Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Institutional Influences on Information Systems Security Innovations

Carol Hsu, Jae-Nam Lee, Detmar W. Straub,

To cite this article:
Carol Hsu, Jae-Nam Lee, Detmar W. Straub, (2012) Institutional Influences on Information Systems Security Innovations. Information Systems Research 23(3-part-2):918-939. https://doi.org/10.1287/isre.1110.0393

Information Systems Research
Vol. 23, No. 3, Part 2 of 2, September 2012, pp. 918–939
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.1110.0393

Institutional Influences on Information Systems Security Innovations

Carol Hsu
National Taiwan University, Taipei 10617, Taiwan, carolhsu@ntu.edu.tw

Jae-Nam Lee
Korea University Business School, Seoul 136-701, Korea, isjnlee@korea.ac.kr

Detmar W. Straub
Georgia State University, Atlanta, Georgia 30302, dstraub@cis.gsu.edu

This research investigates information security management as an administrative innovation. Although a number of institutional theories deal with information systems (IS) innovation in organizations, most of these institutional-centered frameworks overlook external economic efficiency and internal organizational capability in the presence of pressures of institutional conformity. Using Korea as the institutional setting, our research model posits that economic-based consideration will moderate the institutional conformity pressure on information security adoption while organization capability will influence the institutional confirmation of information security assimilation. The model is empirically tested using two-stage survey data from a field study of 140 organizations in Korea. The results indicate that in addition to institutional influences, our six proposed economic-based and organizational capability moderating variables all have significant influences on the degree of the adoption and assimilation of information security management. We conclude with implications for research in the area of organizational theory and the information security management literature, and for practices regarding how managers can factor into their information security planning the key implementation variables discovered in this study. The robust setting of the study in Korean firms allows us to generalize the theory to a new context and across cultures.

Key words: administrative innovation; information security management; institutional theories; adoption and assimilation; economic; organizational; IT capability factors

History: Vallabh Sambamurthy, Senior Editor, William Kettinger, Associate Editor. This paper was received on April 13, 2009, and was with the authors 21 months for 2 revisions. Published online in *Articles in Advance* January 9, 2012.

1. Introduction

Organizations normally consider the value of information communication technology (ICT) as the mechanism that allows them to create and maintain competitiveness both in physical and virtual marketplaces. Nevertheless, given the increasing levels of commoditization of information technology (IT), it is clear that information security breaches and risks that exploit an organization's technical and human behavior vulnerabilities pose increasingly serious threats to the day-to-day running of global organizations. (Gordon and Loeb 2002). Korea, the context in which this empirical investigation takes place, has a highly developed ICT infrastructure.[1] The strong growth of electronic commerce in Korea, which was reported to reach approximately USD 17 billion in 2009, is another indicator of how companies have seized opportunities brought by the widespread adoption and usage of IT. However, the maturing of IT infrastructure and firms' increasing reliance on IT has also led to a rise in information security breaches. For instance, the number of reported cases of personal information violation has increased by 25% from 2005 to 2009. About 30% of Korean companies reported the illegal disclosure of company internal confidential information in 2008 in comparison to 15% in 2005.[2] As a result, the Korean regulatory agencies have introduced a series of compliance requirements to ensure that companies implement appropriate information security management. For instance, the "Act on Personal Data Protection" came into force in 2009; it aims to make it mandatory for business sectors to comply with requirements of personal data protection including online financial transactions.[3] In 2005, the Financial Supervisory Commission also issued guidelines and requirements for security of electronic financial transactions and best practices for corporate governance. Reflecting on

[1] OECD broadband statistics. http://www.oecd.org/dataoecd/21/57/39574824.xls (accessed April 13, 2009).

[2] *Source*. http://www.dt.co.kr/contents.html?article_no=2008061802012369-661001 (accessed April 1, 2009).

[3] *Source*. http://www.csokorea.org/news/download.asp?idx=3348 (accessed March 2, 2009).

these developments in the recent past, we argue in this study that Korean managers are searching for a new, rationalized security management process to manage risks, preserve the confidentiality, integrity, and availability of information, and ensure the business continuity of their organizations. Conceptually, this renewed effort at rationalization of security management can be seen as a form of administrative innovation.

Administrative innovations have been viewed in this light before. First, an innovation is "any idea, practice, or material artifact perceived to be new by the unit of adoption" (Zaltman et al. 1973, p. 158). Ideas and practices that lag in adoption or that are recombined or repurposed may thus be seen as "new" even if the adopting unit views them as regular practices carried out as a part of organizational policy. As Westphal et al. (1997, p. 368) argue, "[Administrative] innovations can potentially include many routines that can be combined in different ways." In this sense, administrative innovation is synonymous with organizational change, however major or minor it may appear to be. It is thus conceptually related to change management.

Incorporating administrative innovations into business processes is not a trivial task. Researchers in a variety of disciplines have discussed the conditions that facilitate or hinder the adoption and assimilation of organizational innovations. Among them, institutional theorists (e.g., DiMaggio and Powell 1991, Scott 1995) have shown that changes in an organization can result from external institutional influences. In the field of information systems (IS), several researchers have examined the role of institutional isomorphism on an organization's decision to adopt or assimilate technological innovations (Chatterjee et al. 2002, Iacono et al. 1995, Liang et al. 2007, Teo et al. 2003).

However, there has been little focus on both adoption and assimilation in a single study, or indeed on other forms of innovation with an administrative core (Teece 1980, Westphal et al. 1997). This research gap should be addressed because a more detailed understanding of information security as an administrative innovation could be highly useful for practice, and it has theoretical implications as well. We believe that Korea is an appropriate setting to examine both adoption and assimilation at the same time. Korean firms are evidently quick and responsive in management style and technology adoption (e.g., Bae and Lawler 2000, Lau et al. 2005). In Koreas' *palli palli* business culture,[4] top management pushes forward new product development and introduction to shorten the time to market (Blasi and Puig 2002). Enhancing response speed is one of the key dimensions of evolving Korean business strategies (Bae 1997). Therefore, Korea could be an ideal place where both adoption and assimilation can be tested in a short period of time in a single study.

No integrative framework depicting how organizations adopt and assimilate administrative innovations in response to institutional pressures exists, thus making the conduct of this research timely. Our research questions are threefold. First, *what conditions shape the diffusion of an information security administrative innovation*? Second, *what are the institutional effects occurring at different stages of innovation adoption and assimilation, as suggested by Westphal et al.* (1997)? Finally, *what moderates institutional conformity during each stage of information security management adoption and assimilation*? Addressing these questions, our proposed model and its hypotheses test data collected from a field study of Korean IT managers.

The remainder of the paper is organized as follows. In the next section, we describe the theoretical background for considering information security management to be an administrative innovation. In §3, we discuss our research framework in the context of information security management; based on the related literature, this section proposes a number of hypotheses. Section 4 introduces our research methodology, and §5 contains analysis and results. In §6, we consider implications as well as future research directions. The last section summarizes findings and overall contributions.

2. Theoretical Background

2.1. Information Security Management as an Administrative Innovation

A review of the literature makes it clear that researchers have used different theoretical lenses to critically assess information security research. Dhillon and Backhouse (2001) applied Burrell and Morgan's framework, whereas Siponen (2005) analyzed five classes of traditional information security methods. Recently, Siponen and Willison (2007) examined information security research between 1999 and 2004 via Laudan's reticulated model of science. Whereas each of these models advances our understanding of information security, none view the phenomenon as an innovation in general, or an administrative innovation in particular, which, we argue, is a legitimate and well-suited theoretical lens.

The theoretical lens applied in the current study is that information security is an administrative innovation rather than a technological innovation. Technological innovation would focus on developments

[4] "*Palli palli*" means "quickly, quickly" in Korean. The term once had a negative connotation for perhaps the too-rapid economic growth of Korea, but recently it has had a resurgence in linguistic use to represent fast information technology adoption and decision making in Korean firms and Korean society generally.

in security technologies, whereas information security management fits with the philosophy of administrative innovation because, as defined in this study, it refers to *the development of a security management program including the security policy, management committee, team structure* (*e.g., CISO or security officers*), *risk-management process, and employee education to preserve the confidentiality, integrity, and availability of information in organizations*. The implementation of such a program involves restructuring and investment in human resources and knowledge development through different levels of organization. This is similar to what Teece (1980, p. 465) describes as the requirement of "major reassignment of tasks and responsibilities."

When security is treated as a technological innovation, research is normally placed under the umbrella of "computer security." This perspective has been the dominant research perspective for the past few decades (Siponen and Willison 2007, Straub et al. 2008). Viewing information security as a technological innovation and with an eye to investment, Cavusoglu et al. (2004, 2005) studied the value of IT security architectures, while Gordon and his colleagues researched the economics of the information security capital expenditures (Gordon and Loeb 2001, 2002). However useful this perspective is, some scholars have argued that research based on the technological innovation paradigm has significant limitations. Dhillon and Backhouse (2001, p. 145) explain that these technical-centric approaches are not appropriate or sufficient "when organizational structures become flatter and more organism-like [sic] in their nature."

Echoing these perspectives, in recent years, Ransbotham and Mitra (2009, p. 122) say that "research on the organizational perspective [of information security management] is limited but emerging." Such studies appropriately characterize what we see as administrative innovations in information security management. This very different stress on the essentially managerial nature of information security is relevant for a number of reasons. As Straub et al. (2008, p. 5) observe,

> . . . it likewise indicates as clearly as possible that the likely problem today is not the lack of technology, but its intelligent application. The management of information security is in its infancy.

This viewpoint was supported by our observation that although many organizations have adopted information security practices during the last decade (e.g., Backhouse et al. 2006, Hsu 2009, Ransbotham and Mitra 2009), it is still difficult to make the business case to top management that increased investment in information security is necessary as a successful information security program. In Korea, despite the rising number of security breaches, the portion of Korean firm's investment in information security is still low. As of 2008, the average security of a Korean firm is about 1% of the total IT budget.[5] Furthermore, unlike the United States or other European countries, the position of the chief information security officer (CISO) or chief security officer (CSO) rarely exists in Korean companies. Therefore, we argue that, overall, information security is still in the primitive stages in terms of the management of information security rather than in terms of the extensiveness of security technologies adopted by organizations. This is one reason why information security still needs to be considered as an administrative innovation.

If information security should be studied as an administrative innovation, how shall we go about this? First, administrative innovation requires precise interpretation of definitions and enumeration of procedures even though "variation in the form of adoption may be especially high" (Westphal et al. 1997, p. 367). Damanpour (1991, p. 561) argues that administrative innovations are "more directly related to its management," while Ransbotham and Mitra (2009, p. 122) indicate that information security management focuses on "managerial actions that promote a secure environment." Goodhue and Straub (1991) argue that managers' concerns over systems security risk differ because of their individual characteristics and their interpretation of the surrounding organizational environment. Thus, because of the managerial orientation of the implementation process, there are likely to be variations in the way it is managed. In other words, decision makers may interpret security management requirements in different ways, and this will impact the scope and scale of adoption and assimilation.

Second, in that information security implementation is typically much larger than a one-off project, the adoption of information security management involves continuous security management improvement and change management to adapt to varying environmental contingencies. This philosophy fits the notion of an administrative innovation that emphasizes the issue of organization-environment coalignment (Venkatraman et al. 1994). Straub and Welke (1998) argue that, with formalized security planning and ongoing feedback within the organizational structure, managers become more aware of security problems, and this allows them to find appropriate solutions more easily.

Third, the diffusion of administrative innovations is associated with ongoing changes in an organization's social structure. In information security management,

[5] *Source*. http://www.dt.co.kr/contents.html?article_no=2008061802012369661001 (accessed March 21, 2009).

the notion of employee awareness and security culture is an important element of policy. Management initiatives in the form of security training programs and rewards for security-related behavior can lead to the creation of a security culture (Ramachandran and Rao 2006). That is, the success of information security management depends on the extent to which employees comply with the policy and demonstrate a high level of security awareness and knowledge. Therefore, information security managers should continually expand employees' knowledge so they can "deal with exceptional situations in which information security policies are in conflict with the business objectives of organizations" (Siponen and Iivari 2006, p. 468). This implies that, to assimilate information security management and cultivate a security culture, organizations must be able to induce changes in employee attitudes as well as their sense of responsibility toward information security.

2.2. Institutional Pressure for Information Security Management Adoption and Assimilation

Based on these definitions of administrative innovations and, in particular, information security innovations, it needs to be noted that, according to neo-institutional theorists, practices travel from one organization to another as a result of social isomorphism (Scott 1995). Researchers on isomorphism describe three mechanisms that make up these institutional forces, namely, coercive, mimetic, and normative isomorphism (Dimaggio and Powell 1991, Scott 1995). First, *coercive isomorphism* refers to the political influence exerted by government agencies or powerful organizations such as supervisory authorities within an industry. Second, *mimetic isomorphism* describes how organizations imitate other organizations to be perceived as successful or legitimate. Institutional mimicry is more likely to occur for competitive reasons or as a strategy to address uncertainties and ambiguities (Guler et al. 2002, Tingling and Parent 2002). When organizations are able to access the same information about emerging security risks and best practices, they engage in a "learning mimicry" (Guler et al. 2002, p. 216) by adopting similar risk-management strategies. According to Hsu (2009), this competitive mimicry has influenced the institutionalization process of information security certification in the Taiwan financial industry. Third, *normative isomorphism* examines the collective influences resulting from the development of professionalization. DiMaggio and Powell (1991, p. 71) observe that the "mechanism for encouraging normative isomorphism is the filtering of personnel," while Hu et al. (2006, 2007) note that "the impact of normative forces seem to be more selective and context specific" (Hu et al. 2006, p. 7) and thus varies among individuals in an organization. The context-dependent nature of normative pressure is also evident in the work of Teo et al. (2003). In their research, normative pressure exhibits the strongest impact on the intention to adopt a financial electronic data interchange system in Singapore. They reason that Singapore's historically strong association with trade might account for the dominance of normative pressure. Given the contextual element of normative pressure, in this study, we will first explore its relevance in our setting via intensive interviews with practitioners before the development of a theoretical model. The description of our interviewing approach and the qualitative results that justify our research model will be discussed in the next section.

3. Theoretical Framing

From an institutional perspective, the above discussion shows that firms face pressures to conform from regulatory bodies or other peer organizations. Nevertheless, there is also evidence that firms can formulate different strategic decisions in response to external legitimacy pressures (Ang and Cummings 1997, Oliver 1991, Perrow 1985). Furthermore, in addition to institutional pressure on adoption, a number of studies also point out the relevance of environmental factors in the post-adoption context (Hirt and Swanson 2001, Gosain 2004). For instance, Butler (2003, p. 215) elaborates on the "institutional tension" among various social actors during the development of Web-based IS development due to their commitments to the external "communities of practices." Liang et al. (2007) argue for the value of external communication at the assimilation stage (Damanpour 1991) and further analyze how the institutional isomorphism can affect managerial actions and the extent of enterprise resource planning (ERP) assimilation in organizations. Hsu (2009) also determined that the competitive mimicry plays an important role in how a financial institution planned and organized its information security certification process. In their review on the use of institutional theory in IS research, Mignerat and Rivard (2009) point to a number of studies where institutional forces are significant in the assimilation of various IS practices such as the business-to-business electronic market (Son and Benbasat 2007) and outsourcing (Miranda and Kim 2006). Following this line of reasoning, we argue that, while acknowledging institutional effects, firms might exhibit different attitudes towards information security management adoption and assimilation because of the influence of various internal and external organizational contingencies. In other words, given the institutional pressure to conform, these contingencies affect the extent to which organizations attribute importance to information security management as an administrative innovation.

3.1. A Two-Step Approach to Develop an Integrative Model

In that the current study attempts to identify the relevance of three institutional forces in information security management in Korea, and within the identified scope, we further wish to develop the other constructs that influence information security adoption and assimilation in this setting. To address this operational issue, we engaged in a two-step approach to flesh out our nomology: (1) an in-depth literature review and (2) intensive interviews with practitioners to validate and supplement the literature review. A similar strategy has been adopted in prior studies, especially when their research topics were replete with different theoretical perspectives (e.g., Ransbotham and Mitra 2009).

3.2. Results from Step 1: Insights from the Prior Literature

In the first step, the in-depth literature review, we identified two major forces: an economic-based force for adoption and an organizational capability force for assimilation. Because these two forces can be applied to any organizational adoption and assimilation, how they operate in the information security management domain is unknown. In a mature area of study where the two forces that underlie a focal adoption or assimilation are well known, prior literature is usually sufficient to identify relevant factors or drivers. However, given that we are early in the process of seeing information security management as an administrative innovation, we felt that further legwork was needed with the nomology.

Given that institutional isomorphism places conformity pressure on organizations during the diffusion process, it is important to note that this process has two stages: adoption and assimilation. Zmud (1982, p. 1422) portrays adoption as the "organizational mandate for change," while Fichman and Kemerer (1999) define assimilation as the point when an innovation becomes embedded within organizational activities. Wang (2008, p. 11) already corroborates this when he says that "the applicability of institutional theory should be extended from studying adoption and implementation to examining assimilation." Liang et al. (2007) associates the interaction between top management and the external institutional pressure with the assimilation of ERP systems in organizations.

According to the existing literature, the relationship between institutional forces and the receptiveness of an organization to information security management is moderated by two major bases: (1) *economic-based considerations for adoption decisions* (Ang and Cummings 1997, Oliver 1991) and (2) *organizational capability considerations during the assimilation stage* (Fichman and Kemerer 1999, Gallivan 2001).

3.2.1. Economic-Based Considerations for Adoption. An adoption decision is made when those who have organizational power mandate actual change. However, scholars have criticized the assumption of complying with taken-for-granted social rules and expectations held by institutional theorists (Oliver 1991, Pfeffer 1982, Zinn et al. 1998). While sharing the viewpoint that organizational behavior is bounded by the constraints of the external environment, critics argue that instead of passive conformity, typical organizations actively manage their relationship within the environment in which they operate. As Pfeffer (1982, p. 197) notes, "Firms do not merely respond to external constraint and control through compliance to environmental demand [such as regulation or expectations of peer organizations and society]. Rather, a variety of strategies may be undertaken to somehow alter the situation confronting the organization to make compliance less necessary."

Research taking on the economics perspective stresses the moderating effect of institutional conformity in the adoption stage of for-profit organizations (Ang and Cummings 1997, Oliver 1991). In other words, organizations that conform to institutional pressures for information security management in the adoption stage do so mainly for economic reasons. For instance, in the report published by the U.S. Committee on Capital Market Regulation in November 2006, committee members argued that "certainly one important factor contributing to this trend [loss of U.S. public market competitiveness] is the growth of U.S. regulatory compliance costs and liability risks" (Zingales et al. 2006, p. x) and recommended that one "should rely on principles-based rules and guidance, rather than the current regime of detailed prescriptive rules" (Zingales et al. 2006, p. xii). In our interviews with practitioners, we found that because security management policy and certification are considered to be new initiatives by many Korean companies, the decision on adoption and assimilation normally requires a careful cost and benefit evaluation. These statements highlight the importance of economic factors in organizational decisions involving the conformity pressure of institutional forces.

3.2.2. Organizational Capability Considerations for Assimilation. As discussed earlier, the introduction of an administrative innovation involves the reassignment of tasks and responsibilities as well as continuous improvement. In other words, an innovation ideally involves organizational learning and should be incorporated into the organizational value chain (Fichman and Kemerer 1997, Zhu et al. 2006). Technology innovation theorists note the presence of an assimilation gap where actual usage lags behind the adoption decision (Fichman and Kemerer 1999). This lag results from insufficient knowledge to leverage

the technology as well as misalignment between the technology and the internal environment (Fichman and Kemerer 1999). It also shows that assimilation is an important stage worthy of intensive research and that its success or failure needs to be interpreted from an organizational capability perspective (Gallivan 2001). As noted earlier, the diffusion of an administrative innovation is associated with a change in the organizational social structure, for example, the creation of a security culture. During our interviews with practitioners, most of them consistently emphasized the importance of management support and organizational capability when assimilating information security management practices adopted. Indeed, the organizational capability viewpoint has been used to explain the routinization process of information security management (Chang and Ho 2006, Junarkar 1997).

3.3. Results of Step 2: Major Forces and Key Factors Derived from the Interviews

Consequently, our second step following the extensive literature review was to conduct 10 qualitative interviews with managers in charge of information security management and top IS managers in IT departments in five Korean firms: Samsung Electronics, LG Electronics, Hana Bank, Woori Bank, and IBM-Korea. The purpose of the interviews was to validate and supplement critical factors or drivers identified in the extant literature with managers who were leading information security management initiatives. The interviews were semistructured, and each interview lasted about two hours. As prescribed techniques preclude prompting interviewees (Ryan and Bonfield 1975), the interviews began by asking what each organization had done regarding information security management. This was followed by three open-ended, unstructured questions: (1) What led the organization to implement information security management initiatives? (2) What were the critical success factors or drivers of the adoption and assimilation of information security management, respectively? and (3) What difficulties did the organization face in adopting and assimilating these practices?

As pointed out earlier, the literature review uncovered conflicting evidence of the significance of normative isomorphism on organizations. Our first interview question allowed us to explore whether the normative force is truly relevant in the diffusion process, at least in the Korean setting. When asked about the initiative, most respondents refer to the development of recent regulations and what other firms are currently doing. One respondent highlighted that "we are expecting something similar to SOX here, what we would call K-SOX, to be implemented. Everyone is talking to each other about how to prepare for it." We realized from the interviews that most large firms try to share important information regarding new regulations so that they can find a better way to cope efficiently with the new environmental pressure together. This means that in our exploratory interviews, we found little evidence of the role of normative isomorphism in this particular context. Furthermore, when we began to arrange the interviews, the intention was to locate the CISO or the senior manager with the delegated responsibility for company information security management. However, we found out that most Korean firms do not have the official position of CISO, but rather assign top IS managers to all security issues (Shin 2009). Thus, there was a lack of recognition that there could be or should be an information security professional specializing in this subfield. Concluding from the literature review and our qualitative interviews, we thus decide to restrict the scope to coercive and mimetic isomorphism for this particular study.

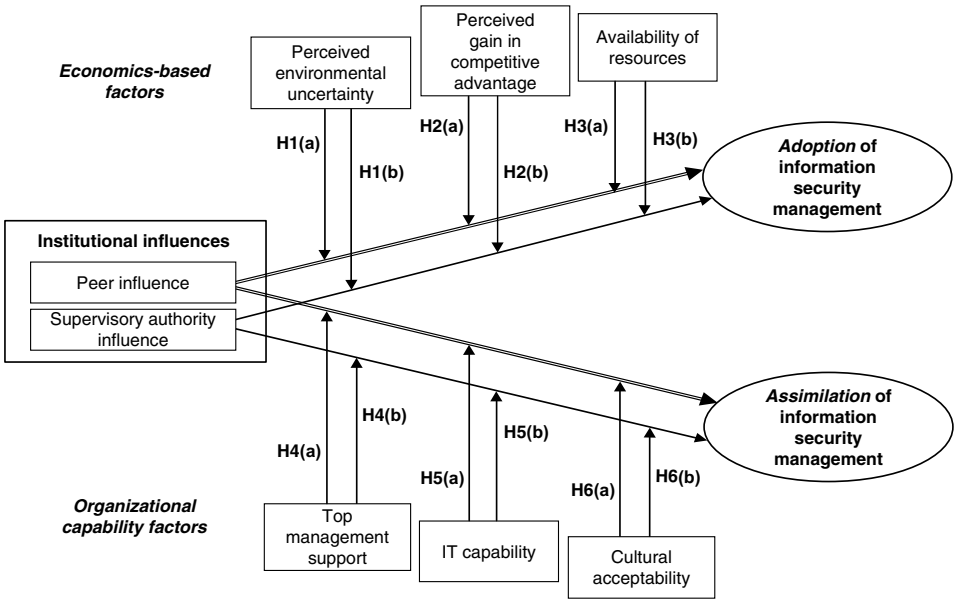
Regarding the moderating variables, this step also involved thematic analysis of the interview scripts (Miles and Huberman 1994) in which notes were codified, issues clustered into factors, and finally, factors classified into two different themes. The themes captured a set of factors that were persistent influences on adoption and assimilation processes. All in all, the important factors that surfaced via these interviews were *three economic-based adoption factors* of information security management: (1) environmental uncertainty, (2) competitive advantage, and (3) resource availability, and *three organizational capability-based assimilation factors*: (1) top management support, (2) IT capability, and (3) cultural acceptability. Our synthesis of critical factors fit nicely into the two broad forces identified in the prior literature. See Appendix A in the online supplement for complete details.[6]

4. Enhanced Research Model and Hypotheses

The result of the two-step method was an enhanced research model of information security adoption and assimilation, as shown in Figure 1. Drawing from the institutional theory on innovation diffusion, we posit that organizational decision to adopt and assimilate information security management practices are influenced by the supervisory authority and peer organizations. As mentioned earlier, administrative innovation can lead to different forms of adoption. Given the nature of administrative innovation, which is a management-oriented and continuous phenomenon, we expect that moderating variables will differ between the adoption and assimilation stages.

[6] An electronic companion to this paper is available as part of the online version at http://dx.doi.org/10.1287/isre.1110.0393.

Figure 1 Research Model for Institutional Influences on Information Security Innovations



In information security, adoption can range from a simple security policy, standardizing on the ISO/IEC 27002 framework, for instance, to an enterprise-wise security management implementation. Each scenario involves different levels of investment. In contrast to adoption decisions, our argument is that the assimilation of an administrative innovation is normally coupled with the process of organizational change; that is, success will depend on the organization's ability to manage the assimilation process. We will next develop the posited relationships.

4.1. Moderators of Institutional Conformity for Information Security Adoption

4.1.1. Perceived Environmental Uncertainty. Organizational theorists have long been interested in the relationship between organizations and their environments and argued that coping with uncertainty is a vital organizational survival skill (Duncan 1972, Milliken 1987). Pfeffer and Salancik (1978, p. 67) define environmental uncertainty as "the degree to which future states of the world cannot be anticipated and accurately predicted." One strategic response to environmental volatility involves interorganizational imitation (Ang and Cummings 1997, Haunschild and Minner 1997). In information security management, environmental uncertainty refers to the unpredictability of major trends or risks in the business environment, and the possible security risks induced by the emerging technologies that organizations deploy to enhance operational efficiency and effectiveness (Chou et al. 1999, Straub et al. 2008). Chang and Ho (2006) show that there is a relationship between environmental uncertainty and implementing information security management. In our interviews, numerous respondents pointed to the rapid technological development in network and mobile technologies in Korea and how this posed a challenge to ensure the confidentiality and availability of information. This reflects the increasing number of hacking incidents reported to the Korean Ministry of Information and Communication (MIC) from 15,940 in 2008 to 21,230 in 2009.[7] Companies, hence, were hoping to find appropriate security management practices to deal with the rapid changing technological environment. Therefore, we hypothesize that organizations conform to external pressures to adopt information security management when they perceive greater environmental uncertainty.

Hypothesis 1 (H1). *The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures—*(a) *peer influence and* (b) *supervisory authority influence—to adopt information security management innovations.*

4.1.2. Perceived Gain in Competitive Advantage. Ang and Cummings (1997) observed that firms are more likely to conform to institutional requirements if doing so results in a gain in production economics. In the hypercompetitive and globalized business environment, organizations and market participants increasingly find it necessary to deploy signaling strategies to potential customers and business partners that differentiate their products and services from those of lower quality. Kankanhalli et al. (2003)

[7] *Source*. http://www.itstat.go.kr/eng/ (last accessed April 8, 2009).

also argue that management investment in effective security management can lead to competitive advantages. In Korea, because of high-volume electronic commerce transactions, customers are very sensitive to how companies are protecting their personal information. Most Korean banks, such as Wooribank and Hanabank, are seeking information security certification to increase customers' confidence in online financial transactions. Therefore, we hypothesize that when an organization perceives an increase in its competitive advantage, it is expected to conform more completely with institutional influences on information security management adoption.

Hypothesis 2 (H2). *The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures—*(a) *peer influence and* (b) *supervisory authority influence—to adopt information security management innovations.*

4.1.3. Availability of Resources. Discussing the economic determinants of organizational innovation, Rosner (1968) contended that the resources available to an organization determine whether it can afford innovation. Other researchers have shown the moderating effect of available resources in response to institutional pressure (Ang and Cummings 1997, Zinn et al. 1998). Available resources allow firms to be flexible in investing in additional human resources for administrative innovation as well as in absorbing failure costs (Kaluzny et al. 1993), which is important when organizations have difficulty achieving a return on investments. In terms of information security, Straub et al. (2008, p. 7) explain that information security management is also an "economic decision" and it usually "requires resources." In the context of our empirical investigation, many Korean organizations are Chaebol, i.e., large conglomerates made up of multiple enterprises, with access to abundant financial and nonfinancial resources. In other words, firms with larger resources, ones that can tolerate more risk and engage in larger investments in security management, hence are more likely to conform to institutional pressure.

Hypothesis 3 (H3). *The greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures—*(a) *peer influence and* (b) *supervisory authority influence—to adopt information security management innovations.*

4.2. Moderators of Institutional Conformity for Information Security Assimilation

4.2.1. Top Management Support. 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 and Jackson (1989) discuss the significance of the top management team in relation to innovation decision-making in the banking sector. In addition, it has been found that the role of top management is much more important in the assimilation stage than in the adoption process (Liang et al. 2007). Thus, the strong participation of top management results in the implementation of an efficient innovation process and activities intended to assimilate these innovations in the organization (Ba et al. 2001). In the information security management literature, Kankanhalli et al. (2003) and Kotulic (2004) both point to the importance of top management in supporting information security management programs in organizations. In Korea, the unique structure of Chaebol and the *palli palli* nature of business practices mean that the top management support can lead to a centralized impact from information security management across different business enterprises. Thus, we hypothesize that stronger top management support will lead to a higher degree of assimilation of information security innovations.

Hypothesis 4 (H4). *The greater the top management support, the stronger the relationship between institutional influences—*(a) *peer influence and* (b) *supervisory authority influence—and information security management assimilation.*

4.2.2. IT Capability. Bharadwaj (2000, p. 171) defines IT capability as "an ability to mobilize and deploy IT-based resources in combination or copresent with other resources." The capability allows an organization to connect people to people as well as people to innovation activities, such as information security management (Junarkar 1997). We argue that IT capability is especially important when the nature of the innovation is administratively oriented. With a sufficient IT infrastructure, firms can quickly adjust to changing environmental contingencies and facilitate the organizational learning process. Chang and Ho (2006) also found a positive relationship between business managers' IT competence and the implementation of information security management. Furthermore, while the importance of the information security maturity model has been emphasized in prior literature, a recent interesting view is that the degree of information security maturity needs to be assessed using a capability perspective (e.g., Chiang et al. 2008). Aligning with that perspective, our qualitative interviews with practitioners also highlighted the importance of the IT capability. Many interviewees emphasized IT capability as a key factor of information security management assimilation. This outcome was almost intuitive in that Korea firms have experienced a successful technology-based transition since

the 1980s, and IT capability has played a critical role in this transition with the *palli palli* business practices (Choung 1998). Based on the above discussion, we hypothesize that when IT capability is high, firms are more inclined to conform to external pressures to assimilate information security management.

Hypothesis 5 (H5). *The greater an organization's IT capability, the stronger the relationship between institutional influences*—(a) *peer influence and* (b) *supervisory authority influence—and information security management assimilation*.

4.2.3. Cultural Acceptability. Similar to the line of argument on IT capability articulated above, cultural acceptability plays an equally vital role in supporting the creation of a *security culture* and the enhancement of employees' security awareness during the assimilation stage. In framing an information security strategy, Baskerville and Dhillon (2008) identify several competencies required to manage information security, e.g., the competence to maintain policy flexibility, the competence to communicate the necessity for information security procedures, and the competence to facilitate informal communication about information security. In her empirical investigation on IS security certification implementation in a financial institution, Hsu (2009) found that the lack of organizational culture partly contributes to the ineffectiveness of IS security management implementation because employees did not change their attitude and behaviors about IS security.

The issue of culture was also mentioned by practitioners in our exploratory qualitative interviews, noting that, if a supportive organizational culture for information security management does not exist, organizational members will not be motivated to engage in activities relevant to the newly introduced practices (Gallivan 2001). Several interviewed professionals stressed the importance of the cultural issue in assimilating information security management. They said that because Korea is one of the most collectivist countries (Hofstede 1980), cultural harmony and acceptability in Korean organizations is strongly valued whenever they introduce new administrative innovations such as information security management. Thus, the relationship between institutional influence and the assimilation of information security management should be stronger when the cultural acceptability of an innovation is high. This leads to our final hypothesis.

Hypothesis 6 (H6). *The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences*—(a) *peer influence and* (b) *supervisory authority influence—and information security management assimilation*.

5. Research Methodology

A field study methodology was adopted to validate the model, but, as explained above, the model itself was developed, in part at least, through qualitative techniques such as interviews. Hence, overall, the study adopted a mixed-methods approach. The hypothesized research model was tested empirically via a questionnaire that collected data about information security management projects in Korea. Data were gathered at two points in time from 140 organizations over a three-month period. In keeping with our desire to capture security management practices as administrative innovations, the unit of analysis was organizations that either were in the process of implementing or had already begun implementing enterprise-wide information security initiatives.

5.1. Development of Measures

Based on theory and prior empiricism, we developed a questionnaire to test the proposed hypotheses. We designed scales to measure two independent variables (i.e., institutional influence, which includes both peer influence and supervisory authority influence), two dependent variables (i.e., the adoption and assimilation of information security innovations), and six moderating variables. Multiple seven-point Likert scales, from "strongly disagree" to "strongly agree," were used to assess each of the variables. All final measures are shown in Appendix B in the online supplement.

Measures were based not only on previously validated instruments, but also on conceptual definitions and theoretical statements drawn from the literature. For example, the institutional influences of information security management, such as external social pressures to conform, arise primarily from peer organizations and supervisory authorities (Ang and Cummings 1997); hence, they were measured via major mimetic forces (Teo et al. 2003) and coercive forces (Liang et al. 2007, Tingling and Parent 2002).

Regarding the two dependent variables, the measures of adoption were developed by applying Ajzen and Fishbein's (1980) definition to the domain of information security.[8] Assimilation of innovation was measured by modifying the well-known six-stage model of the assimilation of technology innovation in organizations by Cooper and Zmud (1990). The focus of our study is on understanding the degree of diffusion of an innovation across the organizational

[8] Because our focus was to collect the data for either the most recently adopted information management standard or an information security management standard that was being considered at the point of our survey, we decided to use the measures for adoption *intention* rather than adoption itself. By using the adoption intention measures and asking respondents to answer all questions retrospectively, we could collect more data from more companies.

activities and processes. Therefore, by distinguishing assimilation from adoption, we developed new items to describe the level of routinization and embeddedness of information security related activities. Meanwhile, measures of the six moderating variables were created in two ways: (1) by adapting existing measures to the research context, e.g., availability of resources (Zinn et al. 1998) and top management support (Kankanhalli et al. 2003); or (2) by converting the definitions of the constructs and theoretical statements into a questionnaire format,[9] e.g., perceived environmental uncertainty (Baskerville 1991), perceived gain in competitive advantage (Terlaak and King 2006), IT capability (Bharadwaj 2000), and cultural acceptability (Gallivan 2001).

To account for the extraneous sources of variation in the adoption and assimilation stages, we added control variables for organization size, IT budget, industry type, the information security practice adopted, and the length of time after the most recent information security practice was adopted. Organizational size was measured in terms of total revenue. Consistent with prior studies, the IT budget was assessed as a percentage of total revenues. Industry type was controlled via classifications for manufacturing, banking/finance, insurance, health care, utilities/energy, retail/warehouse, and transportation. Information security maturity was measured by asking respondents to indicate the standard or framework of information security management (e.g., ISO/IEC 27002 or COBIT) under which they were operating. Finally, we controlled for the length of time after the most recent information security practice was introduced to an organization to eliminate any potential spurious effect of time in information security adoption and assimilation.

To ensure the integrity and validity of the instrument, a pretest and a pilot test were conducted. These tests showed that the instrument was ready for full-scale testing. Details of these tests can be found in Appendix C in the online supplement.

5.2. Sample and Data Collection

The sampling frame for this study was compiled from 500 large firms listed in Maeil Business Newspaper's Annual Corporation Reports in Korea. The main survey was conducted in two phases. The purpose of the first phase was to investigate adoption-related factors while the second phase tried to check on the progress of information security management innovations by investigating assimilation-related factors. To increase the response rate, the total design method proposed by Dillman (1991) and Sivo et al. (2006) was applied in Phases 1 and 2 via two separate instruments. Before mailing out the questionnaire, we phoned the top IS managers to explain the research objective and invite them to be respondents. Questionnaires were then mailed to the top IS managers with personalized cover letters that explained the study again and guaranteed the confidentiality of the collected data. One week after the questionnaires were sent out, a follow-up postcard was mailed, and four and seven weeks later, the same questionnaires were mailed again in both phases.

More specifically, the survey in Phase 1 covered adoption-related factors, such as perceived environmental uncertainty, perceived gain in competitive advantage, and availability of resources at the start of their information security management projects. Respondents were asked to select the most recently adopted information security management practice and answer questions regarding that project. Out of the 500 firms, the questionnaire was mailed to 436 top corporate-level IS managers that were willing to participate in the research. A total of 183 firms responded to the first phase survey for a response rate of 42%. Of the 183 responses, 12 were not related to information security management, and 20 were discarded due to incomplete data. Thus, a total of 151 responses could be used for Phase 2.

In Phase 2, which started three months after the completion of Phase 1, a follow-up survey was initiated by contacting the companies that participated in the Phase 1 survey. Because of Korea's *palli palli* business culture, we believed that the generally accepted six-month time gap between two data collection points in a longitudinal study would not be appropriate. Thus, during the first survey in Phase 1, we asked respondents to tell us what would be the best timing to check their progress in assimilating information security management. The average value of the responses was around three months. Thus, we decided to start the second survey in Phase 2 three months after the completion of Phase 1. In consciously choosing this three-month period, we believed that we were better able not only to enhance data timeliness but also to minimize data distortion and attrition between data collection points, thereby increasing the validity of the data collected. To determine the status of the information security management assimilation process, the top IS managers of the 151 firms were asked to answer questions pertaining to three organizational capability factors, namely top management support, IT capability, and cultural acceptability. Out of the 151 responses, 145 were received, but five were

[9] For the newly developed measures, we used the small-scale card sorting method recommended by Moore and Benbasat (1991).

eliminated due to incomplete data. Thus, 140 valid responses could be used for the final analysis. The initial response rate, therefore, was approximately 96%. Before the final analysis, common method variance and nonrespondent bias were ruled out as described in Appendix D in the online supplement.

Respondent characteristics in terms of industry type, total sales revenue, IT budget as a percentage of total sales, and information security practice adopted are summarized in Appendix E in the online supplement. Industry representation of the respondent organizations shows that many were either manufacturers or they were involved in the banking/finance industry. Of the 140 companies who participated fully in Phase 2, 82 had total annual sales of one billion dollars or more. In addition, information security standard ISO/IEC 27002 was adopted by 49 firms, COBIT by 15, and BS 7799 (part 2) and BS 7799 by 27 and 26, respectively.

6. Analysis and Results

6.1. Analysis Method

Partial least squares (PLS) was selected to evaluate the proposed model and its hypotheses for the following reasons. First, PLS is suitable for assessing theories in the early stages of development (Fornell and Bookstein 1982). Because this study is an initial attempt to advance a theoretical model by investigating information security management as an administrative innovation, the fit of PLS to exploratory science argued in its favor. Moreover, PLS does not have severe distributional assumptions and can readily handle both formative and reflective measures in a model. This study used the PLS-Graph version 3.00 for analyzing the measurement and structural models.

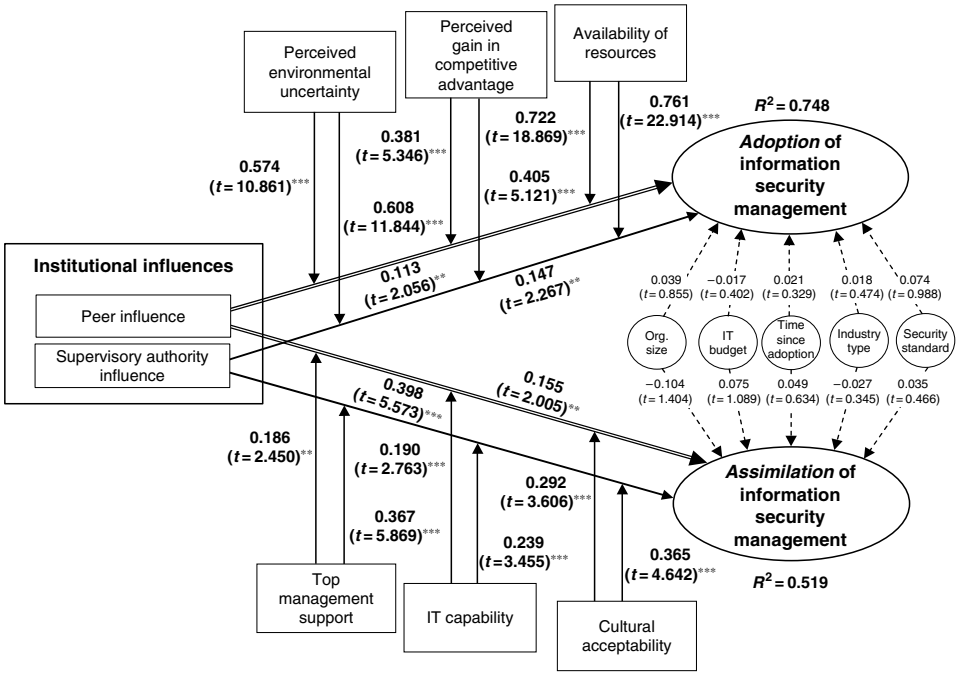
6.2. Measurement and Structural Models

For the measurement model, following the recommended two-stage analytical procedures (Hair et al. 1995), a confirmatory factor analysis was initially conducted to assess the measurement model, after which the structural relationship was examined. This approach ensured that our results regarding the structural relationship were based on construct-valid indicators in the measurement model. Details of tests of the measurement model are described in Appendix F in the online supplement.

With an adequate measurement model and an acceptably low level of multicollinearity, the hypotheses proposed in this study were tested with PLS. The results of the analysis of the structural model are depicted via path coefficients and *t*-values in Figure 2. Test of significance of all paths in the structural model was performed using a bootstrap resampling procedure with resampling of 500.

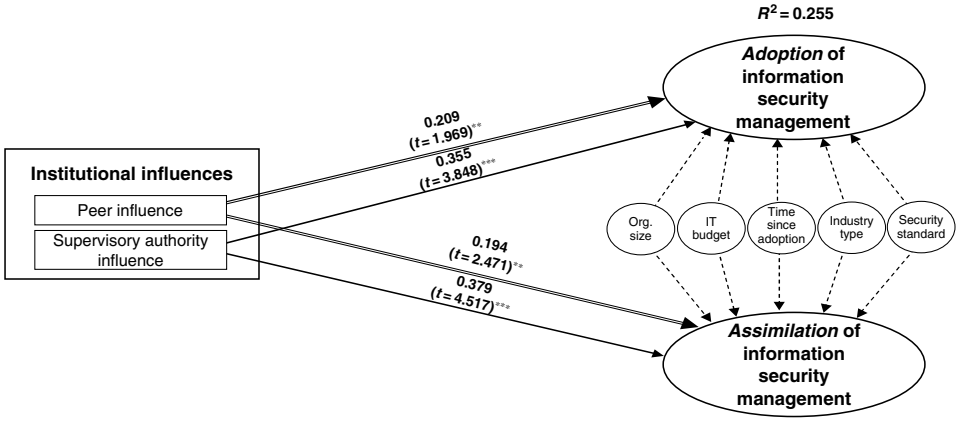
Figure 2 shows the results of the PLS analysis, including the path loadings, *t*-values of the paths, and *R*-squares. All 12 hypothesized paths were found to be significant without exception at our 0.05 alpha pro-

Figure 2 Results of PLS Run



*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

Figure 3 The Baseline Model



*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

tection level.[10] Also, none of the five control variables showed any significant relationship with the adoption and assimilation processes. It is worth mentioning that *R*-square values of the adoption and assimilation of information security management are 0.748 and 0.519, respectively. As this evidence makes clear, the adoption and assimilation processes can be influenced by various political, economic, and environmental variables. This result indicates that in addition to institutional influences, the six moderating variables selected in this study have significant influences on the degree of the adoption and assimilation of information security management and should be paid more attention in further studies. We will next examine the results in greater detail.

6.2.1. Explaining the Adoption of Information Security Management. We note that, as expected, both peer influence ($\beta = 0.113$; $t = 2.056$; $p < 0.05$) and supervisory authority influence ($\beta = 0.147$; $t = 2.267$; $p < 0.05$) had significant effects on the adoption process. Furthermore, as shown in Figure 2, all three economic moderators significantly influence the relationships between peer influence and the adoption process ($\beta = 0.574$, $t = 10.861$, $p < 0.01$ for perceived environmental uncertainty; $\beta = 0.381$, $t = 5.346$, $p < 0.01$ for perceived gain in competitive advantage; $\beta = 0.722$, $t = 18.869$, $p < 0.01$ for availability of resources) as well as between supervisory authority influence and the adoption process ($\beta = 0.608$, $t = 11.844$, $p < 0.01$ for perceived environmental uncertainty; $\beta = 0.405$, $t = 5.121$, $p < 0.01$ for perceived gain in competitive advantage; $\beta = 0.761$, $t = 22.914$, $p < 0.01$ for availability of resources). These findings support H1(a), H1(b), H2(a), H2(b), H3(a), and H3(b).

To confirm the interaction effects of the three moderators, we followed the hierarchical process, recommended by Chin et al. (2003), a process that compares the results of two different models in terms of the difference in *R*-squares, i.e., one without the moderator and one with. According to Cohen (1988), the difference in *R*-squares can assess the overall effect size f^2 at three different levels: 0.02∼0.14 for small effects, 0.15∼0.34 for medium effects, and above 0.35 for large effects.[11]

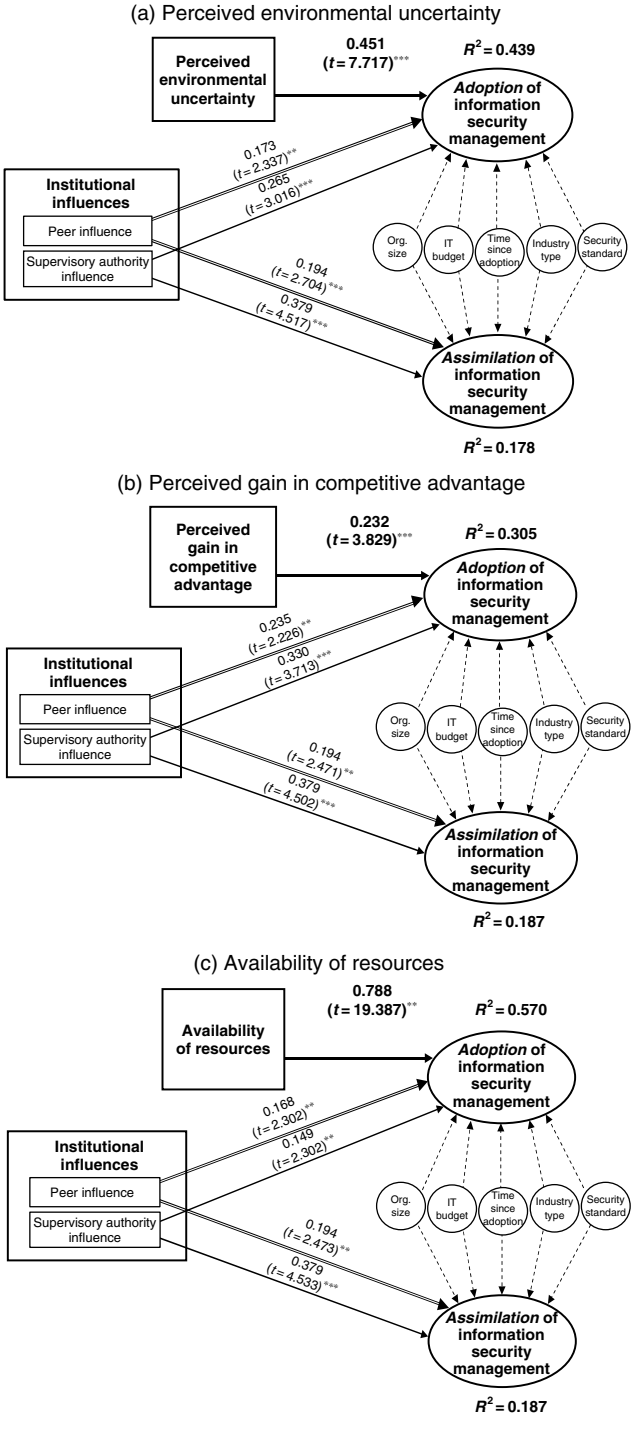
As a first step, the baseline model without three economic moderators was tested, as shown in Figure 3. This model accounts for 25.5% of the variance in the adoption of information security management. The effects of peer influence and supervisory authority influence on the adoption had *p*-values below the 0.05 level. We then examined the direct effect of each economic factor on the adoption process. As illustrated in Figures 4(a), 4(b), and 4(c), the results of the analyses showed that *R*-square values of perceived environmental uncertainty, perceived gain in competitive advantage, and availability of resources were 0.439, 0.305, and 0.570, respectively. Finally, the moderating effect of each economic factor on the adoption process was assessed. The results, as summarized in Figures 5(a), 5(b), and 5(c), showed that the models account for 55% of the variance in the adoption process in the case of perceived environment uncertainty, 42.8% in the case of perceived gain in competitive advantage, and 67.4% in the case of availability of resources.

Based on the hierarchical difference tests, the interaction effects were found to have effect sizes f^2

[10] To check the validity and generalizability of the findings, we reran Overall, the analysis using the data collected from the first round of survey (i.e., adoption model only) and found that the findings of the adoption model are similar to the overall findings of this study.

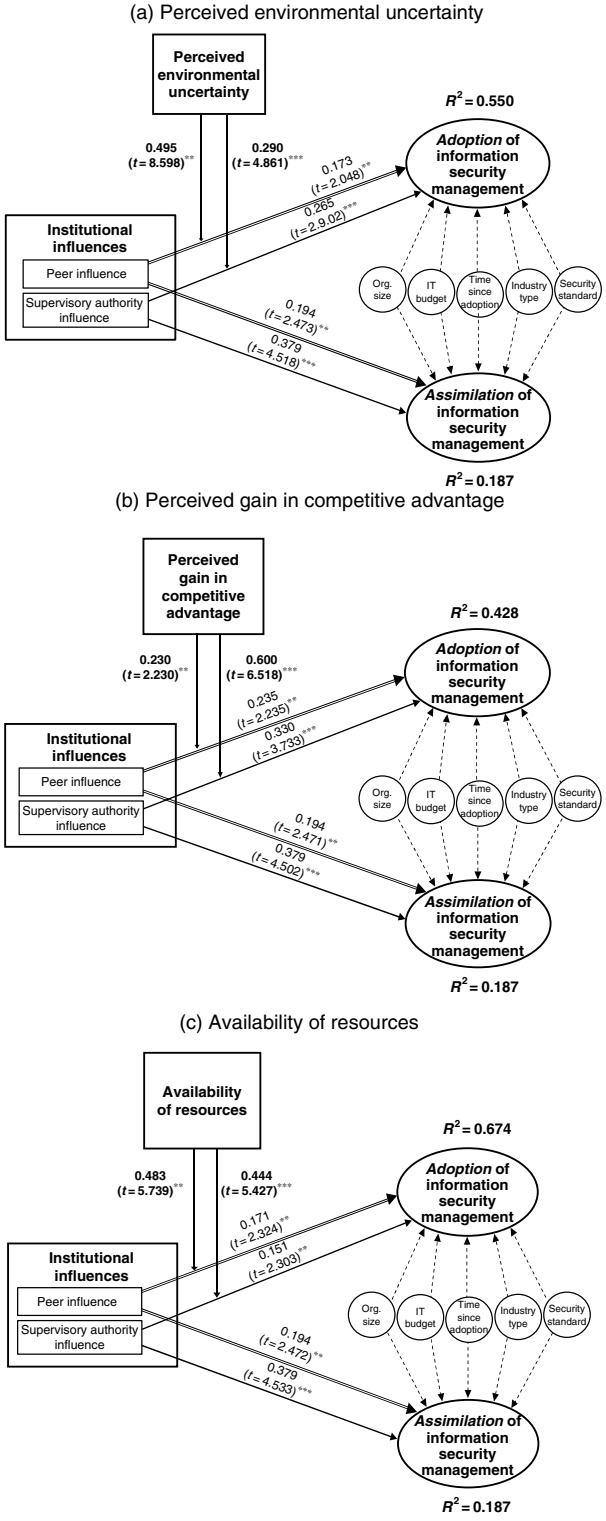
[11] Interaction effect size $f^2 = [R^2$ of interaction effect model $- R^2$ of main effect model$]/[1 - R^2$ of main effect model$]$.

Figure 4 The Direct Effects of Three Economic Factors



*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

Figure 5 The Moderating Effects of Three Economic Factors



*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

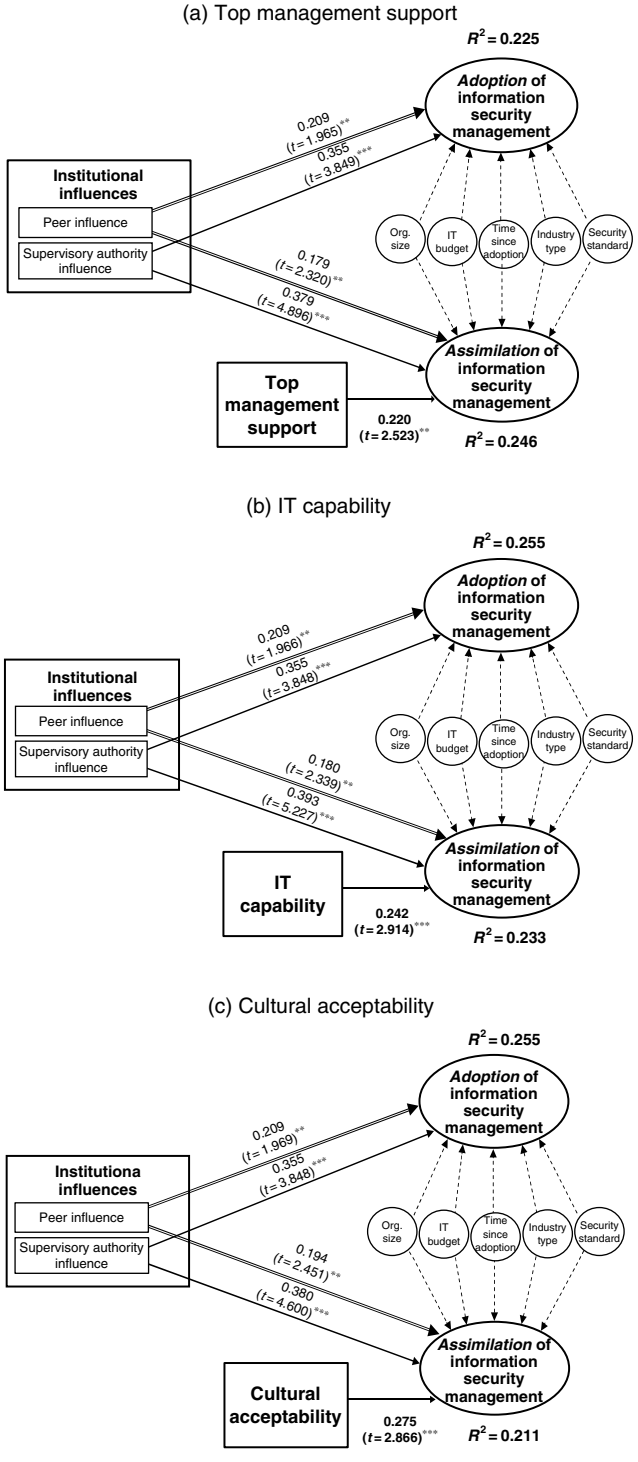
of 0.198 (=[0.550−0.439]/[1−0.439]) for perceived environment uncertainty, 0.177 (=[0.428−0.305]/[1−0.305]) for perceived gain in competitive advantage, and 0.242 (=[0.674 − 0.570]/R[1 − 0.570]) for availability of resources. The results show that all economic factors have medium interaction effects (Chin et al. 2003). In other words, the models in which the three economic factors are proposed to moderate the links between peer influence and the adoption process and between supervisory authority influence and the adoption process have significantly higher explanatory powers than the baseline model.

6.2.2. Explaining the Assimilation of Information Security Management. As in Figure 2, both peer influence ($\beta = 0.155$; $t = 2.005$; $p < 0.05$) and supervisory authority influence ($\beta = 0.398$; $t = 5.573$; $p < 0.01$) showed significant effects on the assimilation process. In addition, all three organizational capability factors were found to be significant moderators on the relationships between peer influence and the assimilation process ($\beta = 0.186$, $t = 2.450$, $p < 0.05$ for top management support; $\beta = 0.190$, $t = 2.763$, $p < 0.01$ for IT capability; and $\beta = 0.292$, $t = 3.606$, $p < 0.01$ for cultural acceptability) and between supervisory authority influence and the assimilation process ($\beta = 0.367$, $t = 5.869$, $p < 0.01$ for top management support; $\beta = 0.239$, $t = 3.455$, $p < 0.01$ for IT capability; and $\beta = 0.365$, $t = 4.642$, $p < 0.01$ for cultural acceptability). The results indicate that H4(a), H4(b), H(a), H5(b), H6(a), and H6(b) are fully supported.

To explore the interaction effects of the three organizational capability factors, we followed the same procedure used to test three economic moderators above, i.e., a hierarchical process (Chin et al. 2003). The baseline model without incorporating three organizational capability factors, and the direct effect and the moderating effect of the capability factors on the assimilation process were tested and their results were summarized in Figures 3, 6, and 7. The baseline model accounts for 18.7% of the variance in the assimilation of information security management. *R*-square values for the direct effects of the three capability factors on the assimilation process, as depicted in Figures 6(a), 6(b), and 6(c), were 0.246, 0.233, and 0.211, respectively, while *R*-square values generated from their individual moderating effects on the assimilation process were 0.406, 0.387, and 0.402, as in Figures 7(a), 7(b), and 7(c).

The hierarchical difference tests showed that the effect sizes f^2 of three organizational capability factors were 0.212 (=[0.406−0.246]/[1−0.246]) for top management support, 0.201 (=[0.387−0.233]/[1−0.233]) for IT capability, and 0.242 (=[0.402−0.211]/[1−0.211]) for cultural acceptability. Thus, indicates that all organizational capability factors also have medium interaction effects on the relationships between peer influence and the assimilation process as well as between supervisory authority influence and the assimilation process (Chin et al. 2003). The models incorporating the three organizational capability factors have more significant explanatory powers than the baseline model, as expected.

Figure 6 The Direct Effects of Three Organizational Capability Factors

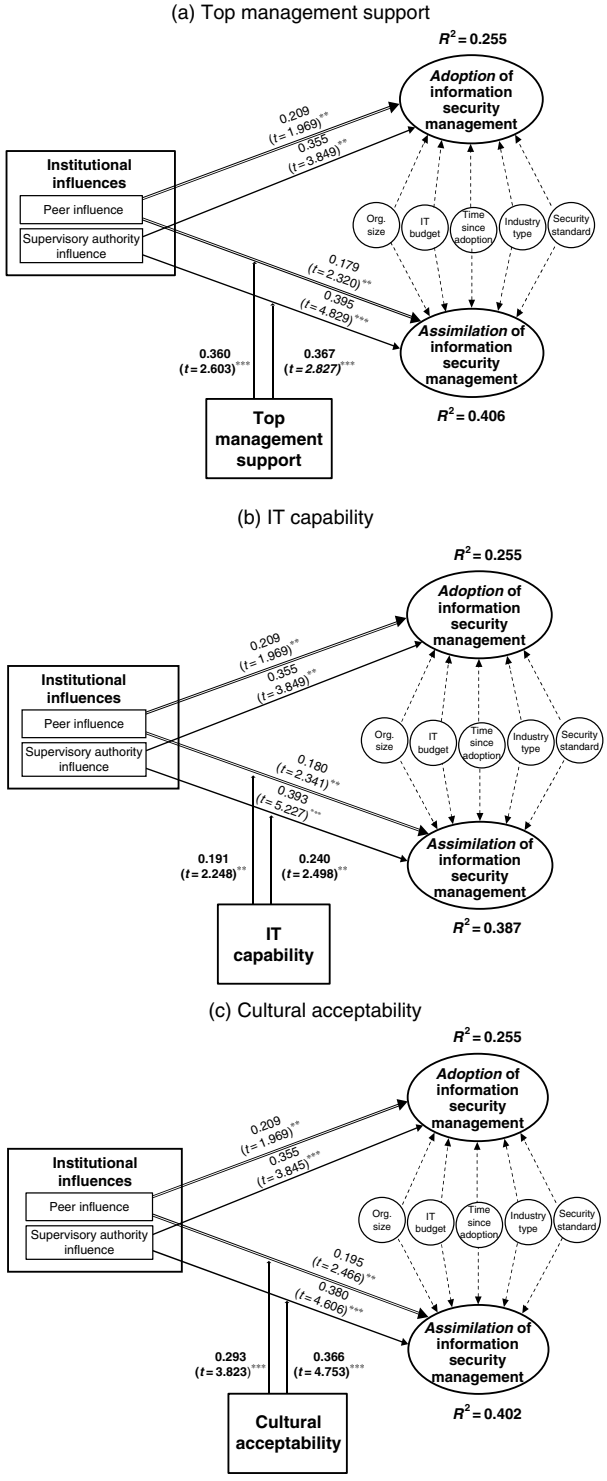


*$p < 0.10$; **$p < 0.05$; ***$p < 0.01$.

7. Discussion and Implications

In response to the recent emphasis on technology vulnerabilities in the organizational field, this study identifies information security management as an administrative innovation that decision makers can adopt to manage security risks. Our findings provide strong support that different management interpretations influence the choices about which best practices to adopt for information security management. Furthermore, from an institutional point of view, the study shows that institutional rules and

Figure 7 The Moderating Effects of Three Organizational Capability Factors



$^*p < 0.10$; $^{**}p < 0.05$; $^{***}p < 0.01$.

norms exert sizeable pressures on firms to adopt and assimilate information security management innovations. Using a two-stage survey technique, we also demonstrate how economic factors and internal organizational capabilities greatly affect the relationship between institutional influences and the adoption/assimilation process. Table 1 summarizes the results of our hypothesis testing. Our findings are consistent with prior studies. From an economic perspective, all three factors had medium moderating effects on both peer influence and supervisory authority influence in the adoption stage. These findings are consistent with those of prior studies. The unpredictability of the business environment motivates organizations to adopt appropriate management tools to mitigate decision-making risks (e.g., Baskerville 1991). Moreover, available organizational resources

Table 1 Summary of Findings

	Hypothesis	Result
H1(a) & 1(b)	The greater the level of environmental uncertainty perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures—(a) peer influence and (b) supervisory authority influence—to adopt information security management innovations.	H1(a): Supported H1(b): Supported
H2(a) & 2(b)	The greater the gain in competitive advantage perceived by an organization, the greater the likelihood that the organization will conform to institutional pressures—(a) peer influence and (b) supervisory authority influence—to adopt information security management innovations.	H2(a): Supported H2(b): Supported
H3(a) & 3(b)	The greater the availability of organizational resources, the greater the likelihood that the organization will conform to institutional pressures—(a) peer influence and (b) supervisory authority influence—to adopt information security management innovations.	H3(a): Supported H3(b): Supported
H4(a) & 4(b)	The greater the top management support, the stronger the relationship between institutional influences—(a) peer influence and (b) supervisory authority influence—and information security management assimilation.	H4(a): Supported H4(b): Supported
H5(a) & 5(b)	The greater an organization's IT capability, the stronger the relationship between institutional influences—(a) peer influence and (b) supervisory authority influence—and information security management assimilation.	H5(a): Supported H5(b): Supported
H6(a) & 6(b)	The higher the cultural acceptability of innovation, the stronger the relationship between institutional influences—(a) peer influence and (b) supervisory authority influence—and information security management assimilation.	H6(a): Supported H6(b): Supported

(e.g., Straub et al. 2008) and perceived gain in competitive advantage (e.g., Kankanhalli et al. 2003) allow firms to be more active in investing in and adopting information security management innovations, even when the potential return is unclear.

With regard to the three organizational capability factors, it was also found that all three factors had medium moderating effects on the base relations between peer influence/supervisory authority influence and the assimilation of information security management. This implies that our empirical outcomes agree with the previous studies that when there is strong top management support (e.g., Ba et al. 2001), high IT capability (e.g., Chiang et al. 2008), and a supportive culture (e.g., Gallivan 2001), organizations are more likely to absorb and disseminate information security management innovations.

In the continuing vein of comparisons to prior studies, our findings compare favorably with those reported by Hu et al. (2007) and Hsu (2009) with respect to institutional pressure. Our results show that peer influence and supervisory authority influence have significant effects on the adoption and assimilation of information security management innovation. Whereas our empirical outcomes do agree with both of these prior studies on the coercive influence on the information security management adoption, they also explain the contradictory findings about the role of mimetic force described in Hu et al. (2007) and Hsu (2009). The former found that the impact of mimetic force was "ambiguous" (p. 166), while the latter revealed the persistence of competitive mimicry on the information security certification implementation process. Our findings further reinforce our qualitative results in that in Korea, organizations are facing the pressure to implement security management practices in light of regulatory enactment on personal data protection and corporate governance. Although no other survey results allow us to make a full comparative analysis, we believe that the close relationship between Korea conglomerates and government is likely to show stronger coercive forces than in North American or European contexts. Regarding the role of the mimetic force, the characteristics of organizations in our empirical setting and Hsu (2009) may help explain why mimetic pressure has a significant impact on adoption and assimilation. The unique context of the Chaebol in Korea and the Finance House in the Taiwanese financial industry may indicate why leading institutions in these countries have a strong influence on interorganizational strategic decisions regarding innovation adoption.

One of the interesting findings is that perceived gain in competitive advantage shows the moderating effect on the relations between institutional influences and the adoption of information security management, which is consistent with the arguments of Kankanhalli et al. (2003) and Wood (1991). We see this result as an important contribution to information security management. Our study reconfirms the argument that broadly institutional mimicry is more likely to take place for competitive reasons (DiMaggio and Powell 1991, Guler et al. 2002). In addition, our findings indicate that when the market is competitive, firms are more actively in imitating the security management practices adopted by the peer firm rather than simply complying with the regulation. This is consistent with prior studies on the development of electronic commerce in Korea that argue that having an appropriate information security management in place is important to generate consumer trust and increase purchasing behavior online (e.g., Cheong and Park 2005, Jung et al. 2001). Furthermore, in recent years, the technological progress of mobile technology in Korea has created and fostered the growth of mobile banking and other financial services (Park and Yang 2008). This further highlights the importance of transaction security in gaining and sustaining market leadership.

Another interesting finding is the role of IT in assimilating information security management into the organization. Our empirical data shows that IT capability does act as a significant moderator in the assimilation stage. Although we implicitly believe that information technologies act as tools to support organizational learning (Gill 1995) and facilitate innovation activities in organizations (Junarkar 1997), no previous study empirically examines IT impacts on the adoption and assimilation of information security management. Although the information security maturity model has appeared in prior literature, its relationship to capabilities has only recently been appreciated (Chiang et al. 2008). We also see this relationship being addressed by the 2009 annual report of the Woori Financial Group, one of the leading financial groups in Korea, where it states that it standardized on both ISO 270001 for information security and CMMI Level 3 for software development as part of the group's overarching IT strategy. In this sense, this study serves as an initial attempt to validate the role of IT capability to information security management adoption and assimilation, and is thereby an important contribution.

Additionally, irrespective of the overwhelming support of our hypotheses, the explained variances in our models were compelling and a major contribution to this stream of research, in our opinion. The overall model had an explained variance of 75% for the security adoption dependent variable; security assimilation was somewhat lower at 52%, but still appreciable. What is equally striking is that the moderating effects reached the medium effect level (Cohen

1988), and that without the six across-the-board significant moderations, the baseline models would be much less impressive with explained variances of 25.5% and 18.7% respectively for adoption and assimilation. The bottom line seems to be that our research model is persuasive, to say the least.

The longitudinal research design and deliberative sampling plan in the study allowed us to collect adoption data at the point at which firms were making these kinds of decisions. The three-month lag in the collection of assimilation data was likewise an attempt to match the timing of the data collection to the phenomenon we were interested in, which in this case was assimilation. Whereas the lag period we chose may be debatable, a point raised again later under limitations, the longitudinal design was helpful in avoiding cross-sectional data that was a good fit for either the firm adoption decisions or assimilation processes but not both. Because this kind of longitudinal research design is unusual in diffusion studies, we trust that the strength of our findings will recommend this approach to other researchers and serve as a methodological contribution of the study.

7.1. Implications for Research

This study has several implications of theoretical and practical importance, which sees the emergence of some new areas for further research. Table 2 details the main implications and contributions of this research.

7.1.1. Organizational Theory on Administrative Innovation. First, findings lend support to other studies that see the merits of an integrative framework in organizational studies (Ang and Cummings 1997, Oliver 1991, Perrow 1985). Like these other works, the present study provides evidence that organizational survival requires firms to account for institutional expectations as well as environmental uncertainty, resource availability, and expected competitive performance. However, the unique contribution of this research is the application of this argument to the context of administrative innovation diffusion and infusion. From the viewpoint of innovation diffusion studies, our empirical investigation represents a further step in the direction of the need to study administrative innovation as a "continuous rather than discrete occurrence" (Westphal et al. 1997, p. 368). Testing our integrative model, we present evidence that institutional effects operate both at the adoption and assimilation stages during the diffusion process.[12] Our work further reveals that the decision of adoption was mediated through the economic factors whereas the success of administrative innovation depends on the degree of cultural acceptability, IT capability, and top management support. Furthermore, in their review of the application of institutional theory across different discipline, Weerakkody et al. (2009, p. 1) conclude that the use of such theory in the IS field "remains in its infancy, with much potential for adoption." Our present study has hopefully made a timely contribution to IS research by highlighting the complex relationship between institutional pressures and the diffusion of information security management practices.

7.1.2. Organizational Perspective of Information Security Research. This study addresses the limitations of current information security research due to the dominance of the technology-centric approach (Siponen and Willison 2007, Straub et al. 2008). We see our contributions from both theoretical and empirical perspectives. Furthermore, among the limited empirical investigation of the social-organizational perspective to information security management, most are concerned with either security effectiveness/misuse (e.g., Kankanhalli et al. 2003, D'Archy et al. 2009) or risk management (e.g., Straub and Welke 1998, Ransobtham and Mitra 2009). From the perspective of administrative innovation, we develop and empirically test an integrative and explanatory framework of information security diffusion processes. In particular, we highlight the importance of external environment on the adoption and assimilation of IS security management practice. In our qualitative interviews, we found that the contextual setting was the United States. In our empirical study, Korean organizations are mostly parts of large conglomerates as compared to the diversity of enterprises in the United States. Further research should be carried out in different countries (e.g., countries with the dominance of small-to-medium enterprises or countries with less of an authoritarian government–industry relationship) and examine the relative strength of each institutional isomorphism in such different environment settings. Additional studies are likely needed to deepen our understanding of the relationship between institutional constraints and information security management diffusion.

Furthermore, our analysis on moderating variables to these institutional forces suggests that technologies alone may not be sufficient to ensure the successful assimilation of a particular innovation, especially an administrative innovation such as information security management. Thus, a possible explanation is that only by combining top management and cultural capability can information technologies fully take effect. In this case, the contribution is that sound

[12] It is possible that institutional forces indirectly impact on assimilation through the adoption of information security management. Thus, we did an additional analysis on an alternative model that decouples the relationship between institutional forces and assimilation and the links between adoption and assimilation. The results summarized in Appendix G in the online supplement show that our arguments have higher explanatory power than the alternative model.

Table 2 Summary of Implications and Contributions

Literature on security management	Our findings	Theoretical and practical contributions
Emphasis on computer security as a technological innovation but not an administrative innovation	Theoretically developed and empirically tested the emergence of IS security management as an administrative innovation.	—Adds both theoretical development and empirical content to the "limited but emerging" (Ransbotham and Mitra 2009, p. 122) IS security management literature. —Offers a practical overarching framework on managerial decisions in making security risks.
Environment characteristics affecting IS security management diffusion	Offered proof that the institutional rules and norms exert sizable pressures on firms to adopt and assimilate IS security management innovations.	—Brings scholarly attentions to the value of institutional theory in IS security research. —The practical validation of coercive force reinforces the value of regulation in IS security management adoption and assimilation. —Our interviews highlight that normative pressure is still less relevant in influencing managerial actions. This calls for more professional development activities in the IS security management community.
Adoption and assimilation of IS security management innovations	Showed that economics-based factors demonstrated a moderating effect of institutional conformity in the adoption stage while the organizational capability factors were important moderators in the assimilation stage.	—Practical contribution in highlighting the balance between the economic and institutional environment in adopting security management. It tells managers to institutionalize factors that can influence the timely adoption of information security management. —Practical contribution in offering metrics that assess the efficacy of IS security management assimilation.
Value of mixed methods approaches	Used both qualitative and quantitative research methods in theorizing and validating our conceptual framework.	—Theoretical contribution in demonstrating the value of utilizing both qualitative and quantitative approaches in articulating and empirically demonstrating new IS security management theories.
External validity extended by setting the study in the Korean context	The theoretical model we propose explains well in the robust environment of Korea; in spite of strong factors favoring security awareness, the model was successful in predicting adoption of new security practices.	—External validity is essentially a contribution to the theory in that it extends the applicability or generalizabilty of the theory to new persons, settings, or times (Cook and Campbell 1979).

security management cannot rely on technical solutions alone (Dhillon and Backhouse 2001, Whitman 2004). In this research, we have attempted to validate three critical factors for successful information security management assimilation, and the opportunity exists for further research on other measurements, such as organizational structure, top management characteristics, and board structure, ways of which might help scholars and managers better evaluate various organizational aspects of their internal information security environments. In addition, our study also foreshadows possible theoretical extensions. For instance, what business performance and information security breaches occur when there are strong institutional forces in place? What managerial actions increase the role of IT capability and culture capability to strengthen the assimilation process?

7.1.3. Mixed Research Methods Approach. As Siponen and Willison (2007) point out, there is a predominance of descriptive and conceptual papers in information security management research. In their assessment, 79% of information security-related studies were "subjective argumentative" (p. 1556), and the rest adopted other methods such as field experiments. In this sense, our study advances information security management research by adding empirical findings to the conceptual-centric and descriptive literature. Furthermore, it demonstrates how different research methods can complement each other in intellectual and theoretical development. Given the lack of theories in information security research, the use of a qualitative approach can identify major security problems and allow scholars to find applicable theories that explain the phenomena. By doing so, it strengthens the capability and validation of developing more theoretically sound models that can be further tested empirically. In this sense, the research is significant because it strengthens a theoretical view of the social and organizational dimensions of information security, a domain that is still evolving according to Dhillon and Backhouse (2001), as well as responding to the critique that "a more coherent socio-organizational framework is required to explain why managers and users behave in certain ways" (Hu et al. 2007, p. 155).

7.2. Implications for Practice

The results of this study provide evidence that the development of regulation in different countries does have an impact on the adoption and assimilation of information security management. The findings indicate that at the outset of information security

management innovation, supervisory authority can play a significant role in stimulating and enforcing the adoption and assimilation of this new management practice. This can offer some encouraging evidence for regulators to evaluate the effectiveness of rules and regulations on corporate governance. Put differently, the results here can also serve as a positive indicator for other countries where information security management is still in its infancy. Findings also indicate that establishment of regulations or guidelines on data protection and governance and increased awareness of regulations are mechanisms that encourage better security and educate organizations about its benefits. Alternatively, given the positive results of mimetic force in our study, there is the practical implication that the regulatory authority can work with leading institutions in initiating information security management. This will be particularly effective where the marketplace is hypercompetitive and there is high uncertainty.

Furthermore, our results demonstrate that whereas external influences are key to good organizational decisions about adoption and assimilation of information security management practices, adoption was moderated by the economic evaluation of the business environment and assimilation was moderated by internal organizational capabilities. Therefore, firms can more effectively diffuse information security practices when they give voice to and make sound business cases for the economic value of security.

Similar to the suggestions put forward by Ang and Cummings (1997), we argue that managers need to carefully factor in key decision-making moderating variables. These variables accommodate institutional expectations, such as supervisory pressure and peer influence. By proactively evaluating economic conditions, managers can make timely strategic responses to institutional pressure to conform when adopting information security innovations. Being more aware of environmental uncertainty, competitive pressures, and the availability of resources, for instance, gives managers insight into how to successfully adopt an information security management framework. As a result, with timely adoption, firms are more likely to avoid risks and the consequent costs associated with information security breaches.

In the assimilation stage, our study shows that top management support, IT capabilities, and cultural acceptability play crucial roles in ensuring that information security management practices become embedded in organizational practices. A sound and effective information security management requires the support of top management and organizational culture. To demonstrate top management support, we consider that the establishment of a CISO role can serve as a strong signal in the commitment of senior management to security. Furthermore, our work reiterates the importance of culture in assimilating information security management in organizations. In an industry survey (Richardson 2008), 42% of organizations responded that their organization spent less than 1% of their security dollars on awareness programs. This calls for managerial attention to creating a security culture (e.g., budget allocation on training or hour requirements on information-security related education), which in turn will better communicate information security procedures and policies to employees.

7.3. Limitations and Future Research

We now turn to the limitations of this study, some of which offer opportunities for future research. First, because of the nature of longitudinal studies (lack of control groups), this work could suffer from internal validity threats such as maturation, history, and mortality (Huck et al. 1974). According to previous literature (Venkatesh and Davis 2000), the three-month duration of our study may not be long enough to minimize these threats, even though we determined it by considering Korea's *palli palli* business culture. Second, the majority of respondents in this study were CIOs. Although the information from top IS managers should provide a high level of confidence in the quality of the information gathered, a single respondent selection bias could still exist. Third, the results of this study may include regional biases due to the data collection taking place solely in Korea. Thus, the results may have to be carefully interpreted and replicated in other industries and countries to improve the generalizability of the findings.

The results of this study suggest several directions for future research. The diffusion of information security management ought to receive more attention from IS researchers. This research provides a starting point for such future studies. Our six proposed moderators are open to refinement and further verification. It is also possible that other conditions may have moderating effects on the relationship between institutional pressures and the adoption and assimilation of information security innovations. Therefore, further theoretical development and organizational practice would stimulate the exploration of new moderating variables.

Furthermore, our work has shown the value of institutional theory in understanding the diffusion of IS security management in organizations. One suggestion for further research is to examine the influence external pressures might have on employee behavior and attitudes towards information security management. In this respect, a deeper revelation on the interaction between institutional pressures and organizational change would be fruitful in enhancing the effectiveness of information security management.

8. Conclusion

Because of the attention given to vulnerability protection and institutional expectations of compliance, information security management has emerged as an administrative innovation in the IS field. Drawing from neo-institutional theory and the innovation diffusion literature, this study proposes an integrative framework of the adoption and assimilation of information security management. Furthermore, the field study findings offer empirical support for the moderating effects of economic and organizational capability in the presence of coercive and mimetic isomorphism. From a theoretical perspective, it provides a good starting point for theoretical refinements on the institutionalization of information security management. It also provides an analytical tool that can be used for managerial intervention in the diffusion of information security management in organizations.

Electronic Companion

An electronic companion to this paper is available as part of the online version at http://dx.doi.org/10.1287/isre.1110.0393.

Acknowledgments

The first author is thankful for a research award by the E. SUN Bank in Taiwan for the conduct of this work. The second author is supported by a 2012 Korea University Grant.

References

Ajzen, I., M. Fishbein. 1980. *Understanding Attitudes and Predicting Behavior.* Prentice Hall, Englewood Cliffs, NJ.

Ang, S., L. Cummings. 1997. Strategic response to institutional influences on information systems outsourcing. *Organ. Sci.* **8**(3) 235–256.

Ba, S., J. Stallaert, A. B. Whinston. 2001. Research commentary: Introducing a third dimension in the information systems design—The case for incentive alignment. *Inform. Systems Res.* **12**(3) 225–239.

Backhouse, J., C. Hsu, L. Silva. 2006. Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quart.* **30**(Special issue) 413–438.

Bae, J. 1997. Beyond seniority-based systems: A paradigm shift in Korean HRM? *Asia Pacific Bus. Rev.* **3**(4) 82–110.

Bae, J., J. J. Lawler. 2000. Organizational and HRM strategies in Korea: Impact on firm performance in an emerging economy. *Acad. Management J.* **43**(3) 502–517.

Bantel, K., S. Jackson. 1989. Top management and innovations in banking: Does the composition of the top team make a difference? *Strategic Management J.* **10**(1) 107–124.

Baskerville, R. 1991. Risk analysis: An interpretive feasibility tool in justifying information systems security. *Eur. J. Inform. Systems* **1**(2) 121–130.

Baskerville, R., G, Dhillon. 2008. Information systems security strategy: A process view. D. Straub, S. Goodman, R. Baskerville, eds. *Information Security Policies, Processes and Practices*. M. E. Sharpe, Armonk, NY, 15–45.

Bharadwaj, A. S. 2000. A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quart.* **24**(1) 169–196.

Blasi, A. D., F. V. Puig. 2002. Conditions for successful automation in industrial applications: A point of view. *IFAC 15th Triennial World Congress Proc.*, http://www.nt.ntnu.no/users/skoge/prost/proceedings/ifac2002/data/content/05002/5002.pdf.

Butler, T. 2003. An institutional perspective on developing and implementing Intranet- and Internet-based information systems. *Inform. Systems J.* **13**(3) 209–231.

Chang, S., C. Ho. 2006. Organizational factors to the effectiveness of implementing security management. *Indust. Management Data Systems* **106**(3) 345–361.

Chatterjee, D., R. Grewal, V. Sambamurthy. 2002. Shaping up for e-commerce: Institutional enablers of the organizational assimilation web technologies. *MIS Quart.* **26**(2) 65–89.

Cheong, J. H., M. C. Park. 2005. Mobile Internet acceptance in Korea. *Internet Res.* **15**(2) 125–140.

Chiang, T. J., R. I. Chang, J. S. Kouh, K. P. Hsu. 2008. An information security education maturity model. Working paper, National Taiwan University, Taipei, Taiwan. http://cnte2008.cs.nhcue.edu.tw/pdf/135.pdf.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. A model for evaluating IT security investments. *Comm. ACM* **47**(7) 87–92.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The value of intrusion detection systems in information technology security architecture. *Inform. Systems Res.* **16**(1) 28–56.

Chin, W. W. 1998. The partial least squares approach to structural equation modeling. G. A. Marcoulides, ed. *Modern Methods for Business Research*. Lawrence Erlbaum Associates, Mahwah, NJ, 295–336.

Chin, W. W., B. L. Marcolin, P. R. Newsted. 2003. A partial least squares latent variable approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inform. Systems Res.* **14**(2) 189–217.

Chou, D. C., D. C. Yen, B. Lin, P. H. Cheng. 1999. Cyber security management. *Indust. Management Data Systems* **99**(8) 353–361.

Choung, J. Y. 1998. Patterns of innovation in Korea and Taiwan. *IEEE Trans. Engrg. Management* **45**(4) 357–365.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. Lawrence Erlbaum Associates, Hillsdale, NJ.

Cook, T. D., D. T. Campbell. 1979. *Quasi-Experimentation: Design and Analysis Issues for Field Settings.* Houghton Mifflin, Chicago.

Cooper, R. B., R. W. Zmud. 1990. Information technology implementation research: A technological diffusion approach. *Management Sci.* **36**(2) 123–139.

Damanpour, F. 1991. Organizational innovation: A meta-analysis of effects of determinants and moderators. *Acad. Management J.* **34**(3) 555–590.

D'Archy, J., A. Hovav, D. Galletta. 2009. User awareness of security countermeasures and its impact on information security misuse: A deterrence approach. *Inform. Systems Res.* **20**(1) 79–98.

Dhillon, G., J. Backhouse. 2001. Current directions in IS security research: Towards socio-organizational perspectives. *Inform. Systems J.* **11**(2) 127–153.

Dillman, D. A. 1991. The design and administration of mail surveys. *Annual Rev. Sociol.* **17** 225–249.

DiMaggio, P. J., W. W. Powell. 1991. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. P. J. DiMaggio, W. W. Powell, eds. *The New Institutionalism in Organizational Analysis*. University of Chicago Press, Chicago, 63–82.

Duncan, R. B. 1972. Characteristics of organizational environments and perceived environmental uncertainty. *Admin. Sci. Quart.* **17**(3) 313–327.

Fichman, R. G., C. F. Kemerer. 1997. The assimilation of software process innovation: An organizational learning perspective. *Management Sci.* **43**(10) 1345–1363.

Fichman, R. G., C. F. Kemerer. 1999. The illusory diffusion of innovation: An examination of assimilation gaps. *Inform. Systems Res.* **10**(3) 255–275.

Fornell, C., F. L. Bookstein. 1982. Two structural equation models: LISREL and PLS applied to customer exit-voice theory. *J. Marketing Res.* **19**(4) 440–452.

Gallivan, M. J. 2001. Organizational adoption and assimilation of complex technological innovation: Development and application of a new framework. *DATA BASE Adv. Inform. Systems* **32**(3) 51–85.

Gill, T. G. 1995. High-tech hidebound: Case studies of information technologies that inhibited organizational learning. *Accounting, Management Inform. Tech.* **5**(1) 41–60.

Goodhue, D. L., D. Straub. 1991. Security concerns of system users: A study of perceptions of the adequacy of security measures. *Inform. Management* **20**(1) 13–27.

Gordon, L., M. Loeb. 2001. Using information security as a response to competitor analysis systems. *Comm. ACM* **44**(9) 70–75.

Gordon, L., M. Loeb. 2002. The economics of information security investment. *ACM Trans. Inform. System Security* **5**(4) 438–457.

Gosain, S. 2004. Enterprise information systems as objects and carriers of institutional forces: The new iron cage? *J. Assoc. Inform. Systems* **5**(4) 151–182.

Guler, I., M. Guillen, J. Macpherson. 2002. Global competition institutions, and the diffusion of organizational practices: The international spread of ISO 9000 quality certificates. *Admin. Sci. Quart.* **47**(2) 207–223.

Hair, J. F., R. E. Anderson, R. L. Tatham, W. C. Black. 1995. *Multivariate Data Analysis with Readings*, 4th ed. Prentice Hall, Englewood Cliffs, NJ.

Haunschild, P., A. Minner. 1997. Modes of interorganizational imitation: The effects of outcome salience and uncertainty. *Admin. Sci. Quart.* **42**(3) 472–500.

Hirt, S. G., E. B. Swanson. 2001. Emergent maintenance of ERP: New roles and relationships. *J. Software Maintenance: Res. Practice* **13**(6) 373–397.

Hofstede, G. 1980. *Culture's Consequence: International Differences in Work Related Values*. Sage Publications, London.

Hsu, C. 2009. Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *Eur. J. Inform. Systems* **18**(2) 140–150.

Hu, Q., P. Hart, D. Cooke. 2006. The role of external influences on organizational information security practices: An institutional perspective. *39th Hawaii Internat. Conf. System Sci.*, IEEE Computer Society Press, Los Alamitos, CA, 1–10.

Hu, Q., P. Hart, D. Cooke. 2007. The role of external influences on organizational information security practices: An institutional perspective *J. Strategic Inform. Systems.* **16**(2) 153–172.

Huck, S. W., W. H. Cormier, W. G. Bounds. 1974. *Reading Statistics and Research*. Harper-Collins, New York.

Iacono, C., I. Benbasat, A. Dexter. 1995. Electronic data interchange and small organizations: Adoption and impact of technology. *MIS Quart.* **19**(4) 465–485.

Junarkar, B. 1997. Leveraging collective intellect by building organizational capabilities. *Expert Systems Appl.* **13**(1) 29–40.

Jung, B., I. Han, S. Lee. 2001. Security threats to Internet: A Korean multi-industry investigation. *Inform. Management* **38**(8) 487–498.

Kaluzny, A., C. McLaughlin, B. Jaeger. 1993. TQM and a managerial innovation: Research issues and implications. *Health Services Management Rev.* **6**(2) 78–88.

Kankanhalli, A., H. H. Teo, K. K. Wei. 2003. An integrative study of information systems security effectiveness. *Internat. J. Inform. Management* **23**(2) 139–154.

Kotulic, A. G. 2004. Why there are not more information security research studies. *Inform. Management* **41**(5) 597–607.

Lau, T. Y., S. W. Kim, D. Atkin. 2005. An examination of factors contributing to South Korea's global leadership in broadband adoption. *Telematics Informatics* **22**(4) 349–359.

Liang, H., N. Saraf, Q. Hu, Y. Xue. 2007. Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quart.* **31**(1) 59–87.

Mignerat, M., S. Rivard. 2009. Positioning the institutional perspective in information systems research. *J. Inform. Tech.* **24**(4) 369–391.

Miles, M. B., A. M. Huberman. 1994. *Qualitative Data Analysis*. Sage Publications, Thousand Oaks, CA.

Milliken, F. J. 1987. Three types of perceived uncertainty about the environment: State, effect, and response uncertainty. *Acad. Management Rev.* **12**(1) 133–143.

Miranda, S. M., Y. M. Kim. 2006. Professional versus political contexts: Institutional mitigation and the transaction cost heuristic in information systems outsourcing. *MIS Quart.* **30**(3) 725–753.

Moore, G., I. Benbasat. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Inform. Systems. Res.* **2**(3) 192–222.

Oliver, C. 1991. Strategic response to institutional processes. *Acad. Management Rev.* **16**(1) 145–179.

Park, C., H.-D. Yang. 2008. Mobile business in Korea. Y. Yoo, J.-N. Lee, C. Rowley, eds. *Trends in Mobile Technology and Business in the Asia-Pacific Region*. Chandos Publishing, Oxford, UK, 109–126.

Perrow, C. 1985. Review essay: Overboard with myth and symbols. *Amer. J. Sociol.* **91**(1) 51–55.

Pfeffer, J. 1982. *Organization and Organizational Theory*. Pitman, Boston.

Pfeffer, J., G. Salancik. 1978. *The External Control of Organizations: A Resource Dependence Perspective*. Harper & Row, New York.

Ramachandran, S., S. Rao. 2006. Security cultures in organizations: A theoretical model. *Americas Conf. Inform. Systems, Acapulco, Mexico*.

Ransbotham, S., S. Mitra. 2009. Choice and chance: A conceptual model of paths to information security compromise. *Inform. Systems. Res.* **20**(1) 121–139.

Richardson, R. 2008. *CSI Computer Crime and Security Survey: U.S.* Computer Security Institute, New York.

Rosner, M. 1968. Economic determinants of organizational innovation. *Admin. Sci. Quart.* **12**(4) 614–625.

Ryan, M. J., E. H. Bonfield. 1975. The Fishbein extended model and consumer behavior. *J. Consumer Res.* **2**(2) 118–136.

Scott, W. R. 1995. *Institutions and Organizations.* Sage Publications, London.

Shin, H. 2009. Is it possible to force firms to have CISOs? CIO Biz (September 27), http://www.ciobiz.co.kr/news/articleView.html?idxno=1114. [In Korean.]

Siponen, M. 2005. An analysis of the traditional IS security approaches: Implications for research and practice. *Eur. J. Inform. Systems* **14**(3) 303–315.

Siponen, M., J. Iivari. 2006. Six design theories for IS security policies and guidelines. *J. Assoc. Inform. Systems* **7**(7) 445–472.

Siponen, M., R. Willison. 2007. A critical assessment of IS security research between 1990–2004. *Proc. 15th Eur. Conf. Inform. Systems, St. Gallen, Switzerland*, 1551–1559.

Sivo, S., C. Saunders, Q. Chang, J. Jiang. 2006. How low should you go? Low response rates and the validity of inference in IS survey research. *J. Assoc. Inform. Systems* **7**(6) 351–411.

Son, J. Y., I. Benbasat. 2007. Organizational buyers' adoption and use of B2B electronic marketplaces: Efficiency—And legitimacy-oriented perspectives. *J. Management Inform. Systems* **24**(1) 55–99.

Straub, D., R. J. Welke. 1998. Coping with systems risk: Security planning models for management decision-making. *MIS Quart.* **22**(4) 441–469.

Straub, D., S. Goodman, R. Baskerville. 2008. Framing of information security and practices. D. Straub, S. Goodman, R. Baskerville, eds. *Information Security Policies, Processes and Practices.* M. E. Sharpe, Armonk, NY, 5–12.

Teece, D. J. 1980. The diffusion of an administrative innovation. *Management Sci.* **26**(5) 464–470.

Teo, H. H., K. K. Wei, I. Benbasat. 2003. Predicting intention to adopt interorganizational linkage: An institutional perspective. *MIS Quart.* **27**(1) 19–49.

Terlaak, A., A. King. 2006. The effect of certification with the ISO 9000 quality management standard: A singaling approach. *J. Econom. Behav. Organ.* **60**(4) 579–602.

Tingling, P., M. Parent. 2002. Mimetic isomorphism and technology evaluation: Does limitation transcend judgment? *J. Assoc. Inform. Systems* **3**(5) 113–143.

Venkatesh, V., F. D. Davis. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Sci.* **46**(2) 186–205.

Venkatraman, N., L. Loh, J. Koh. 1994. The adoption of corporate governance mechanism: A test of competing diffusion models. *Management Sci.* **40**(4) 496–507.

Wang, P. 2008. Assimilation it innovation: The longitudinal effects of institutionalization and resource dependence. *Proc. Internat. Conf. Inform. Systems, Paris*.

Weerakkody, V., Y. Dwivedi, Z. Irani. 2009. The diffusion and use of institutional theory: A cross-disciplinary longitudinal literature survey. *J. Inform. Tech.***24**(4) 1–15.

Westphal, J., R. Gulati, S. Shortell. 1997. Customization or conformity? An institutional and network perspective on the content and consequences of TQM adoption. *Admin. Sci. Quart.* **42**(2) 366–394.

Whitman, M. E. 2004. In defences of the realm: Understanding the threats to information security. *Internat. J. Inform. Management* **24**(1) 43–47.

Wood, C. C. 1991. Using information security to achieve competitive advantage. *Comput. Security* **10**(5) 399–404.

Zaltman, G, R. Duncan, J. Holbek. 1973. *Innovations and Organizations.* John Wiley & Sons, New York.

Zhu, K., K. Kraemer, S. Xu. 2006. The process of innovation assimilation by firms in different countries: A technology diffusion perspective on e-business. *Management Sci.* **52**(10) 1557–1576.

Zingales, L., R. Glauber, R. Litan, A. Ferrell, A. Kuritzkes. 2006. Interim report of the committee on capital markets regulation. Report, Committee on Capital Markets Regulation, Washington, DC.

Zinn, J., R. Weech, D. Brannon. 1998. Resource dependence and institutional elements in nursing home TQM adoption. *HSR: Health Services Res.* **33**(2) 261–273.

Zmud, R. 1982. Diffusion of modern software practices: Influence of centralization and formalization. *Management Sci.* **28**(12) 1421–1431.