2006

Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organisation: An Empirical Analysis

Suhazimah Dzazali
University of Malaya

Social Factors Influencing the Information Security Maturity of Malaysian Public Service Organisation: An Empirical Analysis

Suhazimah Dzazali,
University of Malaya, Malaysia

Abstract

Information security maturity is the measurement of the organisation's capability to remain secure. This article focuses on the social aspect of the management approach as part of a larger study that uses a socio-technical theory as a basis for analysing the relationship between the social and technical factors in the information security management system of Malaysian Public Service organisations. The empirical analysis was conducted to identify the antecedents of the information security maturity of an organisation, mainly through the study of several social factors. Through the sample obtained from the key players of information security in Malaysian Public Service organisations, results of the multivariate test reveal the underlying dimensions of a few social factors. The final result provides empirical proof of the social factors that has the most influence on the Malaysian Public Service organisations' information security maturity.

Keywords

Malaysian Public Service, Information Security Management, Information Security Maturity and Socio-technical Theory

INTRODUCTION

Information security is often mistaken to revolve around technical issues and usually delegated to information system entity within an organisation. This view is slowly changing especially in the commercial enterprise where the risks involved for the organisation is no longer limited to compromise of information system or network infrastructure but also include legal liabilities, loss of trust and severe financial repercussion (McAdams, 2004). It is said that the involvement of top management is crucial in the acculturation of information security in all levels of the organisation (Von Solms et al, 2004; ITGI, 2003; Andersen, 2001). The Malaysian Public Service (MPS) may not have exactly the same security issues as those commercial enterprises but the stakes are similar. Public trust, national sovereignty, national security and service delivery are at risk. Hence confidentiality, integrity, and availability of the information asset should be the ultimate goal of information security management in MPS organisations and that would be reflected in the information security maturity level of the organisations.

Using social-technical theory as guidance, this study examines the information security management practices in the MPS organisations by focusing on the social aspect of the management system. The article is part of a larger research study that deployed a survey questionnaire measuring the social factors namely the perception of the information security custodians in the organisation, the organisation's security culture and the technical factor recognized as the formal mechanism of managing information security. The criterion is the information security maturity measured through the organisation's information security management practice and control. A social-technical perspective describes the organisation as a composite of a social system and a technical system (Kawalek, 1996; Cherns, 1976). In the context of information security management system, the social system is made up of people and their concern where as the technical system is the management tool used in the system (Dhillon & Backhouse, 2001; Land, 2000).

In the next section, the literature on the criterion and factors are briefly reviewed. Then the article discussed the quantitative study deployed followed by the multivariate tests to describe the relationships of the variables. The theoretical and managerial findings are also presented.

LITERATURE REVIEW

Malaysian public service like other public and private enterprises in the world has seen a rapid deployment of information system throughout the enterprise for the past two decades. Intrinsic in this endeavour is the importance of information protection, which is linked to the emerging knowledge of information security. Changing times bring forth new dimensions to the concept of information security. In the beginning, when the computing world used to consist only of a centralised and isolated mainframes or mini computer, the challenge of managing security is not as overwhelming compared to current borderless scenario. As the technological systems grow more sophisticated and complex so does the security threat. The perpetrator is just not the technology alone but the social systems consisting of the organisation, individual and society. Schneier (2000)

observed that users often represent the weakest link in the security chain. Putting in placed all the technological based security solution is a futile effort if the people interacting with the system do not implement prudent security practice. A study of an effective information security management system would not be complete if it does not consider the organisation, human and social factors besides the technological factor (Dhillon & Backhouse, 2001; Schneier, 2000; Armstrong, 1999).

Information Security Maturity

Information security maturity of an organisation is the measurement of the organisation's capability to remain secure. Siponen (2002) suggested that information security maturity could be a mean of self-assessment by the organisation. It could also be an approach that demonstrates to either the internal or external parties the confidence in the security level or maturity of an organisation. In this study, the maturity levels are measured based on the extent information security management processes are successfully implemented in an organisation. Three standards or methodologies found to take the maturity level approach to information security are Cobit: Management Guidelines (ISACA, 2000), The Information Security Management Maturity Model - ISM3 V1.0 (Aceituno, 2004), and System Security Engineering-Capability Maturity Model (SSE-CMM, 1998).

Two models were used as references for this study; the Information Security Maturity Model ISM3 V1.0 (Aceituno, 2004) and the information security processes and practices maturity model found in Cobit: Management Guidelines (ISACA, 2000). Both model use process oriented approach towards information security management and have similar description for all levels 1 to 5. Each of the maturity level described processes that reflect the extent information security management processes are implemented hence the information security level of the organisation.

Organisation responsibility and communication structure and Other Social Factors

Organisational culture has a significant function in the implementation of information security. Although cultivating an information security culture is vital, the current perspective on information security culture is not well defined and there is only limited literature available on the concept (Andress, 2000; Borck, 2000; Eloff & Von Solms, 2000; Gaunt, 2000). Information security characteristics such as integrity and availability of information need to be valued and pursued by the organisation. Information security culture is also an assumption about what is and what is not acceptable in relation to information security. Information security culture will also emerge from encouraging acceptable information security behaviour. An example could be that people are encouraged to report security incidents via the appropriate management channels. Information security culture can thus be defined as the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation (Dhillon & Backhouse, 2001).

Instilling an information security culture requires the commitment of the senior management and the cooperation of the group or individual levels of the organisation. Issues such as information security policy and information security awareness as well as training need to be addressed by an organisation to develop a culture conducive to the protection of information assets. (Von Solms & Thomson, 2005) This research does not examine the organisational behaviour that influences the information security culture rather the management practices formulated at the senior management level and adhering to procedure at the individual or group level as the manifestations of the entrenched security conscious culture. On another level are the perceptions of the people responsible for the information security. Among those perceptions is their regard for the value of information security, the perception about risk elements such as threat that could harm critical operation or vulnerability of the information system as well as their perceptions about what constitute as barriers to secure information assets (Ezingeard and Bowen-Schrire, 2003; Musekura, J.B. & Ekh, R., 2003; Wallace at al, 2002).

METHODOLOGY

A quantitative approach using a survey questionnaire as the data collection methodology was chosen as the research design for this study. The empirical data obtained would enable the study between antecedent social factors and information security maturity. Consequently, relationship-based statistical measures were employed.

Population and Sample

A mail survey was carried out and 210 useable questionnaires were returned indicating 21.6% response rate. Response bias was determined using wave analysis method (Leslie, 1972), whereby responses to questions pertaining to the three construct was examined weekly over 8 weeks period. There were no significant differences found between the responses in the final weeks and the earlier ones, thus establishing a strong case for absence of response bias. The sampling frame constitutes a list of 970 individuals comprising 180 chief

information officer, 100 information and communications technology (ICT) managers, 630 ICT security officers, and 60 line-of-business managers. The people basically represent the senior management, middle management and the operational level positions. The respondents consist of civil servant carrying various roles related to information and communications technology, with one role in common vis-à-vis the administration and management of information security in their organisations.

Measurement

The questionnaire was structured as Section 1 to Section 10 each encompassing a different subject as shown in Table.

Table 1: Questionnaire Structure

Section	Subjects
1	Information Security Incidents Experienced by Organisations (*Not Relevant To Article*)
2	Value Of Information Security To My Organisation
3	Presence of Security-conscious Cultures In Organisation
4	Responsibility And Communications Structure For The Management Of Information Security
5	Information Security Related Policies And Procedures
6	The Handling Of Information Security Incidents And The Assurance Of Service Continuity
7	Awareness About The Elements Of Information Security Risks And Its Management
8	Barriers To Effective Information Security
9	Safeguard Measures Deployed In The Organisation (*Not Relevant To Article*)
10	Background Information Of Respondents

Measures of Dependent and Independent Variables

The information security maturity as dependent variable and the independent variables were measured using 45 and 69 items respectively. The scales were developed based on analysis of information security issues and processes found in the literatures. The respondents were asked whether they agree to the statements about issues and practices of information security management in their organisations. Each item in the construct consist of a seven-point Likert scale ranging from 1=strongly disagree to 7=strongly agree.

Consistent with the conventional process, the questionnaire was pre-tested with four categories of people. In the first stage, the selected individuals were the information security specialists from MAMPU (Malaysian Management and Modernisation Planning Unit of Prime Minister's Department)[1], a Professor from a local university, the information security specialists from private consulting companies and the information security managers from government-linked companies. The pre-testers were asked to indicate ambiguities or difficulties with the instruments and to make suggestions for improvement. After modification was carried out the revised instrument was tested on information security academics and after further revisions a pilot test with potential respondents was carried out. As no significant ambiguities were reported at this stage the pre-testing provided evidence of content validity and the instrument was adopted.

RESULTS

Validity and Reliability of the Research Constructs

Approach to ascertain content validity of the scales has been discussed in the previous paragraph. Here, the discussion revolved around assuring construct validity of the instrument. Multi-item indicators used for measuring the three research variables were tested for construct validity and reliability. The construct validity was evaluated using factor analysis to confirm whether all the items measuring the construct cluster together to measure a single construct. The method of principal component with varimax rotation was used for factor analysis. The minimum factor loading for the construct is more than 0.5, a value considered to be practically significant loading limit (Hair et al, 1998). The internal consistencies of items for each factor are gauged through the computation of Cronbach's coefficient alpha score. As this study is exploratory in nature alpha score of above 0.6 is deemed sufficient for further analysis (Malhotra, 2004; Hair et al, 1998). All scales were found to exceed the minimum threshold of 0.6. The results of each item's factor loading and group's alpha scores are shown in Table 2 and Table 3.

[1] MAMPU is an entity under the Prime Minister's Department, which is responsible for the Malaysian Public Service information security policy and programme implementation.

Underlying Dimensions of Information Security Maturity

In this study, measure of information security maturity used 45 items in the questionnaire. The original number of items was reduced to 23 items after principal component analysis process that also revealed two underlying dimensions as shown in Table 2. The appropriate cut-off significant loading point is 0.5, based on number of sample and the underlying principle of practically significant (Hair et al, 1998).

The first dimension is the management process for *information security maturity*. Analysis of the items highly loaded under the first dimension reveal that they mostly belong to the maturity level 3 to 5 of the information security maturity rankings (Aceituno, 2004; ISACA, 2000). The responses towards the fifteen items showed the mean distribution ranging from 4.17 to 5.09. Most respondents said that in their organisations the intrusion testing is a standard and formalised process lead to improvement (mean=5.09, SD=1.583). This is followed by the practices where information security incidents and response handling responsibilities are assigned, managed and enforced (mean=4.90, SD=1.425). Interestingly the third highest mean for this dimension is also related to security incident handling, where the respondents agreed that root caused analysis of security incidents is the basis for continuous improvement (mean=4.79, SD=1.475).

The second dimension comprised of items that describe risk assessment process. The mean of the distribution of risk assessment variables were more than 4.16. The respondents tend to agree that cost/benefit analysis is increasingly being used to support the implementation of security measures associated with risk assessment findings (mean=4.28, SD=1.355). While most respondents tend to agree that risk assessment process were practiced in their organisation as indicated by items Ism 16 to 17 and 20 to 23 (mean ranging between 4.15 to 4.28), they however tend to disagree that there are defined and documented risk assessment process available as evidenced in their responses to item 18 and 19 shown in Table 2.

In general, the findings suggest that the key players of information security management in MPS think that their organisations had put into practice processes towards achieving information security maturity.

		Mean	Std. Dev.	Loading	Alpha Score
Information Security Maturity					0.944
Ism1	Information security policies implemented and enforced.	4.60	1.474	.811	
Ism2	Information security process and technology are integrated.	4.64	1.650	.787	
Ism3	Critical system inventory strictly maintained.	4.79	1.584	.773	
Ism4	Information security processes co-ordinate with organisational functions.	4.67	1.575	.750	
Ism5	User identification, authentication or authorization is standardized.	4.57	1.354	.738	
Ism6	Clearly assigned responsibility for information security	4.64	1.593	.721	
Ism7	Standard Operating Procedures are defined and fit information security policy.	4.42	1.423	.686	
Ism8	Information security incident and response handling responsibilities are assigned, managed and enforced.	4.90	1.425	.649	
Ism9	Intrusion testing is standard and formalized process leading to improvement.	5.06	1.583	.648	
Ism10	Root cause analysis of security incidents is the basis for continuous improvement.	4.82	1.475	.629	
Ism11	Policies and procedure developed based on security baseline.	4.68	1.347	.625	
Ism12	Pro-active identification of risk is the basis for continuous improvement.	4.17	1.518	.620	
Ism13	Incidents are promptly addressed with formalised incident response procedures supported by automated tools.	4.62	1.344	.594	
Ism14	Responsibilities and standards for continuous service are enforced.	4.69	1.387	.590	
Ism15	Continuous service plans and business continuity plans are integrated, aligned and routinely maintained.	4.23	1.555	.536	

Risk Assessment					0.895
Ism16	An organisation-wide policy defines when and how to conduct risk assessments	4.15	1.408	.860	
Ism17	Risk assessment is a structured, organisation-wide process.	4.20	1.477	.854	
Ism18	Risk assessment follows a defined process that is documented and available to all staff through training.	3.90	1.376	.822	
Ism19	Failure to follow the standard risk assessment procedure is detected by the management.	3.96	1.449	.784	
Ism20	Top management has determined the levels of risk that the organisation would tolerate and have standard measures for risk/return ratios.	4.27	1.423	.772	
Ism21	Risk assessment is conducted when changes affecting organisational asset occur.	4.24	1.319	.747	
Ism22	Cost/benefit analysis, supporting the implementation of security measures, is increasingly being utilised.	4.28	1.355	.660	
Ism23	Informal risk assessments of project-by-project basis take place as determined by each project.	4.25	1.260	.546	

Table 2 Descriptive Statistics and Reliability Analysis of Information Security Maturity

Underlying Dimensions of the Social Factors

The results of factor analysis on the independent variables revealed five social factors as shown in Table 3. They are Organisation Structure, Awareness and Training Culture, Individual Perception on Information Security, Perceived Social Barriers, and Perceived Technical Barriers.

		Mean	Std. Dev.	Loading	Alpha Score
Factor 1: Organisation Structure					0.890
Os1	Information security unit/personnel plays important role in decision-making process about information security.	4.94	1.497	.739	
Os2	The operation of the overall information security structure is evaluated and adjusted to adapt to changing conditions.	4.70	1.396	.687	
Os3	Information security plans and details communicated to all unit/division head.	4.64	1.526	.679	
Os4	Information security unit/personnel get business objectives & needs from relevant unit head.	4.26	1.564	.640	
Os5	Information security awareness communicated regularly to all users.	4.32	1.457	.599	
Os6	Sensitive actions are logged to assign responsibility.	4.68	1.357	.564	
Factor 2: Awareness and Training Culture					0.858
At1	User trained to identify and report suspicious activity	4.41	1.585	.750	
At2	Continuous training for employee	4.34	1.456	.698	
At3	Digital operation data classification	4.22	1.601	.689	
At4	Manual operation data classification	4.52	1.494	.630	
At5	Information security awareness briefing is standardised and formalized.	4.10	1.418	.560	
At6	Checking of information system or network log is daily routine.	4.39	1.736	.550	
At7	Information security awareness briefing is mandatory	3.70	1.562	.534	
Factor 3: Individual Perception on Information Security					0.893
Ip1	Information security important to successful service delivery	5.95	1.333	.753	

Ip2	Information security is important for achieving organisation's goal	5.97	1.294	.739	
Ip3	Unauthorised modification of information is tackled	5.24	1.419	.738	
Ip4	Organisation success rely on exchange of information with other parties	5.39	1.418	.722	
Ip5	Essential service rely on information	5.26	1.605	.683	
Ip6	Unauthorised disclosure is tackled	5.19	1.393	.679	
Ip7	Leader appreciate information security value	5.76	1.338	.674	
Ip8	Organisation gather information to comply with regulation	5.15	1.469	.623	
Ip9	Organisation accumulate sensitive information	5.06	1.418	.620	
Factor 4: Social Barriers					0.798
Ps1	Lack of management commitment.	4.31	1.657	.666	
Ps2	Lack of security awareness among users.	5.11	1.475	.605	
Ps3	Lack of management awareness.	5.21	1.366	.600	
Ps4	Lack of clear Government guideline on information security management.	3.88	1.740	.586	
Ps5	Lack of information security skilled staff.	4.49	1.615	.583	
Ps6	Difficulty proving the value of information security.	4.83	1.440	.576	
Pr2	Lack of time to implement information security process.	4.40	1.438	.562	
Pr3	Balancing the need for meeting business/service objectives and maintaining security.	4.73	1.345	.504	
Factor 5: Technical Barriers					0.668
Pt1	Budget constraints or limitation.	5.33	1.464	.638	
Pt2	Fast pace of information technology change.	5.23	1.308	.563	
Pt3	Rapid changes to the type of attacks on information system.	5.26	1.323	.519	

Table 3 Descriptive Statistics and Reliability Analysis of Five Social Factors

Relationship between the social factors and the information security maturity of organisation

How well do the five social factors influence ISM and which one of the social factors is the most influential was determined by performing linear multiple regressions.

Multiple R	.796				
R^2	.634				
Adjusted R^2	.625				
Standard error	14.057				
		Analysis of Variance			
	DF	Sum of Squares	Mean Square	F	Significance of F
Regression	5	68146.778	13629.356	68.978	.000
Residual	199	39320.557	197.591		
		Variables in the Equation			
Independent Variable	B	SE_B	Beta	t	Significance of t
Individual Perception on Information Security (IPS)	.273	.122	.111	2.750	.027
Organisation Structure (OC)	1.767	.166	.544	10.618	.000
Awareness and Training Culture (ATC)	. 859	.151	.299	5.684	.000
**Perceived Social Barriers (PSB)*	-.040	.141	-.013	-.281	.779
**Perceived Technical Barriers (PTB)*	-.366	.346	-.051	-1.059	.291
(Constant)	22.554	8.201		2.750	.007

Table 4: Predicting Information security maturity (ISM) by five social factors

As depicted in Table 4, three out of five factors were found to be significant predictors of information security maturity. The three significant factors are included in the following model:

ISM = 22.554 + 1.767 (OC) + .859 (ATC) + .273 (IPS)

All three independent variables were significant ($p<0.05$) and they accounted for most of the explained variance (R^2 = .634; Adjusted R^2 = .625). The values for both R^2 and Adjusted R^2 are very close indicating that both contribute much in explaining information security maturity. The value of Adjusted R^2 suggests that 63.4 per cent of what influence the information security maturity of an organisation is explained by the three social factors. Nevertheless the relative importance of each social factor still needs further analysis. Organisation structure has the highest predictor (beta=.544), followed by Awareness and Training Culture (beta=.299) and Individual Perception on Information Security (beta=.111). In summary, clearly Organisation responsibility and communication structure is relatively more important in predicting the information security maturity than the other two social factors.

DISCUSSIONS AND CONCLUSION

The goal of information security management is to establish and maintain a security programme that ensures at least three requirements are met; the confidentiality, integrity, and availability of the organisation's information resources. It is measured through the Information security maturity level, which represent the assessment of security processes in deployed by the organisation.

What these results suggest is that, if an organisation desires to increase its information security maturity level it is more significant to put effort or resources in instituting positive information security culture through top-driven initiatives rather than depending on the individual information security key player. Viewed from another perspective, any individual entrusted with the organisation's information security responsibility will stand a better chance in increasing the information security maturity level if he/she can get senior management's commitment and support before initiating any related programme. Concerted effort between all units dealing with information assets and the senior management drives for continuous improvement will create positive information security culture able to meet the highly challenging information security threats and issues. The findings imply that indeed information security maturity is not exclusive to the technical environment. Improvement to information security posture of the organisation should take into account the process of institutionalising security conscious culture right from the strategic level at the top of the organisation down to the operational level. The findings also suggest that Awareness and Training Culture should not be neglected.

The study succeeded in obtaining empirical evidence of the information security management practices in Malaysian Public Service. The results with regard to processes in practiced are consistent with the international best practices adopted by many organisations worldwide. However, as the study deployed a quantitative method future effort should combine it with the qualitative approach for a more rigorous data of the information security practices and perceptions.

REFERENCES

Aceituno, V. C., (2004) ISM3 1.0. - Information Security Management Maturity Model, Institute for Security and Open Methodology, URL http://isecom.securenetltd.com/Security_Maturity_Model_v3.0.pdf, Accessed 10 Jan 2005

Andersen, W. P. (2001) Information Security Governance, *Information Security Technical Report*, 6(3), 60-70.

Andress, M. (2000) Manage people to protect data, *InfoWorld*, 22(46), November.

British Standard 7799 - A Code of Practice for Information Security Management and Specification for Information Security Management Systems, By the British Department of Trade and Industry Commercial IT Security Group with the British Standards Institution. London: BSI-DISK, 1993, URL http://www.bsi-global.com/Information+Security+Homepage/index.xalter, Accessed 10 March 2003.

Borck, J.R. (2000) Enterprise strategies: Advice for a secure enterprise: Implement the basics and see that everyone uses them, *InfoWorld*, 22(46), November.

Cherns, A., (1976) The Principles of Socio-technical Design, *Human Relations*, 2(9), 783-792.

Information Systems, Audit, and Control Association (2000) COBIT (Control Objectives for Information and Related Technology), 3rd Edition Extracts, IT Governance Institute, Illinois, USA.

Dhillon, G. & Backhouse, J. (2001) Current direction in IS security research: toward socio-technical perspectives, *Information System*, 11(2), 127-153.

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

Ezingeard, J.N. and Bowen-Schrire, M. (2003) Information Security: A Strategic Issue. A conjoint report study, Hanley Management College, UK and Dataföreningen, Sweden, URL http://www.henley.se, Accessed 20 Nov 2004).

Gaunt, N. (2000) Practical approaches to creating a security culture*, International Journal of Medical Information,* 60(2), 151-157.

IT Governance Institute (2003) Board Briefing on IT Governance, URL http://www.isaca.org , Accessed 11 Aug 2004.

Kast, F.E.and Rosenzweig, J.E., (1976) "The Modern View: A Systems Approach" in Beishon, J., Peters, G., (eds.) Systems Behaviour, Second Edition, The Open University Press, 15 – 29, London:Harper and Row.

Kawalek, P., Leonard, J. (1996) Evolutionary Software Development to Support Organisational and Business Process Change: A Case Study Account, *Journal of Information Technology*, 11, 185-198.

Land, F.F., (2000) "Evaluation in a Socio-Technical Context" in Basskerville, R., Stage, J., and DeGross, J.I., Organisational and Social Perspectives on Information Technology, 115-126, Boston: Kluwer Academic Publishers.

Hair, J.F., Anderson, R.e., Tatham, R.L., and Black, W.C. (1998) Multivariate Data Analysis, 5th ed., New York:MacMillan.

Malhotra, N. K. (2004) Marketing Research: An Applied Orientation, 4th ed., New York: Pearson-Prentice Hall.

McAdams, A.C. (2004) Security and Risk Management: A fundamental Business Issue, *The Information Management Journal*, July/August, 36-44.

MS 1536: Part 3 (2002) Malaysian Standard for Information Technology- Guidelines for the Management of IT Security: Part 3: Techniques for the Management of IT Security, Department of Standards Malaysia.

Musekura, J.B. & Ekh, R. (2003) Information Security Issues- Difference between Perception and Practice in Organisations, Orebro University, Sweden, URL http://www.oru.se/oru-upload/, Accessed 20 Nov 2005

Schneier, B. (2000) Secret and Lies – Digital Security in a Networked World, New York:Wiley Computer Publishing.

Siponen, M., (2002) Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned From Software Maturity Criteria, *Information Management and Computer Security*, 10/5, 210-224.

SSE-CMM - System Security Engineering Capability Maturity Model V.3.0 (2003), Carnegie Mellon University, URL http://www.sse-ccm.org/model/model.asp, Accessed 20 Jan 2005.

Tipton, H.F. & Kraus, M. (2000) Information Security Management Handbook, (4th ed), Eds. New York: Auerbach Publications.

Von Solms, B. & Von Solms, R. (2004) The 10 Deadly Sins of Information Security, *Computers & Security*, 23(5), 371-376.

Von Solms, B. (2000) Information security – The third wave?, *Computers and Security*, 19(7), November, 615-620.

Wallace, L., Keil, M. and Rai, A. (2004) How Software Project Risk Affects Project Performance: An Investigation of the Dimensions of Risk and an Exploratory Model, *Decision Sciences*, Spring2004, 35(2), 289-320.

COPYRIGHT