2008

Strategic Response to the Institutional Process on the Adoption and Assimilation of IS SECURITY MANAGEMENT: A LONGITUDINAL INVESTIGATION

Carol Hsu
National Taiwan University, carolhsu@ntu.edu.tw

Jae-Nam Lee
Korea University Business School, isjnlee@korea.ac.kr

Follow this and additional works at: http://aisel.aisnet.org/ecis2008

Recommended Citation
http://aisel.aisnet.org/ecis2008/88

This material is brought to you by the European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
**Strategic Response to the Institutional Process on the Adoption and Assimilation of IS Security Management: A Longitudinal Investigation**

**Hsu, Carol**, City University of Hong Kong & National Taiwan University, No.1. Sec. 4, Roosevelt Rd, Taipei, Taiwan, carolhsu@ntu.edu.tw

**Lee, Jae-Nam**, Korea University Business School, Anam-Dong, Seongbuk-Gu, Seoul 136-701, Korea, isjinlee@korea.ac.kr

**Abstract**

Institutional theories have been adopted to explain and predict the process of Information Systems (IS) innovation in organisations. However, most institutional-centred frameworks overlook the significance of external economic efficiency and internal organisational capability when organisations consider strategic responses to institutional conformity pressure. Focusing on the diffusion of IS security management as an administrative innovation, this paper develops an integrative framework that illustrates how economic and organisational factors contribute to the organisational decision-making process in the light of institutional influences on the adoption and assimilation of IS security management. The proposed model and hypotheses then plan to be tested using the data collected from two-stage longitudinal study.

**Keywords:** Administrative innovation, IS security management, Institutional theories, Adoption and assimilation, Economic and organisational capability factors
1. INTRODUCTION

Nicholas Carr (2003), in a highly controversial article, argues that the commoditisation of information technology (IT) requires contemporary organisations to place increasing emphasis on “vulnerabilities, not opportunities” (p.11). In reality, information security breaches and external risks such as terrorism and natural disasters have increasingly posed serious threats to the day-to-day running of an organisation. Furthermore, many industry reports have stated that organisational spending on information security has been on the rise for the past few years (Deloitte 2006, Gordon et al. 2006). Even regulatory agencies have introduced compliance requirements—for example, the Sarbanes-Oxley Act—to ensure that companies implement appropriate corporate governance structure. Reflecting on these recent developments, we argue that given the current focus on vulnerabilities protection, contemporary organisations are in the phase of searching for a rationalised security management process to combat these vulnerability concerns and comply with regulatory standards. Conceptually, this rationalised security management process is seen in the form of an innovation.

Researchers in a variety of disciplines have been discovering the conditions that facilitate or hinder the adoption and assimilation of organisational practices. Besides economic-driven motivation on innovation adoption (Bacon 1992), institutional theorists (DiMaggio & Powell 1991, Scott 1995) show that changes in an organisation can be the result of mimetic, coercive, and normative forces, that is, institutional isomorphism. In the field of information systems (IS), many researchers have examined the role of institutional isomorphism in influencing organisations’ decision to adopt or assimilate technological innovations (Chatterjee et al. 2002, Liang et al. 2007, Teo et al. 2003); nevertheless, little has been found not only on adoption and assimilation at the same time but also on the other forms of innovation with the administrative core (Teece 1980, Westphal et al. 1997). This insufficiency of prior research should be addressed, and a more detailed comprehension of the administrative innovation is certainly required. Westphal et al. (1997) argue that academic researchers tend to consider innovation “as a discrete phenomenon” (p.368). Critiquing this assumption, they suggest that in contrast to technological innovations, administrative innovations have no concrete technical features and are subject to multiple interpretations during the diffusion process. Consequently, they contend that the uniqueness of administrative innovations leads to difficulties to “determine conformity from adoption alone; it may be necessary to examine conformity in the form of the innovation adopted or how it is implemented, treating the adoption of such innovations as continuous rather than discrete occurrence (p.368).”

To date, there has not been any available integrative framework depicting how organisations accept and routinise administrative innovations in response to institutional pressure, thus making the conduct of this research necessary. The research objectives of this paper are as follows. First, it is interested in identifying the conditions that shape the spread of an administrative innovation in the context of IS security; second, its interest is on the investigation of the institutional effects at different stages of innovation by separating adoption from assimilation, as suggested by Westphal et al. (1997); and finally, the study aims to analyse the different moderators of institutional conformity at each stage of IS security management diffusion using the data collected from two-stage longitudinal study. As a work in progress, we propose a conceptual model of IS security management and discuss the next step of research and the expected contributions of the work to extant literature and practice.

2. IS SECURITY MANAGEMENT AS AN ADMINISTRATIVE INNOVATION

Surveying the literature, we found that a number of scholars have called for the non-technical approach to IS security research (e.g. Dhillon and Backhouse 2001). Traditional IS security methods
such as checklist, technical standards, and risk analysis have a set of formal and structured rules. As Siponen (2005) argues, user involvement is “passive,” and this might be “problematic in the long run” (p.313). Furthermore, Dhillon and Backhouse (2001) explain that these traditional approaches are no longer appropriate and sufficient “when organisational structures become flatter and more organism-like in their nature” (p.145). Responding to this problem, Siponen and Iivari (2006) suggest that instead of enforcing IS security policies literally, the design of IS security policies should require the input of “application principles to solve such exceptional situations” (p.448). Echoing these arguments, studies on the social-organisational aspect of IS security management have emerged over the past few years. For example, Dhillon and Trokzadeh (2006) adopt value-focusing thinking approach in measuring IS security within the organisation. Siponen (2000) and Straub and Welke (1998) explain the importance of information security awareness. Some have addressed the concept and creation of security culture in organisations (Chia et al. 2002), while others have explored the role of institutional force in adoption (Hu et al. 2006) and the institutionalisation process of IS security management in an organisation (Hsu 2007). Against this backdrop, we consider that traditional IS security methods signify the technical innovation, but these emerging studies characterise the rise of an administrative innovation in the field of IS security management. Many researchers consider innovation as a discrete rather than a continuous phenomenon. Critiquing this assumption, Westphal et al. (1997) suggest that an administrative innovation like Total Quality Management (TQM) should be understood and interpreted at different and multiple levels. Echoing this approach, institutional researchers have looked into the spread of TQM at the national, regional, and international environments (Shannon et al. 1999, Terlaak & King 2006). Building on the same line of argument, we view that the concept of IS security management contains the characteristics of an administrative innovation, as described below.

First, administrative innovation requires interpretation of definitions and procedure; thus, “variation in the form of adoption may be especially high” (Westphal et al. 1997). As Damanpour (1991) notes, administrative innovations are “more directly related to its (the) management” (p.561). IS security management focuses on the development of policy rather than technical requirements (Backhouse et al. 2006). Goodhue and Straub (1991) argue that managerial concern over systems security risk differs because of their individual characteristics and their interpretation of the surrounding organisational environment. Therefore, part of the process of assimilation is the enhancement of senior managers’ risk management skill (Straub & Welke 1998). Thus, because of the management-oriented nature, variance in managing the implementation process among different organisations is likely. Decision makers in various organisations can interpret security management requirements in different ways, thereby impacting the scope and scale of adoption and assimilation in the organisation. Second, the adoption of IS security management is not a one-off project but an approach for continuous security management improvement in order to adapt to changing environmental contingencies. This philosophy fits the notion of an administrative innovation that emphasises the issue of organisation-environment co-alignment (Venkatraman et al. 1994). Straub and Welke (1998) argue that with formalised security planning and on-going feedback within the organisational structure, managers are more aware of security problems, allowing them to match appropriate solutions. Discussing the design of IS security policies and guidelines, Siponen and Iivari (2006) propose that using the prima-facie, utilitarian, or “universalisability” design theory, organizational members can evaluate the total cost of security action (TCSA) in normal and exceptional situations. Furthermore, as part of security management framework, there is a requirement of compliance through regular and ad hoc audit, thus allowing the organisation to detect errors and correct them in the existing controls. In other words, the process enables single-loop organisational learning (Argyris & Schon 1978). Furthermore, the expected update or irregular revision of the standard opens up the window of opportunities for double-loop organisational learning. Third, the diffusion of administrative innovation is associated with the change in the social structure of the organisation. In the case of IS security management, one important philosophy is the notion of employee awareness and security culture (Siponen 2000). Ramachandran and Rao (2006) suggest that management initiatives on security training programme and rewards for security-related behaviours can lead to the creation of security culture. Put differently, the success of an effective IS security
management rests on the extent to which the employee complies with the policy and demonstrates a high level of security awareness and knowledge. Therefore, IS security managers should build up employees’ knowledge capability on how to “deal with exceptional situations in which IS security policies are in conflict with the business objectives of organisations” (Siponen & Iivari 2006). This implies that the assimilation of IS security management must require organisations to have a capability to facilitate the change of employees’ attitude on responsibilities towards IS security and to cultivate a security culture.

As explained above, the philosophy of IS security management has distinct features that fit the concept of administrative innovations. Among empirical research on administrative innovations, the spread of TQM practices is recognised as the dominant subject of the study (Shannon et al. 1999, Terlaak & King 2006, Westphal et al. 1997). However, not much has been studied on the adoption and assimilation of IS security management. Accordingly, this paper concentrates on identifying conditions that affect the spread of this administrative innovation in organisations. In the following section, we first present institutional isomorphism that induces the adoption and assimilation of IS security management.

3. INSTITUTIONAL PRESSURE FOR IS SECURITY MANAGEMENT ADOPTION AND ASSIMILATION

Neo-institutional theorists suggest that practices travel from one organisation to another because of the operationalisation of isomorphism in a social system (Scott 1995). Institutional researchers have shown three different mechanisms of institutional forces: coercive, normative, and mimetic (DiMaggio & Powell 1991, Scott 1995), which, in the case of IS security management, play a role in influencing an organisation’s decision on adoption and assimilation. Coercive isomorphism refers to the political influence stemming from government agencies or powerful organisations such as monopoly or multinational enterprises. Haworth and Pietron (2006) show the relevance between IS security management and the Sarbanes-Oxley Act in the US, while on the other side of the Atlantic, the requirement of the Data Protection Act 1998 acted as the regulatory mechanism for British firms (Backhouse et al. 2006). Hu et al. (2006) also conclude that compliance with regulation has been one of the key drives for implementing IS security management in organisations.

Mimetic isomorphism represents the imitation of one organisation perceived by others as successful or legitimate in an organisational field. Institutional mimicry is more likely to occur for competitive reasons or as a strategy to address uncertainties and ambiguities (DiMaggio & Powell 1991, Guler et al. 2002, Tingling & Parent 2002). Peer influence on the adoption of IS security management was seen in the example of the International Information Integrity Institute to include IS security management standards as part of their materials for risk management (Backhouse et al. 2006). The financial sector in the US has established the Financial Services Information Sharing and Analysis Centre. Having been able to access the same information on emerging security risks, organisations are experiencing “learning mimicry” (Guler et al. 2002) by adopting similar risk management strategies in light of shared information on security threats. However, Hu et al. (2006) conclude that mimetic force plays only a minimum role in shaping management attitude towards IS security. Accordingly, this research also investigates the significance of mimetic force and compares the results against those found by Hu et al (2006).

Normative force represents the collective influences resulting from the development of professionalisation. DiMaggio and Powell (1991) comment that the “mechanism for encouraging normative isomorphism is the filtering of personnel” (p.71). They further suggest that the filtering normally occurs through specialists, promotion of common practices, and development of skill-level requirements for particular jobs. In this field, we see the growth of the Information System Audit and Control Association (ISACA) with more than 65,000 members worldwide, which is an indication of
professionalisation. Associated certifications, such as CISA and CISM, contribute to IS security knowledge development and assimilation. For the past few years, major consultancy firms have been publishing IS security surveys, which in turn help increase management’s awareness and knowledge on this subject. The empirical results of Hu et al. (2006) show that often the CIOs adopt “professional organisations and publications as their sources for ideas and practices” (p.7). Through the professional association and the network of consultants and senior management, we contend that normative pressure will influence a decision on IS security management adoption and assimilation.

From the institutional perspective, this paper has shown that firms are facing conformity pressures from regulatory bodies or from other peer organisations, or through the mechanism of professionalisation. Nevertheless, due to other organisational or economic factors, firms can formulate different strategic decisions in response to external legitimacy pressures (Ang & Cummings 1997, Oliver 1991, Perrow 1985). Among research on administrative innovations, a number of researchers identified various organisational contingencies that influence the adoption of TQM despite institutional pressure (Shannon et al. 1999, Westphal et al. 1997). Building on this line of reasoning, this paper argues that while acknowledging the institutional effects, firms might show different attitudes towards IS security management adoption and assimilation resulting from the influences of other economic or organisational contingencies.

4. STRATEGIC RESPONSE TO INSTITUTIONAL CONFORMITY

As mentioned above, our main theoretical assumption starts with how institutional isomorphism places conformity pressure on organisations during the diffusion process. In our view, the diffusion comprises two stages: adoption and assimilation. This separation of innovation stages is not a new concept in organisational and IS literature. For instance, Zmud (1982) and Damanpour (1991) have applied this approach to examine an organisation’s adoption on innovations. Zaltman et al. (1973) explained that the determinant distinguishing the adoption and assimilation stage rests on the point when the power holders in an organisation legitimise the introduction of new products or practices. Zmud (1982) shared similar assumptions and considered adoption as “represented by an organisational mandate for change” while an assimilation referring to such an innovation “becomes ingrained within organisation behaviours” (p.1422). Cooper and Zmud (1990) have classified the stages separating adoption and assimilation. The former includes the process of initiation and adoption, while the latter consists of adaption, acceptance, routinisation, and infusion.

This research proposes that the relationship between the institutional forces and receptiveness of an organisation to IS security management is moderated by economics-based considerations for adoption decision and by organisational characteristics during the assimilation stage (see Figure 1). Considering the nature of administrative innovation, which is management-oriented and a continuous phenomenon, the researchers contend that in particular, they expect that the moderating variables will differ at the adoption and post-adoption stages. As discussed earlier, administrative innovation can lead to different forms of adoption. In the context of IS security, the adoption can range from simple security policy, taking up ISO 17799 framework, or enterprise-wise security management implementation. Each scenario involves various degrees of investment cost. Different from adoption decision, our previous argument states that the assimilation of an administrative innovation is normally coupled with the process of organisational changes. That is, the success will depend on the organisational capability to manage the assimilation the process.

4.1 Moderators of Institutional Conformity for IS Security Management Adoption

As defined, an adoption decision is made when those who have power in an organisation mandate change. However, scholars have criticised the assumption of complying with take-for-granted social
rules and expectations held by institutional theorists (Oliver 1991, Pfeffer 1982, Zinn et al. 1998). While sharing the viewpoint that organisational behaviours are bounded by the constraints of the external environment, critics argue that instead of passive compliance, organisations normally actively manage their relationship with the environment in which they operate. As Pfeffer (1982) notes, “firms do not merely respond to external constraint and control through compliance to environmental demand. Rather, a variety of strategies may be undertaken to somehow alter the situation confronting the organisation to make compliance less necessary” (p.197).

![Figure 1: Strategic response to institutional conformity for IS security management](image)

For for-profit organisations, research shows that the moderating effect of institutional conformity at the adoption stage is normally economic driven (Ang & Cumming 1997, Oliver 1991). Besides emphasising the importance of social rules and beliefs, the institutional theory should consider the role of organisational self-interests at the adoption stage. In other words, organisational conformity to institutional pressures for IS security management at the adoption stage will rely on economic factors. Recent reports show that commercial organisations are voicing out their concerns over the high compliance cost of the Sarbanes-Oxley Act, which was indicated by the decreasing number and value of initial public offerings in the U.S. capital market (Magnusson 2007). As one report states, regulation “should rely on principles-based rules and guidance, rather than the current regime of detailed prescriptive rules” (Magnusson 2007, p. 60). This statement highlights the importance of economic cost and benefit analysis for adoption decision. Therefore, by considering the economic standpoint to account for the adoption process of IS security management, this paper proposes three critical factors such as perceived environmental uncertainty, perceived competitive advantage, and availability of resources, which can either strengthen or weaken the relationship between institutional influence and the adoption of IS security management, as described below.

**Perceived Environmental Uncertainty:** Pfeffer and Salancik (1978) define environmental uncertainty as “the degree to which future states of the world cannot be anticipated and accurately predicted” (p.67). When decision makers fail to acknowledge or misinterpret the sources and potential consequences of environmental uncertainties, the impact can be a serious decline in organisational performance or damage in organisational legitimacy in the institutional environment (Elenkov 1995). One strategic response to environmental volatility is through inter-organisational imitation (Haunschild & Minner 1997). In IS security management, environmental uncertainty refers to the unpredictability of major trends or risks in the business environment, or the difficulties in determining the likelihood and impact of different security risks to the survival of the organisation. Chang and Ho (2006) show that there is a positive relationship between environmental uncertainty and implementing IS security management. With such a high degree of environmental uncertainty, managers are
searching for appropriate risk management methodologies to assist their decision-making process (Baskerville 1991). Therefore, we hypothesise that organisations conform to external pressures to adopt IS security management when they perceive greater environmental uncertainty.

**H1:** The greater the level of environmental uncertainty perceived by the organisation, the greater the likelihood of organisational conformity to institutional pressures on the adoption of IS security management.

**Perceived Competitive Advantage:** In a hypercompetitive and globalised business environment, organisations and market participants increasingly find the need to deploy signaling strategies to potential customers and business partners in an attempt to differentiate their products and services from those of lower quality. In the economics literature, this has been understood as the “Lemons problem” where the market experiences the problems of information asymmetry. There is a growing practice of using certification schemes as an effective counteracting mechanism. Terlaak et al. (2006) report that complying with TQM practice can generate greater product volume or yield a higher price premium. In a survey by the DTI/PWC (2006), a respondent commented that achieving security management certification made his company become “more commercially acceptable to the public sector”. Kankanhalli et al. (2003) also argue that management investment in effective security management can lead to competitive advantage. Therefore, we hypothesise that when an organisation perceives an increase in competitive advantage, it is expected to confirm more keenly to institutional influences on IS security management adoption.

**H2:** The greater the level of market competitive advantage perceived by the organisation, the greater the likelihood of organisational conformity to institutional pressures on the adoption of IS security management.

**Availability of Resources:** Discussing the economic determinants of organisational innovation, Rosner (1968) contends that the resources available to an organisation determine whether the organisation can afford innovation. He also argues that available resources allow firms to obtain the innovation, absorb the cost of unsuccessful implementation, and implement the innovation by exploring new ideas. Other researchers have shown the moderating effect of organisational available resources in response to institutional pressure (Ang & Cummings 1997, Zinn et al.1998). Therefore, we argue that the availability of organisational resources is particularly important when organisations have difficulties in projecting the return of investment. Available resources allow firms be flexible in investing additional human resource for administrative innovation as well as in absorbing the failure cost (Kaluzny et al. 1993). In IS security management, the annual CSI/FBI computer crime and security survey also show the management’s doubts in using return on investment or internal rate of return (IRR) to quantify the cost and benefit aspects of computer security investment (Gordon et al. 2006). Under this circumstance, organisations with greater available resources are more willing to accommodate environmental demand even when the possible return is unclear. Therefore, when organisations possess available resources, they are more likely to conform to the institutional pressure.

**H3:** The greater the availability of organisational resources, the greater the likelihood of organisational conformity to institutional pressures on the adoption of IS security management.

4.2 Moderators of Institutional Conformity for IS Security Management Assimilation

When the power holders in the organisation decide to adopt a certain practice, the next important question in the innovation diffusion phase is to what extent the adopted organisational practices are accepted by internal organisational members and become institutionalised. This study defines this as the stage of assimilation. As discussed earlier, the introduction of administrative innovation involves the reassignment of tasks and responsibilities as well as continuous improvement. That is, an innovation should be considered as a process of organisational learning and should be incorporated into the organisation value chain (Fichman & Kemerer 1997, Zhu et al. 2006). Technology innovation
theorists suggest that there usually exists an assimilation gap, that is, actual usage tends to lag behind the adoption of technology, which results not only from insufficient knowledge to leverage the technology but also from the misalignments between the technology and the internal environment (Fichman & Kemerer 1999). This shows that assimilation is an important stage worthy of research, while its success needs to be interpreted from an organisational capability perspective (Gallivan 2001). Therefore, by adopting the organisational capability viewpoint to explain the routinisation process of IS security management, this study selects three important factors, which have been most frequently mentioned in prior studies, as described below.

**Top Management Support:** Management support is believed to be a critical element for any successful innovation assimilation (Gallivan et al., 1994, Zmud, 1982). Damanpour (1991) argues that managerial support is “especially required in the implementation stage, when coordination and conflict resolution among individuals and units are essential” (p.558). Bantel (1989) shows the significance of the top management team in relation to innovation decision in the banking sector. The role of top management has been found to be much more important in the assimilation stage than in the adoption process (Liang et al., 2007). Therefore, the strong participation of top management results in implementing efficient innovation process and activities intended to assimilate them (Ba et al. 2001). Studies on IS security management also show that top management support has a positive impact on increasing security effectiveness (Kankanhalli et al. 2003, Straub & Welke 1998). So, stronger top management support leads to a higher degree of assimilation of IS security management.

**H4:** The stronger the top management support, the stronger the relationship between institutional influences and IS security management assimilation.

**IT Capability:** An organisation manages its innovations through an IT infrastructure, which is a framework connecting different members of the organisation with different internal and external knowledge and processes (Tippings & Sohi 2003). Bharadwaj (2000) defines IT capability as “an ability to mobilise and deploy IT-based resources in combination or co-present with other resources” (p.171). The capability allows an organisation to connect not only people to people, but also people to innovation activities, such as IS security management (Junarkar 1997). The usefulness and roles of IT in the diffusion process have been widely discussed (Teece et al. 1997). For example, Gill (1995) emphasises that using IT to support organisational learning because of modern IT can best support the amount and richness of bi-directional information flow, multi-channel communication, and the performance of tasks that cannot be performed manually. This can eliminate communication barriers among different parts of an organisation in the process of technological diffusion (Teece 1986). Accordingly, we argue that this is notably important when the nature of innovation is administrative oriented. With a good IT infrastructure, firms can quickly adjust given the changing environmental contingencies. Chang and Ho (2006) also show the positive relationship between business managers’ IT competence and the implementation of IS security management. Therefore, this paper hypothesises that when IT capability is high, firms conform to external pressures to assimilate IS security management.

**H5:** The greater the IT capability, the stronger the relationship between institutional influences and IS security management assimilation.

**Cultural Acceptability:** Diffusing administrative innovation in an organisation is as much a social activity as a managerial and/or technical activity, so cultural change is a prerequisite for its successful assimilation (Klein 1998, Miller & Friesen 1980). Organisational culture involves shared meanings, norms, and values that have been collectively constructed over the years. That is, the creation and change of an organisational culture usually take a long time and are context or climate dependent (Schein 1985). To survive in a rapidly changing competitive market, organizations must consider how to adapt themselves to the dynamic environment from a long-term perspective rather than a short term one. According to Leonard-Barton (1988), the success of innovation diffusion depends on the degree
of mutual adaptation of the innovation and the organisational context into which the innovation is being introduced. Similar to the line of argument on IT capability, cultural acceptability equally plays a vital role to support the organisational learning process during the assimilation stage. Put differently, if a supportive organisational culture for IS security management does not exist, there will be no motivation for organisation members to engage in activities relevant to the newly introduced practices (Gallivan 2001). Thus, one can expect the relationship between institutional influence and the assimilation of IS security management to be higher when the cultural acceptability of innovation is high.

**H6: The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences and IS security management assimilation**

5. RESEARCH METHOD

This study adopted a field survey method. The proposed model and hypotheses were tested empirically using two-stage longitudinal study that was conducted three months apart. The unit of analysis was the organisation implementing or which had already implemented enterprise-wide IS security initiatives. The researchers designed survey instruments to measure one independent (i.e., institutional influence), two dependent (i.e., adoption and assimilation of IS security management), and six moderating variables. Based on previous literature on institutional theories and the adoption and assimilation of innovation especially from the economics and organisational capability viewpoints, we developed a questionnaire to test the proposed hypotheses empirically.

Most of the measures were based on previously validated instruments, while others were developed based on conceptual definitions and theoretical statements made in the existing literature. For example, institutional influences were measured in terms of three major pressures including mimetic (Teo et al. 2003), coercive (Liang et al. 2007, Tingling & Parent 2002), and normative pressures (Ang & Cummings 1997, Teo et al. 2003). Regarding the two dependent variables, measures of adoption were developed by applying Azjen and Fishbein’s definition to the context of IS security (Azjen & Fishbein 1980), while its assimilation was measured by the best-known six-stage model of the assimilation of technology innovation in organisations developed by Cooper and Zmud (1990). Each variable was measured based on a seven-point Likert scale. To account for the extraneous sources of variation in the adoption and assimilation stage, we incorporated organisation size, industry type, and time length after IS security management was introduced as control variables in the models. An initial version of the survey instrument was subsequently refined through an extensive pre-test with several academicians and practitioners. The instrument was further tested with 10 companies in Korea that have already adopted IS security management.

This study is currently in the stage of data gathering. The sampling frame of this study came primarily from 500 large firms identified in the Book of Listed Firms in Korea as of 2006. To increase the response rate, the Total Design Method proposed by Dillman (1991) will be applied to two separate surveys in Phases 1 and 2. Questionnaires will be mailed to CIOs in the selected organisations in Phases 1 and 2 with personalised cover letters accompanying an explanation of the study and assurance of confidentiality of collected data. As top IS executives can be expected to be knowledgeable about the adoption and assimilation of their IS security management, they will be selected as key informants in this study. In Phase 1, a survey will be conducted for adoption-related factors such as perceived environmental uncertainty, perceived competitive advantage, and availability of resources at the start of their IS security management projects. In Phase 2, three months later, this study will contact companies participating in the survey of Phase 1 for a follow-up survey to in order determine the status of the assimilation process of IS security management in terms of three organisational capability factors, including top management support, IT capability, and cultural
acceptability. To test the hypotheses of the study, we plan to use hierarchical moderated logistic regression models.

6. EXPECTED CONTRIBUTIONS AND CONCLUDING REMARKS

In response to the recent emphasis on technology vulnerabilities in the organisational field, this study identifies IS security management as an administrative innovation that decision makers can adopt to manage security risks. Furthermore, drawing from the institutional perspective, the study shows that institutional rules and norms place conformity pressure on firms for adoption and assimilation. It also shows how economic-based factors and internal organisational capabilities affect the relationship between institutional influences and the adoption/assimilation process from a longitudinal perspective. We argue that this research will contribute not only to the literature of institutional theories but also to the area of IS security management. The integrative framework described in this paper provides a better understanding of the diffusion process of administrative innovations, that is, adoption and assimilation; it also can be used as an analytical tool in investigating organisational strategic behaviours at different stages of innovation diffusion in the light of institutional conformity influences. In addition, the framework contributes to the “still at a theory-building stage” of the social-organisational perspective in IS security research (Dhillon & Backhouse 2001).

References


