sookhak, M., von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. 2015. "Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security* (53), pp. 65–78.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. 2013. "Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany," *Global Journal of Flexible Systems Management* (14:4), pp. 225–239.

Soomro, Z. A., Shah, M. H., & Ahmed, J. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review," *International Journal of Information Management* (36:2), pp. 215–225.

Ula, M., Ismail, Z., & Sidek, Z. M. 2011. "A Framework for the Governance of Information Security in Banking System," *Journal of Information Assurance & Cybersecurity* (2011), pp. 1–12.

von Solms, B. 2001. "Corporate Governance and Information Security," *Computers & Security* (20:3), pp. 215–218.

von Solms, B. 2006. "Information Security – The Fourth Wave," *Computers & Security* (25:3), pp. 165–168.

von Solms, B. 2010. "The 5 Waves of Information Security–From Kristian Beckman to the Present," in *IFIP International Information Security Conference,* Springer, pp. 1–8.
von Solms, B., & von Solms, R. 2009. *Information Security Governance*. Boston, MA: Springer US.
Whitman, M., & Mattord, H. J. 2012. "Information Security Governance for the Non-Security Business Executive," *Journal of Executive Education* (11:1), pp. 97-111.
Williams, P. 2001. "Information Security Governance. *Information Security Technical Report* (6:3), pp. 60–70.