WHAT INCREASES FIRMS' PERFORMANCE OF INFORMATION SECURITY MANAGEMENT AND THE ROLE OF REGULATORY PRESSURE

Geuna Kim, School of Business Administration, Kyungpook National University, Korea, applenana@knu.ac.kr

Sanghyun Kim, School of Business Administration, Kyungpook National University, Korea, ksh@knu.ac.kr

Aaron M. French, School of Business Administration, Kyungpook National University, Korea, afrench@knu.ac.kr

Abstract

With the continued expansion of corporate information systems and the increasing use of networks, information security management (ISM) has become more important than ever. However, few empirical studies have examined the effects of firms' internal and external factors on their ISM processes. This study investigates the role of Need Pull and Technology Push on the ISM process, and examines the regulatory pressure within ISM process. To test the research model, the study considers data from a random sample of organizations obtained through the Korea Composite Stock Price Index (KOSPI), the Korean Securities Dealers Automated Quotation (KOSDAQ), and the Korea Foreign Company Association (FORCA). Results demonstrate that need-pull and technology-push had positive effects on the ISM process. In addition, regulatory pressure as a moderator had positive effects between ISM awareness - ISM development and ISM development - ISM performance.

Keywords: Information Security Management, Need-Pull/Technology-Push, Regulatory Pressure

1 INTRODUCTION

With the continued expansion of corporate information systems and the increasing use of networks, information security management (ISM) has become more important than ever (Yildirim, Akalp, Aytac, & Bayram, 2011). In particular, an organization's security failure may lead to a heavy monetary loss, irreparable damage to its reputation, and even bankruptcy (Lee & Larsen, 2009). Efforts to sufficiently manage information security and reinforce competitiveness have led to the construction and implementation of ISM systems. As a result, ISM has been recognized to play an important role in fostering desirable business environments (Gupta & Hammond, 2005; Chang & Ho, 2006).

However, few studies have examined ISM in organizational contexts, and therefore there is a need for further research on the effective measurement of performance, detailed evaluation criteria or construction, and the actual implementation of ISM. Here the difficulty lies in estimating the success of enterprise ISM through the introduction of fragmented security solutions or related policies and guidelines (Zhang, Reithel, & Li, 2009). This means that the use of an organization's security system may be limited to formal activities and that the success of security management and control cannot be determined.

In this regard, this study considers the following research questions in order to have better understanding on organizations behaviors related to ISM: What factors influence organizational members' recognition of ISM? What routes facilitate the specific implementation and outcome of ISM? What factors enhance the relationship between ISM variables? To address these questions, the current study investigates the effects of an organization's need-pull and technology-push on its ISM process in regards to ISM awareness, development, and performance. In addition, the study examines the moderating effect of regulatory pressure on the relationships between ISM variables.

2 LITERATURE REVIEW

The objective of ISM is to minimize damage to organizations by preventing and controlling security problems caused by unexpected intrusions and accidents (Kankanhalli, Teo, Tan, & Wei, 2003). Firms can enhance their security by managing their administrative, technological, and physical security to protect themselves from various threats (e.g., natural disasters, intentional and unintentional threats, and system failures) that may damage information systems and assets (Cavusoglu, Mishra, & Raghunathan, 2004). However, despite the development of costly technological solutions for security management, many physical and technological measures cannot sufficiently address various risk factors associated with information security. Although previous studies of security management have generally focused on technological methods, there is a need for new approaches (e.g., users' behavior) to security management because of the increased mobility of information (Baker & Wallace, 2007). In this regard, information management has become part of the organizational culture fostered not only by technological issues but also by social and economic motives.

Firms need to take preventative action for information security by analyzing and continuously monitoring various risk factors and thus increasing security awareness (Spears & Barki, 2010). Although security awareness is an important factor in ISM, it alone cannot serve as a viable preventative countermeasure. Hsu (2009) proposed an ISM model including ISM awareness, development, and performance as a new paradigm for information security. Thus, the present study examines the effects of regulatory pressure and various factors on ISM awareness and presents need-pull (NP) and technology-push (TP) as factors influencing ISM awareness. In addition, the study considers the factors influencing the ISM process.

2.1 Need-Pull/Technology-Push

Schon (1967) introduced Need-Pull (NP) and Technology-Push (TP) as two concepts of technological innovation to describe technology adoption. Researchers in various fields such as engineering, R&D, marketing, and information systems have investigated NP and TP (Chau & Tam, 2000). In addition, previous studies have indicated a need for harmony between NP and TP as a solution for the development of technological innovation processes within organizations (Munro & Noori, 1988). Push/pull theory provides a way to differentiate between the success and failure of organizations' core projects and plays a critical role in understanding and adjusting internal motives and external forces in the context of innovation (Mowery & Rosenberg, 1979).

NP refers to an organization's key drivers that increase the final user's demand as a basis for innovation (Lee & Shim, 2007). In NP, users' needs represent the key driver calling attention to the benefit of innovation diffusion within the organization. The present study considers NP because of users' need to call attention to the organization's need for innovation in the ISM process. Previous studies have proposed various factors representing NP. For example, Chau and Tam (2000) and Lee and Shim (2007) considered market uncertainty, performance gaps, task interdependence, and task predictability and claimed that these are positive determinants of organizations' or users' decision on new technologies or processes. Shih (2006) adopted the "push-pull" concept to explain the effects of technology adoption and classified various determinants such as task interdependence, task predictability, perceived information-sharing norms, perceived ease of use, and perceived usefulness into either push or pull elements with significant effects on users' behaviors.

TP relies on a scientific foundation and technical competence, which can facilitate the diffusion and application of new technologies (Chau & Tam, 2000). Based on the need to enhance performance, new technologies can be discovered and disseminated within the organization. The present study considers TP in the context of the discovery and diffusion of ISM technologies and examines its effects on ISM awareness. Previous studies (e.g., Chau & Tam, 2000; Lee & Shim, 2007) have claimed that perceived benefits, vendor pressure, learning from external information sources, and the level of cooperation are part of TP and play critical roles in explaining innovation-related decision processes at the organizational level.

However, most studies have been theoretical in nature. That is, few empirical studies have examined NP and TP simultaneously. Although many firms recognize the importance of ISM, they lack knowledge of internal requirements that can induce a need for security management or external pressure that can force them to manage security. Therefore, this study proposes some sub-concepts of NT and TP and empirically evaluates their effects on the ISM process.

2.2 Information Security Management

Information security refers to a series of behaviors for maintaining and managing an organization's information assets requiring protection. For various institutions, information security can be defined as a set of tools used to protect their information assets. Keller, Poweel, Horstmann, Predmore, and Crawford (2005) defined information security as the process, including awareness, development, and performance, of storing systematically analyzed and sorted information such that it can be applied to real-life problems based on materials collected through observations or measurements by the organization. In addition, Yeh and Chang (2007) claimed that information security can prevent inevitable security accidents, guarantee the continuity of business, and minimize damage. In this regard, previous studies (e.g., Wessel, Yang, & Vries, 2011) have defined information security as a series of security countermeasures for managing all information that needs to be protected and safely stored according to the organization's requirements.

With various definitions of information security, information security management (ISM) is the process of maintaining an appropriate level of security for information based on human factors and materials provided by a system following the general management cycle (Spears & Barki, 2010).

Security management includes all the processes used to evaluate information assets and related risks, identify appropriate countermeasures, and efficiently execute such countermeasures.

In business, organizational members' awareness is generally viewed as the extent to which they have knowledge of fundamental information and its relevance to problem areas within the organization. In the context of ISM, organizational members need to be aware of security objectives set by the organization. Organizations recognize security as an important issue, but many do not have a full understanding of what they should be doing or how it can be achieved (Furnell, Gennatou, & Dowland, 2002). If the organization is not aware of the security measures it should be implementing, then it is not able to educate its employees about how its intellectual property can be protected. An insufficient level of user awareness can make even the best security mechanisms inadequate.

Some empirical studies of security management have reported that information security management and decision making can vary according to various variables dormant in the organization (Ma & Ratnasingam, 2008). That is, the identification and minimization of threats to the security of organizational assets require continuous verification, evaluation, and empirical efforts. Such studies have proposed diagnostic tools that can help a firm's ISM by developing management models that extend the firm's information management responsibilities and duties and found that institutional pressure has positive effects on the adoption and assimilation of ISM. In addition, they have provided support for direct and moderating effects of three variables for ISM adoption—perceived environmental uncertainty, perceived gain in competitive advantage, and resource availability—as well as for those of top management support, IT capability, and cultural acceptability.

Previous studies of ISM and related factors have focused on frameworks and thus have been limited in terms of proposing advanced models and explaining structural relationships between various factors, particularly in ISM process. Although researchers have examined ISM, they have been unable to present stable solutions that can be effectively designed and practiced by firms. Therefore, for firms to benefit from their security management efforts, they must have appropriate insights into imminent problems and security management measurements within the scope that they can sufficiently accommodate. In this regard, this study contributes to the literature by empirically verifying those internal and external characteristics intrinsic to ISM process, including awareness, development, and performance.

2.3 Variables in the ISM Innovation Decision Process

Previous studies have proposed various innovation steps or stages. Grover and Goslar (1993) claimed that the process of implementing new technologies or systems in various organizational settings includes the following three steps: use intentions (or positive attitudes), actual use or development, and implementation. These processes can vary according to the type of technology being implemented; the organization to which they are applied; and the scope and content of research (Cooper & Zmud, 1990). For an organization, the innovation decision process is a process through which the organization shifts from its awareness of a new technology or strategic process to its development (i.e., adoption) and implementation of the innovation for everyday business operations (Kim & Garrison, 2010). Based on this line of reasoning, this study takes a three-step approach to the innovation decision process, including ISM awareness, development, and performance.

ISM awareness refers to the step in which organizations collect and evaluate information on the importance of ISM (Grover & Goslar, 1993). After identifying the internal and external factors influencing their intention to engage in IT security management, organizations become aware of the importance of ISM in terms of their strategic or operational efficiency and effectiveness through ISM. In this study, ISM awareness implies an organization's intention to adopt ISM after becoming aware of internal needs and external resources associated with ISM. ISM development is the second stage in the ISM process. Here organizations adopt and implement IT security management in a gradual manner, and ISM becomes more routine and less foreign to organizational members. Finally, ISM performance is the stage in which organizations integrate ISM for innovation and realize

financial/nonfinancial improvements such as reduced work errors, the protection of organizational assets, and increased profitability (Spears & Barki, 2010). In this stage, organizational members no longer regard ISM as unique because it is fully integrated into the organization's daily routine.

In this regard, Spears and Barki (2010) proposed user participation, organizational awareness, control development, and control performance as part of information security risk management and demonstrated organizational members' rational decision making in the context of security management. Therefore, the present study considers ISM awareness, development, and performance as the three stages of the ISM process and examines their relationships.

2.4 Regulatory Pressure

Firms must comply with continuously evolving national and industrial security regulations (Flanagin, 2000). Organizations tend to imitate others facing similar environments of uncertainty pertaining to goals and effectiveness to change their organizational structure to better reflect social value systems and rules (Khalifa & Davison, 2006). However, an organization can achieve social approval and legitimacy as a social subsystem because of the integration and implementation of relationships between organizations in conjunction with the decrease in the scope of individuals' behavior through institutionalized environments (Teo, Wei, & Benbasat, 2003).

In addition, an organization's innovation activity can be influenced by coercive pressure from government regulations, government policies, and competitive requirements within an industry or market. Therefore, the coercion of regulatory institutions under uncertain environments can help specify organizations' structure or strategic adoption. An organization's reliance on regulators is an important factor that can reinforce their authority within the industry and help the organization to avoid various internal and external security risks (Appari & Johnson, 2009).

Previous studies have demonstrated that regulatory pressure has positive effects on organizational members' ISM implementation (Gosain, 2004; Hu et al., 2007; Liang, Saraf, Hu, & Xue, 2007). Regulatory pressure can be official or unofficial pressure imposed by society and involve social, cultural, and political factors. This pressur manifests through external forces of persuasion, and an organization may witness changes in its environment through changes in government policies, social systems, or other organizations.

3 RESEARCH MODEL AND HYPOTHESES

Figure 1 shows the proposed research model. For this model, a survey reflecting various internal and external elements that may play important roles in ISM from the perspective of organizational members was administered by conducting interviews with managers and staff members and using a basic research model based on a literature review. Therefore, this study includes an organization's NP and TP as the key factors influencing the organization's ISM awareness, development, and performance. In addition to the interviews, previous research was reviewed to develop the research model. In this regard, the present study contributes to the ISM literature by taking this new approach.

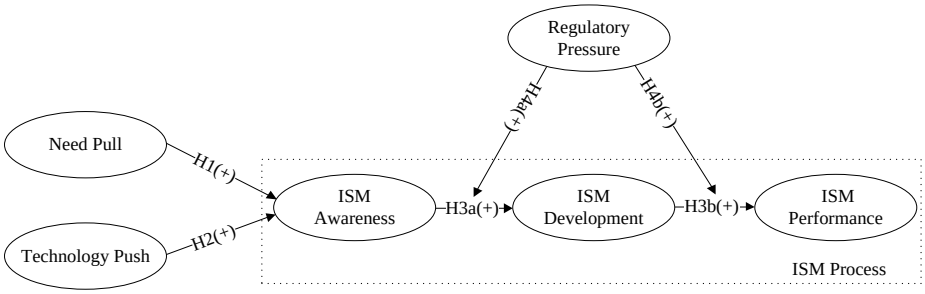

Figure 1. The Research Model and Hypotheses

4 RESEARCH METHODS

4.1 Measures

The measurement model used in the current study was adapted to the ISM context using previously validated. Proper measures were taken to ensure reliability and validity of the measurement instrument being used. All the measures were developed based on a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7).

After the measurement variables were developed, the face validity of the measurement items was assessed. For this, three IS scholars and one management scholar reviewed the measurement items and provided feedback on the length and clarity of each item. Based on the results, several items were modified to fit the purpose of this study. Finally, a pilot study (n=50) was conducted to validate the measurement model, and the results indicate sufficient validity and reliability.

4.2 Data Collection and the Sample

A sample of firms that practiced ISM in various industries was considered. Because it was difficult to collect data from firms, a research firm was employed to conduct a survey of 2,000 firms that were randomly chosen from two stock markets in Korea—the Korea Composite Stock Price Index (KOSPI) and the Korean Securities Dealers Automated Quotation (KOSDAQ)—and an industry association—the Korea Foreign Company Association (FORCA). FORCA included more than 12,160 foreign firms.

Here the generalizability was enhanced by considering a diverse set of firms in terms of their size, sales, and locations, among others. A total of 197 responses were collected, but 12 were excluded for a final sample of 185 respondents because of incomplete responses or because the firm did not practice ISM. Table 1 shows a breakdown of these 185 respondents in terms of their industry, HQ location, and position, among others.

Demographic Characteristics	Frequency (*n=185*)	Percentage (100.0%)
Primary Industry		
IT	32	17.3%
Manufacturing	40	21.6%
Education/service	31	16.8%
Logistic/transportation	29	15.7%
Finance/banking	44	23.8%
Other	9	4.9%
Location of Corporate Headquarters		
North America (U.S./Canada)	41	22.2%
Europe (e.g., Germany, France, the U.K., and the Netherlands)	55	29.7%
Asia (e.g., Japan, Korea, China, and Singapore)	79	42.7%
Other (e.g., Australia and Africa)	10	5.4%
Position		
CEO	19	10.3%
CFO	40	21.6%
CIO	38	20.5%
CTO	46	24.9%
Senior IT Manager	32	17.3%
Other	10	5.4%
Number of Full-Time Employees		
Fewer than 300	7	3.8%
300-499	27	14.6%
500-999	50	27.0%
1,000-1,499	48	25.9%

1,500-2,000	26	14.1%
More than 2,000	27	14.6%
Annual Sales ($) in the Most Recent Year		
Less than 100 million	15	8.1%
100-499 million	61	33.0%
500 million -1 billion	78	42.2%
More than 1 billion	31	16.8%
Frequency of ISM Practices		
Once a year	6	3.2%
Quarterly	36	19.5%
Bimonthly	49	26.5%
Monthly	83	44.9%
Other	11	5.9%
Penalties for ISM Violations (Multiple Responses)		
No action taken	6	3.2%
Reprimand by management	116	62.7%
Suspension from duties	79	42.7%
Dismissal	65	35.1%
Legal action	60	32.4%
ISM Actions (Multiple Responses)		
Presenting strong security policies (penalty/compensation)	126	68.1%
Controlling access to internal systems	43	23.2%
Maintaining a system of precaution/monitoring	22	11.9%
Checking any security vulnerability on a continuous basis	137	74.1%
Using up-to-date hardware/software (e.g., antivirus software and firewalls)	114	61.6%
Providing continuous ISM-related education and training programs	59	31.9%
Investing in ISM in conjunction with placing related personnel	42	22.7%
Other	8	4.3%

Table 1. Respondents

4.3 Assessment of Non-Response Bias

For the maximization of the external validity of the instruments and the determination of any bias in the results, non-response bias was assessed. This bias assumes that late responses are more likely to be similar to non-responses and compares early responses with late ones with respects to all measurement items for both samples (Rogelberg & Stanton, 2007). Any difference between early and late responses implies some non-response bias.

The first 25% of the responses were classified as early responses and the last 25%, as late responses. The mean difference between the two groups of responses was examined. The results show that two items for need pull (np5) and technology push (tp4) display significant differences between the two groups. For example, early respondents were more likely than late ones to support the establishment of strategic planning processes with business partners and show a clear understanding of ISM. Therefore, these two items were excluded. No other items showed such differences, and therefore non-response bias was not a serious concern.

5 RESULTS

5.1 Assessment of the Measurement Model

Variance-based structural equation modeling (SEM) using SmartPLS 2.0 was employed to analyze the measurement model. This PLS approach was taken for the following two reasons: First, the main objective was to determine the predictive validity of the specified paths, not to establish a causal

model with the best fit. Second, this study is more exploratory than confirmatory in nature because few studies have examined the factors influencing ISM awareness, development, and performance. Therefore, variance-based SEM based on the PLS was more appropriate for this study than covariance-based SEM such as LISREL and AMOS. In addition, the PLS approach tests both the measurement and structural models simultaneously.

The reliability and validity of the measurement model were assessed by evaluating internal consistency (reliability), convergent validity, and discriminant validity. However, two items (np 5 and tp 4) were excluded because of non-response bias. Internal consistency was assessed using Cronbach's alpha for each latent variable. Here the generally accepted threshold for sufficient internal consistency is 0.7 (Nunnally, 1978). Cronbach's alpha for all variables ranged from 0.782 to 0.914, indicating sufficient internal consistency. Table 2 presents the results for reliability and internal consistency.

Convergent validity was assessed by examining loadings of individual items. Sufficient convergent validity is generally indicated when these loadings exceed 0.7 with respect to their proposed factors, which implies that more than 50% of the variance in the observed variable is shared with measurement items (Chin, 1998). As shown in Table 3, all items showed loadings exceeding the recommended threshold, indicating that the survey instrument was sufficient for measuring each construct individually. In addition, all items had AVE and composite reliability values exceeding their respective thresholds (0.5 and 0.7, respectively) (Fornell & Larcker, 1981).

Latent Variable	# of Items	AVE	C.R	Cronbach's Alpha
Need Pull	7	0.610	0.866	0.821
Technology Push	7	0.643	0.882	0.856
Regulatory Pressure	4	0.619	0.866	0.782
ISM Awareness	5	0.589	0.877	0.820
ISM Development	4	0.655	0.883	0.914
ISM Performance	4	0.592	0.853	0.899

Table 2. Results for Reliability

Finally, discriminant validity was assessed by examining the square root of the AVE and correlations between constructs. For sufficient discriminant validity, the square root of the AVE should exceed the respective correlation between constructs (Chin, 1998). As shown in Table 4, all AVE values (diagonal value) exceeded their respective correlations (off-diagonal values), indicating sufficient discriminant validity. Because the measurement model demonstrated sufficient validity and reliability, the structural model and hypotheses were evaluated with confidence.

Items	1	2	3	4	5	6
np1	**0.767**	0.098	0.025	0.155	0.204	0.021
np2	**0.791**	0.141	0.038	0.098	0.121	0.035
np3	**0.800**	0.065	0.060	0.036	0.070	0.107
np4	**0.780**	0.036	0.217	0.327	0.155	0.136
np5	**0.458**	0.208	0.246	0.201	0.069	0.417
np6	**0.756**	0.162	0.218	0.228	0.045	-0.075
np7	**0.792**	0.154	0.300	0.019	0.167	0.355
tp1	0.121	**0.815**	-0.075	0.212	0.065	0.054
tp2	0.250	**0.828**	0.125	0.098	0.030	0.220
tp3	0.051	**0.813**	0.238	0.083	0.334	0.122
tp4	0.172	**0.485**	0.060	-0.002	0.153	0.416
tp5	-0.142	**0.729**	0.027	0.074	-0.013	0.184
tp6	0.117	**0.812**	-0.161	0.092	0.148	0.027
tp7	0.282	**0.810**	0.051	0.116	0.101	0.020
rp1	0.367	0.225	**0.781**	0.203	0.163	-0.046

rp2	0.110	0.133	**0.848**	0.017	0.001	0.021
rp3	0.241	0.179	**0.770**	0.122	0.086	0.044
rp4	0.201	0.178	**0.743**	0.207	0.107	0.068
isma1	0.291	0.296	-0.171	**0.793**	0.153	-0.018
isma2	0.278	0.352	-0.160	**0.773**	0.133	-0.055
isma3	0.286	0.058	-0.299	**0.715**	-0.009	-0.203
isma4	0.235	-0.052	0.111	**0.783**	0.013	0.022
isma5	0.270	0.142	-0.263	**0.771**	0.052	-0.058
ismd1	-0.067	-0.375	0.017	-0.217	**0.751**	0.295
ismd2	0.260	0.080	0.132	0.038	**0.848**	-0.100
ismd3	0.283	0.047	-0.039	0.087	**0.823**	0.069
ismd4	-0.149	-0.070	0.118	0.080	**0.812**	0.035
ismp1	-0.016	-0.184	0.143	-0.199	0.078	**0.742**
ismp2	0.257	-0.025	0.081	0.044	0.101	**0.780**
ismp3	0.271	0.239	-0.175	0.101	0.011	**0.736**
ismp4	0.174	0.082	0.119	0.069	-0.052	**0.818**

Note: 1: Need Pull; 2: Technology Push; 3: Regulatory Pressure; 4: ISM Awareness; 5: ISM Development; 6: ISM Performance. Two items (np5 and tp4) were removed due to a low factor-loading value.

Table 3. Loadings and Cross-Loadings for the Measurement Model

Latent Variable	1	2	3	4	5	6
1. Need Pull	**0.781**					
2. Technology Push	0.232	**0.802**				
3. Regulatory Pressure	0.271	0.382	**0.786**			
4. ISM Awareness	0.456	0.391	0.340	**0.767**		
5. ISM Development	0.432	0.257	0.355	0.441	**0.809**	
6. ISM Performance	0.327	0.422	0.422	0.499	0.476	**0.770**

Note: Items in bold type along the diagonal represent the square root of the AVE. For discriminant validity, diagonal values should exceed off-diagonal correlations.

Table 4. Results for Discriminant Validity

5.2 Assessment of the Structural Model

The structural model was formulated using SmartPLS 2.0 to test the relationships between the constructs in the research model. This approach yields two crucial pieces of information for testing hypothesized relationships. The first piece is the standardized coefficient (β), which specifies the strength of the relationship between two constructs (Wixom & Watson, 2001). The second piece is the squared multiple correlation (R^2) for each endogenous variable, which serves as a measure of the predictive power of the research model (Chin, 1998). The R^2 value indicates the percentage of the variance explained by independent variables in the structural model.

Figure 2 shows the standardized path coefficients of the variables along with their respective significance levels and variance explained.

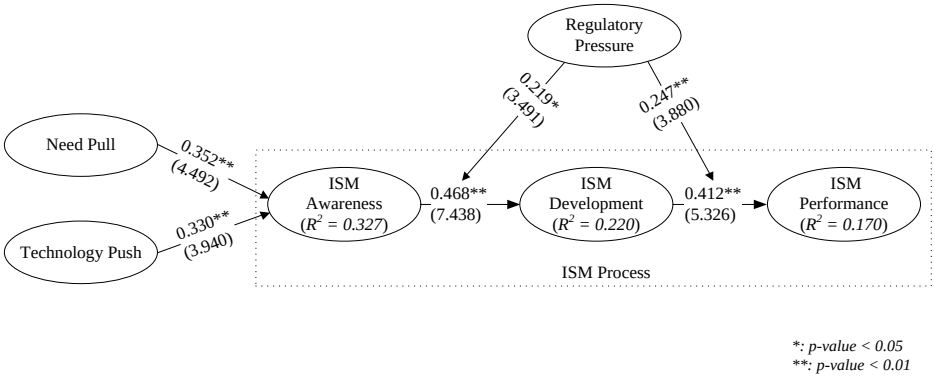

Figure 2. The Structural Model

6 DISCUSSION AND CONCLUSION

The goal of ISM is to minimize damage to organizations by preventing and controlling security problems caused by unexpected intrusions and accidents. Information security is highly complex and involves many threats both within and outside the organization consisting of intentional as well as unintentional acts. ISM is the process of managing potential security threats to protect information assets. Here information awareness is an important factor in the ISM process.

The results have important theoretical and practical implications. The study contributes to the literature by providing a better understanding of ISM. The proposed model contributes to previous literature by applying both need-pull and technology-push in the context of ISM. The model clearly demonstrates the ISM process in which information security flows from ISM awareness to ISM development and performance, and reveals the moderating effect of regulatory pressure on the relationships among ISM variables in the process. This model provides a new theoretical foundation for future research on information security. By employing real data from organizations practicing ISM, future research can generalize this study's results to various industries.

The results provide practitioners with important insights by highlighting the benefits that organizations can derive through a better understanding of ISM and various factors that influence it. In particular, small and medium-size firms with little or no ISM experience can gain a deeper understanding of this process to better protect their information assets. By understanding organizations' internal needs and external pressure, security analysts can seek new technologies that can be pushed to employees to protect information assets. In addition, managers can better meet employees' needs if they have a clearer understanding of those needs, and this can help protect their sensitive information. The proposed model can serve as a guide for developing and implementing an ISM system within an organization. The results highlight the importance of ISM awareness among all members of the organization in enhancing their security-related behavior.

This study has some limitations. First, like most surveys, this study reflects a low response rate and some non-response bias. Non-response bias was assessed by comparing early respondents with late ones, and the results indicate that it was not a serious concern in this study. However, because late respondents may be different from non-respondents, future research should validate this study's results. Second, the generalizability of the results may be limited at the global level. In this study, a random sample of firms listed on the Korean stock exchange and those belonging to an association of foreign firms (i.e., FORCA) were employed. In this regard, any generalization of the results to markets outside Korea should be made with caution. Although the inclusion of foreign firms through FORCA may increase the generalizability of the results to foreign contexts, future research should validate the results by considering a wider range of markets at the global level.

References

Appari, A. and Johnson, M.E. (2009), HIPAA compliance: an institutional theory perspective. AMCIS 2009 Proceedings.

Baker, W.H. and Wallace, L. (2007). Is information security under control?. IEEE Security & Privacy, 5(1), 36-44.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

Chang, S.E. and Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361.

Chau, P.Y.K. and Tam, K.Y. (2000). Organizational adoption of open systems: A 'technology-push, need-pull' perspective. Information & Management, 37(5), 229-239.

Chin, W. (1998). The partial least squares approach for structural equation modeling. In G.A. Marcoulides (Ed.) Modern methods for business research, Hillsdale, NJ: Lawrence Erlbaum. 295-336.

Cooper, R. and Zmud, R. (1990). Information technology implementation research: A technological diffusion approach. Management Science, 36(2), 123-139.

Flanagin, A. J. (2000). Social pressures on organizational website adoption. Human Communication Research, 26(4), 618-646.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.

Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002). A prototype tool for information security awareness and training. Logistics Information Management, 15(5/6), 352–357.

Gosain, S. (2004). Enterprise information systems as objects and carriers of institutional forces: The new iron cage?. Journal of the Association of Information Systems, 5(4), 151-182.

Grover, V. and Goslar, M.D. (1993). The initiation, adoption, and implementation of telecommunications technologies in U.S organizations. Journal of Management Information Systems, 10(1), 141-163.

Gupta, A. and Hammond, R. (2005). Information systems security issues and decisions for small business: An empirical examination. Information Management & Computer Security, 13(4), 297-310.

Hsu, C.W. (2009). Frame misalignment: Interpreting the implementation of information systems security certification in and organization. European Journal of Information Systems, 18(2), 140-150.

Hu, Q., Hart, P. and Cooke, D. (2007). The role of external and internal influences on information systems security- A neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.

Kankanhalli, A., Teo, H.H., Tan, B.C Y. and Wei, K.K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154.

Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M. (2005). Information security threats and practices in small business. Information System Management, 22(2), 7-19.

Khalifa, M. and Davison, R.M. (2006). SME adoption of IT: The case of electronic trading systems. IEEE Transactions on Engineering Management, 53(2), 275-284.

Kim, S. and Garrison, G. (2010). Understanding users' behaviors regarding supply chain technology: Determinants impacting the adoption and implementation of RFID technology in South Korea. International Journal of Information Management, 30(5), 388-398.

Lee, C.P. and Shim, J.P. (2007). An exploratory study of radio frequency identification (RFID) adoption in the healthcare industry. European Journal of Information Systems, 16(6), 712-724.

Lee, Y. and Larsen, K.R. (2009).Threat of coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, 18(2), 177–187.

Liang, H., Saraf, N., Hu, Q. and Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. MIS Quarterly, 31(1), 59-87.
Ma, Q. and Ratnasingam, P. (2008). Factors affecting the objectives of information security management. International Conference on Information Resources Management 2008 Proceedings.
Mowery, D. and Rosenberg, N. (1979). The influence of market demand upon innovation: A critical review of some recent empirical studies. Research Policy, 8(2), 102-153.
Munro, H. and Noori, H. (1988). Measuring commitment to new manufacturing technology: integrating technological push and marketing pull concepts. IEEE Transactions on Engineering Management, 35(2), 63-70.
Nunnally, J.C. (1978), Psychometric theory, New York: McGraw Hill.
Schon, D. (1967). Technology and social change. Delacorte, New York.
Shih, H.P. (2006). Technology-push and communication-pull forces driving message-based coordination performance. Journal of Strategic Information Systems, 15(2), 105-123.
Spears, J.L. and Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.
Teo, H.H., Wei, K.K. and Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. MIS Quarterly, 27(1), 19-49.
Wessel, R.V., Yang, X. and Vries, H.J.D. (2011). Implementing international standards for information security management in China and Europe: A comparative multi-case study. Technology Analysis & Strategic Management, 23(8), 865-879.
Wixom, B. and Watson, H. (2008). An empirical investigation of the factors affecting data warehousing success. MIS Quarterly, 25, 17-29.
Yeh, Q.J. and Chang, A.J.T. (2007). Threats and countermeasures for information system security: A cross-industry study. Information & Management, 44(5), 480-491.
Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), 360-365.
Zhang, J., Reithel, B.J. and Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330-340.