An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization

Azah Anir Norman and Norizan Mohd Yasin
Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
azahnorman@um.edu.my and norizan@um.edu.my

Abstract

The adoption of Information Systems (IS) in many businesses is at a fast tempo in order to be more competitive. This fast adoption is very much supported by the rapid technology advancement and the increasing demand from business stakeholders. Together with the introduction of the Internet with its remarkable features, plus the free-form of policing practiced make the Internet more attractive and engaging. The only problem is this attraction has become the magnet for the abuser to misuse the Internet for their profit. This problem has led to many Information Security study to combat threats and protect the business. However, many studies are focus on the technical and engineering solution, where less work were conducted in the IS, management and business issues. In the context of e-commerce, there are very few studies done to understand the problem faced by this subject. Only few e-commerce company manage IS security as the rest believe it is not important. This preliminary paper is written to study the IS security management on the emergent organization environment (e.g. e-commerce) as to the hierarchical organization is dominant in this research field. A framework of analysis is derived to show the contrast of the research objective above.

1. Introduction

Information Systems Security Management (ISSM) from the emergent organization perspective e.g. the e-commerce is way under study and requires attention from the academician. Although emergent organization may be smaller in size and resources, the threats on the information systems is very much similar and as disastrous as compared to the hierarchical organizations. Although that is the case of current security threats, the steps towards managing information systems security between the emergent organization and the hierarchical organization is very much different in terms of the technology, the people and the procedure. This is agreed by [1], [2], [3], [4] and [5] in their work and the call for such research is highly welcome [1], [2], [3], [6], [7].

In the current information age, there is clearly a challenge in managing security using the conventional approaches [5]. The evolution of business model from being hierarchical-oriented to an emergent organization, form one of the crucial challenges requires serious attention concerning to the Information System Security Management [4], [2], [3]. Current policies and procedure are not ready to support the emergent organization [2]. Emergent organization is very dynamic and appears to have higher volatility feature. This statement is true as findings of [8] appears to show in the evaluation of selected standard approaches, where current standards are succumb to supporting stable environment rather the emergent ones. This is because bigger organizations face bigger threats and different organizations type face different type of threats. As there are many type of organizations and business models, IT environment in these company is unique [9] for example, it has its own unique set of software products, which products may have been evaluated in terms of different IS evaluation schemes, either in part or in full. Due to these factors, evaluators are suggested -particularly in emergent organizations- to take more liberties in modifying the evaluation process for their own purposes [8].

Critical success factors of e-commerce as discussed by [10], [11] and [12] shows that trust factors and security issues are part and parcel of e-commerce success. The critical success factors indicate that all businesses wishing to adopt e-commerce as their business model or as an alternative profit generator must implement security measures vital for competitive advantage. In whole, these e-commerce companies have to understand and implement security measure appropriate to the

business based on current security standards. E-commerce company must be smart in choosing the most appropriate security measure for the business and suitable to support the business objective. If wrong measures are adopted, company may face with serious problem such as waste of resources. Current standards which are widely use such as BS ISO/IEC17799: 2000 fail to look into the content of the standards, rather focus on the processes [13]. The processes also are often abstract and oversimplified. There are no advices given to assist companies in the practice of IS security management. Hierarchical companies with mountain of resources may not face too much problems to practices the standards, but e-commerce company will. Limited resources and time constraint makes the task of IS security management tiresome and in attractive, thus living this most important task aside. Most e-commerce retailers have a business model unique to its own entity and require a dynamic procedure to safeguard its Information Systems. Thus, an Information Systems Security Management (ISSM) supporting a dynamic business model is highly needed. A method appropriate to this business context is required to fast-forward their business to enter the market before their competitors.

This preliminary paper discusses on the past work of researchers in the field of ISSM between the hierarchical organizations vs. the emergent organizations in this case the e-commerce company. This work is conducted to understand the important issues between these organizations and identify required criteria for ISSM by e-commerce business. This paper also highlights some of the critical success factors contributing to the ISSM in an organization. The relationship between required criteria with the critical success factor will be analyzed. This paper will also discuss the importance and contribution of ISSM to sustain in the e-commerce business.

The implementation of ISSM in emergent organization today is precarious and it is a virtue for researchers to carry out empirical and interpretive study to explore ISSM in the emergent organization to better understand the situation. A generalization of solution for ISSM in e-commerce company will be hard to achieve as each business model in e-commerce is volatile. Nevertheless, understanding in a focus context of e-commerce model through this research will bring new insight to our existing knowledge. May with the negative and positive results of this research help enlighten the Internet entrepreneurs to jump start business, thus stay competitive.

2. Literature review on ISSM

Information Systems Security Management (ISSM) today plays an important role in any organization security implementation. Information Systems Security as defined by [14] is the broader view of computer security term, incorporating system analysis and design method, manual information systems, managerial issues and both societal and ethical problems. The same article asserts, computer security connotes threats concepts and the physical and logical techniques applied in protecting the electronic computer and communication systems. Definition above clearly shows that IS security encompasses a broader perspective as compared to computer security (technical oriented). Thus, in this challenging business world today, it is far more cost-effective to view business's IS security plan and management in the IS security basis as issues such as people and procedure are addressed as important as other technical measure in securing company's asset [15] and [16]. Although this has been made clear in [15], [16], [3] and [4], however in actual practice, the adoption and implementation of ISSM is still very low. In the recent Deloitte's annual technology, media and telecommunications (TMT) security survey found that 32 per cent of respondents have reduced their information security budgets in the past year [17]. There are many plausible explanations to this situation and one glaring reason is low management concern about IS security [18]. To raise management involvement in IS security decisions, it is important to convince managers about the benefits of IS security efforts and let them know types of IS security measures effective depending organizational circumstances [3]. Using traditional approaches as IS security effort are no longer suitable as the traditional approaches focuses into technical fixes, which are not pliable with the dynamic nature of business today. The management has to picture IS security effort in holistic point of view and not consider IS security as just another commodity, but sees IS security effort as a booster to the business and the business image among business competitors.

2.1 Previous work of ISSM in the hierarchical organizations vs. the emergent organizations

Information security is not a new field. Information security has a very long history even before the computer existed. Information security, for instance encryption, has been used since human knows how to write. Information security today encompasses more complex scenario compare to the

older days. The introduction of computers together with the development of the Internet technology has change how we handle and secure information. Today many information systems are created to handle sensitive information for the benefit of organizations. The evolving of the technology and new business arrangement in distributing information [19] has made it vital for all business owners and business management to consider IS security effort. One effort that has been discussed in great extends by IS researchers are in the field of ISSM commonly based on standardization namely the BS ISO/IEC17799: 2000. This standard is widely adopted by large organization for their competitive advantages. The adaptation of ISSM not only serves to manage organizations' IS Security resources, but this exercise certifies the organization as being capable of managing its IS Security in the enterprise-wide environment. By being certified, organization is verified (by the standardization body) competent in managing IS security, thus creates a better position for the business in the market among its users. This effort may sound easy as detail guide is provided from the standard, but in actual fact, it takes years to exercise all the processes in the standards, thus make it part of organizations' business process and policy. Although there are many major standards such as BS ISO/IEC17799: 2000, Generally Accepted Information Security Principles (GAISP), Systems Security Engineering Capability Maturity Model (SSE-CMM) and Standard of Good Practice for Information Security are available, most of them fail to look into the content of the standard. The focus were given on the existence of process without further advise to assist the practitioner [13]. Because of this scarcity, the applicability of this standardization toward business becomes tough and timely [2], [3], [13]. The inflexibility of the chosen standards to a business is also questioned. The same scarcity also elevated issues on how well the security activities are carried out in an organization, and how exactly the objectives are to be achieved in organizations [13]. For those reasons, it may provide a false sense of security in an organization. Besides these scarcity, most of the standards are built based on hierarchical organizational experience, practice and structure[2], [7], [20], which are inflexible and has rigid structure [15]. As the business orientation and business objectives between the hierarchical organizations and the emergent organizations are different, using the current standards to achieve ISSM in e-commerce company will be difficult. General information security management standards and guidelines fail to pay adequate attention to the fact that organization differ, therefore their security requirements will differ [7]. Using only one standard is not adequate without further assistance or advice because these guidelines will help different business context. Guideline accompanying any standards as point of reference will be off help even to the novice.

There are different types of ISSM work available today, some researcher focuses on the security design method used e.g. [7]. Others look at the standards and practices e.g. [13], [21]and [22]. Some look into the socio-organization perspective e.g. [5]. All of their works have been published in the top-tier ranking journal and receives significant citations from other research fields besides from the field of information systems. Many of the researcher above look onto the hierarchical organization. Unfortunately, there are not many empirical and conceptual researches on ISSM in emergent organization (e.g. e-commerce business). One reason may be because of the state of e-commerce is still very young in the business as compared to the traditional hierarchical company. Many thing are clearer in the hierarchical company as compared to the emergent organization for example the organizational physical governance, which is important to implement ISSM as claimed by [23].

In order to understand the gap between two different organization orientations, this study tries to classify the previous work of ISSM researcher. This classification is important to analyze the status of the work and identifies the main future research to focus on. Classifications are based on six aspects which derived the framework. These aspects were chosen from selected researches to help shape a new perspective of highly sought research in the ISSM area. The classification framework as Table 1, encompasses six aspects which are: 1)type of research 2)context of research 3)IS category 4)theory used/developed 5)focus benefiter 6)future research. In the types of research, two divisions are identified which are empirical research vs. conceptual analysis. Through the literature analysis, researches in ISSM based on conceptual analysis have higher number as compared to the empirical research. Many conceptual analysis has not been tested, thus empirical research is highly invited. In the context of research, the table is divided in two main research focuses which are the hierarchical organization and the emergent organization. From table 1, it is clear that the emergent organization is under study. As for the IS category, three main IS categories as define by [4], [24], [1], [14] which are people, technology and procedure are being categorize. The focus of ISSM today very much looks on the procedural issues. Less study were carried out to study the people issue. The technology issue is not the focus here as we have already discussed them earlier. In theory used and developed, it highlights theories, which are significant to the selected research. Usually in

empirical research theories are used to prove findings or highlight methodologies used. Thus we could see no theory we discussed in the conceptual study compared to the empirical research. Lastly, future research is included in the matrix, to identify and provide information on the research direction in an emergent organization (e.g. e-commerce). Most researchers agree on adding value towards the success of ISSM in an organization. Researchers also highlighted the importance to study emergent organization such as the e-commerce company and SMEs as these two context needs further help in the effort to manage its IS security. Few theories were being used in the ISSM study were most of them uses standards as point of reference. Very little study looks at the socio-organization aspect which in the context of e-commerce will be vital as it faces different socio-organizational issue different to the traditional-hierarchical organizations. The framework also shows many conceptual works are done to discuss ISSM issues. Empirical research is highly sought to provide more understanding in ISSM from the e-commerce perspective.

Table 1 ISSM Classification Framework

type of research	reseach context		IS category	theory used/developed	future research	seminal work
	HIERARCHY	EMERGE				
empirical research (quantitative and qualitative)	√		people		evaluation of cost-effectiveness user participation in IS	Albrechtsen, E. (2007)
	√		technology		suggest on more studies in e-commerce context	Kankanhalli et. al (2003)
	√		procedure	ISO/IEC 17799	methodology development on Security management in SME	Sanchez et. al (2006)
	√		procedure	Nolan Stage Theory	footprint characterizes its IS/ICT management capability maturity	Jaco R. (2004)
	√		procedure		methodological support of security to systems development processes	Tryfonas, et. al (2003)
	√		procedure	Soft Systems Methodology (SSM) by Checkland (1981)	different approaches of research to add value ascertaining success of ISSM	James H. L. (1996)
		√	procedure	SSE-CMM	fine tune Holistic Security Management Framework (HSMF) and provide guidelines for tailoring.	Zuccato, A. (2007)
conseptual analysis	√		procedure		objectives of security standards to meet organizations and information security management standards are applied.	Siponen M. (2006)
	√		procedure		integrated system development and security method	Richard, B. (1993)
	√		procedure		combination of product and/or systems evaluation with process certification	Eloff and Von Solms (2000)
	√		procedure		future research the ISS metrics by Murine and Carpenter (1984)	Siponen M. (2005)
	√		procedure		test the ISMS model to emergent organization	Steven W. (2008)
	√		procedure		to Implement information security plan using the essential components	Von Solms, B. & Von Solms, R. (2004)
		√	procedure		usability of the meta-policy in security management with respect to security policies	Baskerville, R., & Siponen, M. (2002).

3. Influential factor in implementing ISSM in e-commerce business

E-commerce is a business that is volatile and flexible in nature. Although threats may be the same between large organizations (hierarchical-organization) compared to the e-commerce business, the ISSM in e-commerce business may differ. Organizational factors such as organizational size, top management support and industry type [25] are the most influential factors in IS implementation which has very strong relationship with IS security effort. Thus, leads to the different level of acceptance on ISSM in an organization. Hence, it is proper to consider organizational factors in e-commerce business case, as e-commerce business also has its own size, management and type/services offered. However, organizational factor can bring positive and negative influence towards ISSM implementation in e-commerce. In influential factor, there are two classes. There are the positive influence and the negative influence. The positive influence include the

high staff awareness [26], [27] and requirement by users. As for negative influence, it includes back-burner issues [28], organizational physical governance [23], staff lack of understanding and awareness [26].

High staff awareness promises the high understanding and staff competency in ISSM implementation in the company. This creates a positive influence and feed to the management effort in ISSM. With the high awareness, staff will have higher understanding on the importance of ISSM to the company. Staff will also keep themselves abreast with threats and solution, hence consecutively practices IS security measure without the force from the management. This can only be achieve if the staff has motivation, knowledge, attitudes, values and behavior of how to perceive risk [29]. In positive influence, users' requirement is also seen as vital. This refer to the customer's request of having IS security measure in any IS application provided by the e-commerce company. This is not easy to achieve as seldom customer look for this as part of offer.

The negative influences of ISSM in e-commerce highlight the back-burner issues, which answer the question of why there are still many business fail to employ ISSM in their IS applications. Many managers even among managers who specialize in information technology (IT) [28] know the challenge pose by the growing threats but continue to ignore this fact [30]. Although there are many findings convey IS security [31], [32] is an important issue, IS security implementation is still low. It is not easy to change the managers' perception but this scenario has created the back-burner issues and it continues to happen today. Organizational physical governance is another negative influence towards ISSM in e-commerce. The physical governance of a business determines the ISSM effort of the company. The e-commerce company must have a proper information security organizational structure to make an information security governance plan successful [23]. It is so because without it, there will be no job responsibility dedicated to a specific staff, which will make the ISSM effort worthless. This role is important in communicating the top management requirement among the staff. Finally, lack staff understanding and awareness are part of the negative influence in ISSM effort. It is clear that without staff support and acceptance, ISSM will not be successful. Staffs are IS users, thus they have to be fully educated on the importance of IS security and the impact of their negligence towards the business. The e-commerce company must not relay hundred percent on the staff awareness, but find ways to nurture a positive environment in securing the IS in their company.

4. The critical success factors of ISSM in an e-commerce business

The critical success factors of ISSM are derived from many forces. From authors' analysis of selected journal articles and proceedings, the forces are divided in two main categories; the internal forces and the external forces. Under the internal forces there are four sub-classes including the organizational factors [25], informal component [26], technical component [26], [23] and formal component [26].

Organizational factors consist of top management support, organizational size and industry type. As mentioned earlier, organizational factors are part of critical success factors in ISS effort. This relationship is discussed by [33] [34], [35], [36], in their research. Thus, ISSM is relatively related to organizational factors because ISSM is part of IS security effort.

The informal component sub-class discusses about the information security awareness and staff competency. The informal control such as information security awareness and staff competency is assess as part of the critical success factors as these two components represent the readiness of the business. It is an added advantage for an e-commerce business to have and recruit staff having both qualities because it will facilitate the process of managing IS security.

The formal control component looks at the organization IS security objective and strategy. IS security effort is not a technical issue, rather a business issues requires sound objective and planned strategy for ISSM execution. The management will not be able to derive with comprehensive solutions, thus money will be wasted as a consequence of treating ISSM issue as a technical issues [23].

Finally, the technical component focuses on the security infrastructure and tool or support mechanism. A well-planned strategy with competent staff requires solid infrastructure, tool or support mechanism to execute business objectives. Technical component is an essential requirement in the quest to be successful in ISSM of any business. Any business will not be able to forecast or estimate risk without having tools to help them make decision. There are many tools available such as risk analysis tools, security and monitoring software, which are used by businesses today. It is critical for an e-commerce business to choose the right software for the business following the planned strategy and market standard for e-commerce benefit and success.

As for the external forces, two significant classifications are identified, which are the

government enforcement and users' involvement. Both mentioned classifications have direct impact towards the critical success of ISSM. The government enforcement is a push-factor for e-commerce business to deploy ISSM in the e-commerce business. Without ISSM implementation, the e-commerce business will not be able to enter the market or enjoy benefits the government may provide in the effort of enforcing this regulation. Dissimilar with users' involvement, this classification is seen as a pull-factor because with the rising of savvy users, involvement from savvy users in using secure system will be high. The higher the users' involvement, the stronger e-commerce business is forced to implement IS security effort as such implementing ISSM.

5. The importance and contribution of ISSM to sustain in the e-commerce business

E-commerce business is like any other businesses. It is all about survival. In this network world, e-commerce faces different form of threats from internal and external sources. These threats if not controlled, may bring damages to the business and much worst, force the business to exit the market. There are varieties of control measures available today. The control measures are commonly classified as deterrent and preventive measures [33], [18], [37], [38], [3]). Generally, business takes up different types of security measure suitable to the business needs. Although this is the case, there are little study done to measure the IS security efforts in e-commerce business [3].

Besides survival, it is hoped that with proper ISSM implementation, cost of implementing control will be less or at least equal to the risk confronted [16]. This is the basic assumption found in many risk analysis literature. It is essential that a company to base its information security plan on some type of risk analysis exercise in order to provide measures to mitigate risk associated to the company' information resources [23]. Without a clear understanding of potential threats and the types of assets in the company that required protection, the company may not be able to justify the investment on the control chosen [16]. Further, company will be spending money on risk that may not really be that dangerous to the business information systems and ignoring others which may be extremely serious [23].

A holistic ISSM implementation will optimize the performance of an e-commerce business as ISSM looks into issues concerning technology, people and procedure. Implementation of ISSM with accordance to selected standard or best practice, plus proper exercise in all the e-commerce processes by the employee, will help positioned the company in the benevolence level [39], the highest level maturity. At this level, the e-commerce business who had taken serious attention on ISSM implementation in their e-commerce business will become a benchmark for other e-commerce business efforts and automatically creates a strong business brand for the business, which is as significant as to 'Google' in the search-engine business.

6. Summary and future research

The classification framework discussed earlier show the extent of research gap between hierarchical organization and the emergent organization (in this context the e-commerce company). Focus of research must be given to the e-commerce business to help them implement ISSM for all benefit. The research in understanding the people issues is one of the research gap need to be address using empirical research method. A socio-organizational theory may be off help to understand the different social construction of an e-commerce company, hence providing answer to how best can ISSM fit the e-commerce context.

The influential factor and critical success factors discussed in this paper highlights the major obstacle and motivation in ISSM implementation in e-commerce. This discussion is important to identify the weakest and the strongest point to help close the research gap, thus help proposed the best way in ISSM implementation in e-commerce company.

This paper is our first work of the whole research which is planned to complete in year 2011. Our first work is to identify the current scenario of hierarchical organization vs. emergent organization in implementing ISSM. This will assist us in understanding the problems, implications, benefit, and gaps in current ISSM implementation from the emergent organization perspectives. Consequent work will focus on the empirical research on the identified critical success factors and implication factors of emergent organizations in implementing ISSM mentioned in this work. The research will follow with the identification of common maturity level among the emergent organization as a reference tool to implement and maintain ISSM in emergent organization especially the e-commerce business. Future research also is required to test the maturity level identified in selected e-commerce business cases to understand the applicability and ability of the maturity tool in ISSM implementation and maintenance.

7. References:

[1] T.S. Mikko and O.-K. Harri, "A review of information security issues and respective research contributions," *SIGMIS Database*, vol. 38, no. 1, 2007, pp. 60-80; DOI http://doi.acm.org/10.1145/1216218.1216224.

[2] A. Zuccato, "Holistic security management framework applied in electronic commerce," *Computers & Security*, vol. 26, no. 3, 2007, pp. 256-265.

[3] A. Kankanhalli, et al., "An integrative study of information systems security effectiveness," *International Journal of Information Management*, vol. 23, no. 2, 2003, pp. 139-154.

[4] G. Dhillon and J. Backhouse, "Technical opinion: Information system security management in the new millennium," *Commun. ACM*, vol. 43, no. 7, 2000, pp. 125-128; DOI http://doi.acm.org/10.1145/341852.341877.

[5] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* vol. 11, no. 2, 2001, pp. 127-153.

[6] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logistic Information Management*, vol. 15, no. 5/6, 2002, pp. 337-346; DOI 10.1108/09576050210447019.

[7] R. Baskerville, "Information systems security design methods: implications for information systems development," *ACM Comput. Surv.*, vol. 25, no. 4, 1993, pp. 375-414;

[8] M. Siponen, "Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria," *Emerald Journal*, vol. 10, no. 5, 2002, pp. 210 - 224 DOI 10.1108/09685220210446560.

[9] M.M. Eloff and S.H. von Solms, "Information Security Management: A Hierarchical Framework for Various Approaches," *Computers & Security*, vol. 19, no. 3, 2000, pp. 243-256.

[10] E. Kaynak, et al., "An analysis of the factors affecting the adoption of electronic commerce by SMEs:Evidence from an emerging market," *International Marketing Review*, vol. 22, no. 6, 2005, pp. 623-640; DOI 10.1108/02651330510630258.

[11] S.M. Furnell and T. Karweni, "Security implications of electronic commerce: a survey of consumers and businesses," *Internet Research: Electronic Networking Applications and Policy*, vol. 9, no. 5, 1999, pp. 372-382.

[12] R. Eid, et al., "A cross-industry review of B2B critical success factor," *Internet Research: Electronic Networking Applications and Policy*, vol. 12, no. 2, 2002, pp. 110-123.

[13] S. Mikko, "Information security standards focus on the existence of process, not its content," *Commun. ACM*, vol. 49, no. 8, 2006, pp. 97-100; DOI http://doi.acm.org/10.1145/1145287.1145316.

[14] R. Baskerville, *Designing Information Systems Security*, John Wiley Information Systems Series, 1998, p. 239.

[15] H.L. James, "Managing information systems security: a soft approach," *Proc. Information Systems Conference of New Zealand, 1996. Proceedings*, 1996, pp. 10-20.

[16] R. Baskerville, "Research directions in information systems security," *International Journal of Information Management*, vol. 14, no. 5, 1994, pp. 385-387.

[17] S. Staff, "A third of companies drop their investment in security," *Book A third of companies drop their investment in security*, Series A third of companies drop their investment in security, SC Magazine UK, 2009.

[18] J. Detmar W. Straub, "Effective IS security: An empirical study," *Information Systems Research* vol. 1, no. 3, 1990, pp. 255-276.

[19] C.C. Wood, "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature," *Computer Fraud and Security*, vol. 2004, no. 1, 2004, pp. 16-17.

[20] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Journal of Logistics Information Management*, vol. 15, no. 5/6, 2002, pp. 337 - 346; DOI 10.1108/09576050210447019.

[21] B. von Solms, "Information Security governance: COBIT or ISO 17799 or both?," *Computers & Security*, vol. 24, no. 2, 2005, pp. 99-104.

[22] M.M. Eloff and S.H. von Solms, "Information Security Management: An Approach to Combine Process Certification And Product Evaluation," *Computers & Security*, vol. 19, no. 8, 2000, pp. 698-709.

[23] B. von Solms and R. von Solms, "The 10 deadly sins of information security management," *Computers & Security*, vol. 23, no. 5, 2004, pp. 371-376.

[24] M.T. Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, vol. 8, no. 1, 2000, pp. 31-41; DOI 10.1108/09685220010371394.

[25] P. Ein-Dor and E. Segev, "Organizational Context and the Success of Management Information Systems," *Management Science*, vol. 24 no. 10, 1978, pp. 1064-1077; DOI 10.1287/mnsc.24.10.1064.

[26] J.M. Torres, et al., "Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness " *Lecture Notes in Computer*

Science, vol. 4176/2006, 2006, pp. 530-545; DOI 10.1007/11836810.

[27] Q. Hu, et al., "The role of external and internal influences on information systems security- a neo-institutional perspective," *Journal of Strategic Information Systems*, vol. 16, no. 2007, 2007, pp. 153-172.

[28] D.W. Straub and R.J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, vol. 22, no. 4, 1998, pp. 441-469.

[29] E. Albrechtsen, "A qualitative study of users' view on information security," *Computers & Security*, vol. 26, no. 4, 2007, pp. 276-289.

[30] K.D. Loch, et al., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, vol. 16, no. 2, 1992, pp. 173-186.

[31] J.C. Brancheau and J.C. Wetherbe, "Key issues in Information Systems Management," *MIS Quarterly*, vol. 11, no. 1, 1987, pp. 23-45.

[32] F. Niederman, et al., "Information Systems Management Issues for the 1990s," *MIS Quarterly*, vol. 15, no. 4, 1991, pp. 475-500.

[33] W.D. Nance and J. Detmar W. Straub, "Discovering and disciplining computer abuse in organizations: A field study," *MIS Quarterly*, vol. 14, no. 1, 1990, pp. 45-60.

[34] J.A. Hoffer and J. Detmar W. Straub, "The 9 to 5 underground: Are you policing computer crimes?," *Proc. Management of information systems* Fort Worth, TX: Harcourt Brace., 1994.

[35] J.H.P. Eloff, "Computer security policy: Important issues," *Computers and Security*, vol. 7, no. 6, 1988, pp. 559-562.

[36] D.L. Goodhue and J. Detmar W. Straub, "Security concerns of system users: A study of perceptions of the adequacy of security," *Information and Management*, vol. 20, no. 1, 1991, pp. 13-27.

[37] D.B. Parker, *Computer Security Management* Prentice Hall 1981.

[38] K.A. Forcht, *Computer Security Management* Boyd & Fraser Pub. Co., 1994 p. 486.

[39] H. James, et al., "Software quality and the Capability Maturity Model," *Commun. ACM*, vol. 40, no. 6, 1997, pp. 30-40; DOI http://doi.acm.org/10.1145/255656.255692.

