A Study on the Factors Affecting the Establishment of Personal Information Management Systems (PIMS)

Young-soo Seo* · Seong-il Lee** · K.T. Hwang***

Abstract

As the dependence on information is increasing, the protection of personal information (PI) becomes a critical issue for the organizations, causing not only financial loss but also negative impacts on corporate images and reputations.

To date, academic research in this area is scarce. This study analyzes the factors affecting the establishment and/or implementation of Personal Information Management System (PIMS) and provides direction for the practice.

In this study, we assume that PIMS is one of the new technology adopted by organizations, and Unified Theory of Acceptance and Use of Technology (UTAUT) model is selected as a base model for the study. Using structural equation modeling technique, both measurement and structural models are validated, and hypotheses are tested.

Major findings of the study include (1) the major driver of the organizations attempting to adopt PIMS seems to be the improvement of the business outcomes, (2) organizational capability and resource are important in the establishment of PIMS, and (3) the perceived difficulty of the establishment of PIMS is not affecting the intention to adopt PIMS.

Since the importance of personal information security is high, establishment of PIMS is becoming one of the critical issues in the organizations. The establishment of PIMS should be encouraged to strengthen the competitiveness of businesses and to enhance the security level of the entire nation. It is expected that this study may contribute to developing plans and policies for establishment of PIMS in practice, and to providing a foundation for further research in this area.

Keywords : Personal Information, Information Security, Personal Information Management System(PIMS)

Received : 2012. 08. 07. Final Acceptance : 2012. 09. 11.

* Director, Deloitte Anjin LLC, e-mail : youngseo@deloitte.com
** Security Consultant, Deloitte Anjin LLC, e-mail: seongilee@deloitte.com
*** Corresponding Author, Professor, Dongguk University-Seoul, e-mail: kthwang@dongguk.edu

1. Introduction

As the dependence of both private and public sectors on information is increasing, concerns for the adverse effects of information are also increasing. Accordingly, social responsibilities of organizations for protection of information are expanding. In addition, compliance requirements for organizations to satisfy the laws and regulations (e.g., Promotion of Information and Communications Network Utilization and Information Protection Act, and Personal Information Protection Act), most of which have been enacted recently, are increasing and strengthening.

In particular, protection of personal information (PI) has become a distinct area beyond just a part of the existing information security, and has been identified as a critical management area which requires special managerial attention. The importance of protection of PI can be demonstrated by the impact of incidents occurred in recent years.

In 2010, two major privacy incidents have occurred, which led a disclosure of 18 millions and 11.25 millions of customers' PIs, respectively. For the cases, the court ruled against the plaintiff due to the difficulty of proving the loss of the plaintiff and fault of the business. However, since the enaction and rectification of the privacy related laws in 2011, the court ruled the business that leaked PIs to pay the suffered customers in another subsequent case. From the case, we can confirm that the protection of PI is a critical issue for the organizations, not only causing financial loss but also impacting corporate images and reputations [KCC, MOPAS, MKE, 2011] [MK Business news, 2012].

Recent development and rapid growth of the new services and devices, such as smart phones, tablet PC and Social Network Service (SNS) require more PIs, and organizations should put in place a management system for protecting PI and privacy of customers [KCC, MOPAS, MKE, 2011]. In addition, management of PIs of both customers and employees are increasingly outsourced for cost and efficiency purposes. Accordingly, the scope and number of person who can access the PI are expanding, and risks of data disclosure and misuse are increasing, resulting in a vicious cycle of strengthening regulations on PI and privacy [KCC, MOPAS, MKE, 2011].

In order to improve the organizational activities for protecting PIs, top management and personnel should recognize the importance of the issue and the need for establishing personal information management system (PIMS), as well as national level regulations and compliance enforcement. Academic research to support and provide direction for the practice is needed, but so far research in this area is extremely scarce. Therefore, this study attempts to analyze various factors affecting the establishment and/or implementation of PIMS, and aims to contribute to promoting the implementation of PIMS in practice and to provide a theoretical basis for further research in this area.

2. Literature Review

In this chapter, before identifying the factors affecting the establishment of PIMS, related

concepts, standards/guidelines and literature are reviewed. First, basic concepts and current status of the area, including the definitions of PI and certification standards, are summarized, Then, we assume that PIMS is one of the new technology adopted by organization, and existing literature on technology adoption and acceptance is reviewed.

2.1 Personal Information and PIMS

In this section, the target and scope of the study are described by summarizing the concept of PI and related management systems and standards.

2.1.1 Concept of PI

While parties that manage and assume responsibilities for information security are normally internal members of organization, privacy or protection of PI should deal with other parties, especially external customers, clients and other outside stakeholders of organizations. Therefore, the scope of protection of PI is broader than the traditional information security [Kim, 2008].

In this context, each organization should define the concept and categories of PI based on the privacy-related laws and regulations at a minimum, and expand them according to its own business structure and service type. In other words, organizations should identify and control PIs to be protected based on the general concept of PI.

According to the related laws, PI refers to an information of an alive person which can be used to identify the person through name, social security number (SSN), images, etc. It includes information that cannot identify a person directly by itself, but can identify a person by combining with other information.

2.1.2 Standards on PIMS

Major PIMS certification standards adopted currently in Korea include PIMS scheme of Korea Information Security Agency (KISA) and BS 10012 of British Standard Institution (BSI). PIMS scheme of KISA is a certification scheme recognized by the Korea Communications Commission in December of 2011. It certifies an organization that exceeds a certain level by reviewing whether the organization has implemented a series of protection measures required for performing activities of protecting PIs systematically and continuously [KISA, 2011].

The scheme describes definition of PIMS, components of the management system and ways to implement the system. It further classifies the system into three major categories : management process, security measures and life-cycle phases [KCC, 2011]. As of 2012, there are about 20 certified organizations, and the organizations are provided with the benefit of fine/penalty reduction in the event of breach of privacy related regulations. In addition, the certification scheme provides customers with the objective criteria to evaluate and identify the organizations that manage PIs securely, and it is expected that the certified organizations can obtain credibility from customers. In October of 2011, the Commission submitted a proposal to ITU-T and ISO/IEC to make the domestic PIMS scheme an international standard, and standardization activities are progressing.

Data Protection Act (DPA) of the United Kingdom is a privacy related law which was initially enacted in 1998 and rectified later in 2000. Purpose of the law is to regulate the activities performed by both public and private organizations, including acquisition, maintenance, use and disclosure of PIs [BSI, 2010]. BSI announced a standard, BS 10012, in May of 2009 to provide specification of the establishment and operations of PIMS to improve the conformance of the legal requirements and maintain compliance [BSI, 2010]. BS 10012 is a first international standard on PIMS, and Korean financial and IT sectors in which protection of PI is critical are attempting to obtain the certification [BSI, 2010].

〈Table 1〉 Concept of PI and PIMS

PI (Personal Information)	An information of an alive person which can be used to identify the person through name, SSN, images, etc.
PIMS (Personal Information Management System)	A scheme for an organization to exceed a certain level by reviewing whether the organization has implemented a series of protection measures required for performing activities of protecting PIs systematically and continuously.

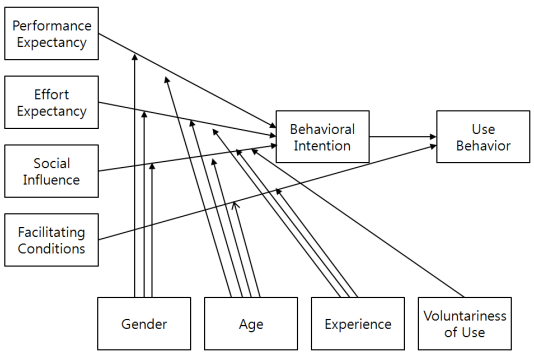
2.2 Literature on Technology Adoption and Acceptance

The adoption and acceptance of new technology have been studied extensively using various models, and attitude and intention of person which are dealt in the social psychology area have been used as major variables. Typical theories on technology adoption include Theory of Reasoned Action (TRA) which applies social psychology, and is used to forecast behaviors of individual's technology acceptance in broad areas [Fishbein and Ajzen, 1975], Technology Acceptance Model (TAM) which is used to forecast behaviors of adoption and acceptance of business related technology [Davis, 1989], and Theory of Planned Behavior (TPB) which adds 'perceived behavioral control' construct, which theorized determining factors of behavior and intention to TRA [Ajzen, 1991]. All these models have become a basis for the various models proposed later.

Until recently, TAM, which has applied TRA to IT area, is being utilized widely in MIS area [Kim, 2011]. However, Venkatesh et al. [2003] has proposed a more refined model, considering that TAM has a limitation in supporting the validity of relationship among various independent variables, and that there is a need for research with more integrated perspective. They proposed Unified Theory of Acceptance and Use of Technology (UTAUT) which integrates eight related models, including TRA (see <Figure 1> below).

UTAUT integrates the constructs that have been proved to be significant in the existing research, and proposed the following four core constructs as independent variables : Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions. These independent variables are assumed to be direct determining factors of Behavioral Intention and Use Behavior. In addition, Gender, Age, Experience and Voluntariness of Use are assumed to mediate the relationship between independent and dependent variables [Yoo et al., 2008]. While the power of the existing TAM to explain the dependent

variables is about 40~50%, UTAUT is known to have improved power of about 70% [Kwon, 2010].



〈Figure 1〉 UTAUT Model

3. Research Model

3.1 Research Model and Hypotheses

This study attempts to analyze the factors affecting the establishment of PIMS focusing on social psychology and human behavior. From the perspective, PIMS is regarded as a new technology adopted by organizations, and UTAUT model is selected as base model for this study. The original model has been slightly modified for the purpose of the study as follows :

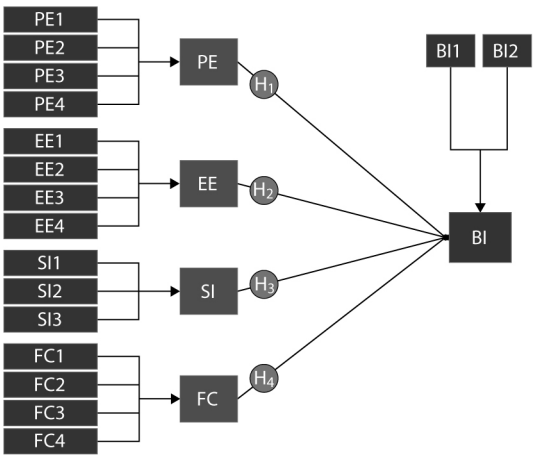
First, Use Behavior construct, which measures the actual status of adoption, is excluded from the research model. The rationale for the exclusion is explained below. The history of PIMS in Korea is quite short. It has been less than 3 years since domestic organizations started to implement PIMS in full scale, and the number of organizations which have already established PIMS is less than 20 as of August 2012 [KISA, 2012]. Under these conditions, it is determined that the measurement of the construct may lack practical validity and reliability at this point, and that research on intention rather than the actual status should be performed in advance to contribute to the practice and further research.

Second, the four mediating constructs (Gender, Age, Experience and Voluntariness of Use) are excluded from the research model. Since PIMS, the target of the study, is a technology utilized by organizations rather than individuals, individual level constructs such as Age and Gender are excluded naturally. As explained earlier, since the history of domestic PIMS is short, Experience with PIMS does not have sufficient meaning, and is excluded from the research model. In case of Voluntariness of Use, PIMS is usually adopted by the mandatory legal requirements rather than voluntary intention. Therefore, Voluntariness of Use does not make sense in the PIMS context, and the construct is decided to be excluded from the model.

Exclusion of mediating variables can be further justified by the previous research on UTAUT in which mediating variables are excluded flexibly by the purpose and target of the study [Lee, 2010; Kim, 2011; Kwon, 2010; Il Im, 2011; Wang, 2010].

Third, the original UTAUT model proposes that Facilitating Conditions (FC) affects only Use Behavior (UB). However, UB is decided to be excluded from the research model. Since FC is one of the important factors, it is assumed that FC would affect not only UB but also Behavioral Intention, and the relationship is added to the research model.

The research model designed based on the above rationale is depicted in <Figure 2>.



〈Figure 2〉 Research Model

Research hypotheses based on the research model is summarized in <Table 2>.

3.2 Operationalization of Variables

Operationalization of the variables has been perform based on the original UTAUT model, but the measurement items have been slightly modified within the scope of not undermining the validity and reliability of the original ones. The items are measured using 5-point Likert scale. Operational definitions and measurement items are summarized in <Table 3>.

〈Table 2〉 Research Hypotheses

No	From	Direction	To	Effect	Description
1	PE	→	BI	+	PE will have positive effect on BI.
2	EE	→	BI	+	EE will have a positive effect on BI.
3	SI	→	BI	+	SI will have a positive effect on BI.
4	FC	→	BI	+	FC will have a positive effect on BI.

〈Table 3〉 Operationalization of Variables

UTAUT Name	Operational Definition	UTAUT Measurement Items	Change	Code	Final Measurement Item
Performance Expectancy	degree to which a person believes that the establishment of PIMS would help improve the business outcome	task usefulness	O	PE1	task usefulness
		task speed	O	PE2	task speed
		productivity	O	PE3	productivity
		salary raise	△	PE4	efficiency improvement
Effort Expectancy	difficulty of establishment of PIMS	degree of understanding	O	EE1	degree of understanding
		degree of proficiency	O	EE2	degree of proficiency
		ease of operation	O	EE3	ease of operation
		ease of use	O	EE4	ease of use
Social Influence	degree to which others agree that establishment of PIMS is important	influence of others	△	SI1	influence of the 3rd party
		opinion of others	△	-	-
		management support	O	SI2	management support
		organizational resource	O	SI3	organizational resource
Facilitating Conditions	degree to which a person perceives that the organization has capability to establish PIMS	degree of resource secured	O	FC1	degree of resource secured
		degree of knowledge secured	O	FC2	degree of knowledge secured
		interoperability	O	FC3	interoperability
		availability of personnel with experience	O	FC4	availability of personnel with experience
Behavioral Intention	intention or plan to establish PIMS	intention to use	O	BI1	intention to use
		expectation to use	△	-	-
		plan to use	O	BI2	plan to use

O : No Change, △: Slight Change.

Performance Expectancy (PE) refers to the degree to which a person believes that establishment of PIMS would help improve the business outcome [Agarwal and Prasad, 1997]. This study revised an item, 'salary raise,' to efficiency improvement (PE4) taking the context of PIMS into consideration.

Effort Expectancy (PE) is a construct which measures the perceived difficulty of establishment of PIMS, including degree of understanding and skillfulness required for establishing PIMS [Davis et al., 1989]. This study utilizes all the original measurement items without modification.

Social Influence (SI) refers to the degree to which others inside and outside of the organization agree that establishment of PIMS is important [Venkatesh et al., 2003]. The original UTAUT model distinguishes 'Influences of others' and 'Opinion of others.' However, in the process of establishing PIMS, Korean organizations usually observe the other organizations' status and effort, but do not attempt to seek the opinion of others. In this regard, the two items were combined into one item, 'Influence of the 3rd party (SI1).'

Facilitating Conditions (FC) is a construct that measures the degree to which a person perceives that the organization has capability to establish PIMS [Davis et al., 1989]. The original measurement items are used without modification.

Behavioral Intention (BI) refers to the intention or plan to establish PIMS [Davis et al., 1989]. In order to reduce the confusion of respondents, two items, 'intention to use,' and 'expectation to use,' are combined since both items can be understood to have a similar meaning to the respondents.

4. Data Collection and Analyses

4.1 Data Collection and Demographics of the Respondents

300 questionnaires are distributed online to the persons working in the information security area between May 30 and June 8 of 2012. The e-mail list of the persons was obtained from ISACA Korea, a professional association specializing in Security, Audit and Control. Of these, 110 questionnaires were collected.

Demographic information of the respondents is summarized in <Table 4>.

If we look at the industry in which the respondents work, Information Communications, Finance and Public Sector, in which the importance of IT and thus PIMS is known to be high, represents nearly 70% of all respondents. The sample shows a good distribution of industry representation.

Size of the organization in which respondents belong, measured by the number of employees, also shows a good representation of organizations. Except the extremely big (more than 10,000 employees) and small (less than 100) organizations, each category of organizations is equally distributed. Experience of respondents in the information security area also shows an even distribution among categories. By the experience of respondents in PIMS, we can confirm the fact that the establishment of PIMS has not been performed in full scale yet.

〈Table 4〉 Demographic Information of the Respondents

Industry	Frequency	Ratio
Information Communications	30	27.3
Finance	24	21.8
Public Sector	22	20.0
Manufacturing	13	11.8
Education	6	5.5
Medical	6	5.5
Distribution	3	2.7
Others	6	5.5
No of Employees		
> 10,000	9	8.2
1,000~10,000	33	30.0
500~1,000	22	20.0
100~500	28	25.5
< 100	18	16.4
Experience (Information Security)		
> 10 Years	21	19.1
5~10 Years	31	28.2
2~5 Years	34	30.9
< 2 Years	24	21.8
Experience(PIMS related)		
ISO 27001	4	12.5
Information Security Checking Service	6	18.8
PIMS	1	3.1
G-ISMS	1	3.1
KISA-ISMS	8	25.0
Other Scheme and Consulting	12	37.5

The collected data are analysed using SPSS 18 and AMOS 18 for confirmatory factor analysis, structural equation model, regression analysis and transformation of variables, etc. SPSS 18 and AMOS 18 are statistics programs to perform various statistic analyses.

4.2 Validity and Reliability Analysis

4.2.1 Analysis Method and Assumptions

Confirmatory Factor Analysis (CFA) is performed for the constructs and measured variables of the research model. CFA performs a factor analysis after setting relationship between variables based on the theoretical background, and can be used to confirm inherent factor dimensions and hypotheses based on the knowledge of the researcher [Kim, 2010]. Therefore, on the ground that hypotheses are established based on the verified factors of UTAUT model, and that there is no formal or universal research method available in the PIMS area, CFA is performed. Through the analysis, construct validity is established. AMOS used in the analysis utilizes maximum likelihood method. The method assumes that all variables follow multivariate normal distribution, and calculates value of factor loading [Kim, 2010].

4.2.2 Validity and Reliability of Variables

Validation of the measurement model includes evaluation of validity and reliability of measured variables. In the structured equation modelling, typical validity to be tested includes convergent validity and discriminant validity.

Convergent validity measures the extent to which an item in an instrument correlates with other measures of the same construct. For convergent validity to be established, value of the factor loading between the measured items and the construct should be greater than 0.7 [Barclay et al., 1995]. The discriminant validity measures whether a construct does not correlate too highly with measures with which it is expected to be different [Churchill, 1999]. For discriminant validity to be established, value of AVE (Average Variance Extracted) should be greater than 0.5 [Chae, 2004; Kim, 2010].

Composite reliability is used to verify the construct reliability. Composite reliability is calculated based on factor loading and sum of errors of measured variables. If the value exceeds 0.7, then construct reliability is established.

<Table 5> summarizes the results of factor loading and composite reliability analyses for the construct and measured variables used in the study. First, most of measured variables exceeds the threshold of 0.7, but EE4, SI1 through SI3, FC3 and FC4 do not satisfy the criteria and convergent validity of the variables is not established. In addition, in case of Social Influence construct, value of the composite reliability is less than the threshold of 0.7, and the construct reliability is not established.

<Table 6> shows the value of AVE for testing the discriminant validity of the construct. As can be seen from the table, the constructs, values of SI and FC do not satisfy the threshold of 0.5, and discriminant validity of the constructs is not established.

In order to resolve the situation, it is decided to remove the Social Influence construct which does not have validity (both convergent and discriminant) and reliability from the model. In addition, measured items which do not contribute to the convergent validity, EE4, FC3 and FC4 from the analysis.

〈Table 5〉 Results of Factor Loading and Composite Reliability

Factor	Code	Variables	Factor Loading	Composite Reliability
Performance Expectancy	PE1	task usefulness	0.835	0.901
	PE2	task speed	0.865	
	PE3	productivity	0.817	
	PE4	efficiency improvement	0.874	
Effort Expectancy	EE1	degree of understanding	0.728	0.817
	EE2	degree of proficiency	0.832	
	EE3	ease of operation	0.775	
	EE4	ease of use	**0.584**	
Social Influence	SI1	influence of the 3rd party	**0.685**	**0.628**
	SI2	management support	**0.531**	
	SI3	organizational resource	**0.711**	
Facilitating Conditions	FC1	degree of resource secured	0.746	0.748
	FC2	degree of knowledge secured	0.820	
	FC3	interoperability	**0.545**	
	FC4	availability of personnel with experience	**0.578**	
Behavioral Intention	BI1	intention to use	0.853	0.810
	BI2	plan to use	0.867	

〈Table 6〉 AVE and Correlations of the Constructs

	PE	EE	SI	FC	BI
Performance Expectancy(PE)	**0.695***	-	-	-	-
Effort Expectancy(EE)	0.415	**0.532***	-	-	-
Social Influence(SI)	0.084	0.463	**0.364***	-	-
Facilitating Conditions(FC)	0.500	0.625	0.542	**0.433***	-
Behavioral Intention(BI)	0.608	0.406	0.261	0.853	**0.681***

*AVE.

The results of the additional analyses after removing the above mentioned measured items and constructs are displayed in <Table 7> and <Table 8>. As can be seen from the tables, validity and reliability of constructs are now established with all the values exceeding the thresholds.

4.2.3 Model Fit

In addition to validity and reliability analyses of the measurement model, analysis of model fit is performed to determine the degree to which the hypothesized measurement model fits the actual model derived from the sample data. The analysis is performed by examining a variety of fit indices, including absolute fit measures (χ^2, degree of freedom, GFI, RMR) and relative fit indices (NFI and NNFI).

The analysis results are summarized in <Table 9>. As can be seen from the table, all the fit indices exceeds the threshold, and the research model shows a good fit for further hypotheses testing.

〈Table 7〉 Results of Factor Loading and Composite Reliability (Revised)

Factor	Code	Variables	Factor Loading	Composite Reliability
Performance Expectancy	PE1	task usefulness	0.836	0.901
	PE2	task speed	0.864	
	PE3	productivity	0.813	
	PE4	efficiency improvement	0.877	
Effort Expectancy	EE1	degree of understanding	0.714	0.828
	EE2	degree of proficiency	0.906	
	EE3	ease of operation	0.721	
Facilitating Conditions	FC1	degree of resource secured	0.817	0.771
	FC2	degree of knowledge secured	0.829	
Behavioral Intention	BI1	intention to use	0.838	0.811
	BI2	plan to use	0.883	

〈Table 8〉 AVE and Correlations of the Constructs (Revised)

	PE	EE	SI	BI
Performance Expectancy(PE)	**0.694***	-	-	-
Effort Expectancy(EE)	0.322	**0.619***	-	-
Facilitating Conditions(FC)	0.537	0.559	**0.627***	-
Behavioral Intention(BI)	0.614	0.376	0.869	**0.683***

*AVE.

〈Table 9〉 Analysis Results of Model Fit

	Fit Indices	Acceptable Level	Research Model
Absolute Fit Measures	X^2/df	close to 1 = good model fit less than 3 = acceptable fit	1.922
	GFI	0.9 or higher	0.900
	RMR	0.08 or lower	0.073
Relative Fit Measures	NFI	0.9 or higher	0.907
	NNFI	0.9 or higher	0.931

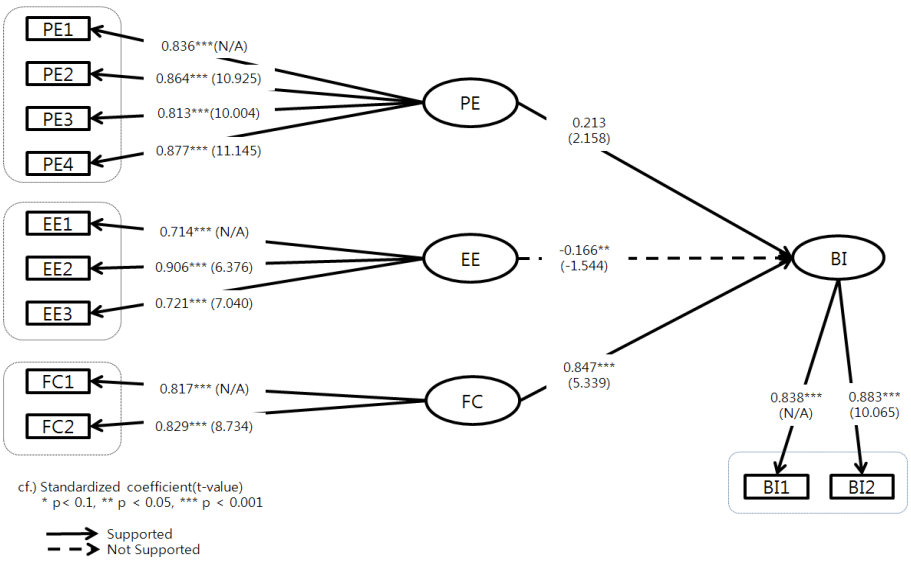
X^2 = 73.045, Degrees of Freedom (DF) = 38, Probability Level = .001

4.3 Hypotheses Testing

Hypotheses testing is performed through AMOS's path analysis to derive both non-standardized and standardized path coefficient with the significance level of 0.05 ($p < 0.05$). Analysis results are summarized in <Table 10> and <Figure 3>. As can be seen from the table and figure, Hypothesis 1 (PE → BI) and Hypothesis 3 (FC → BI) are supported. On the other hand, Hypothesis 2 (EE → BI) was not supported.

From the results of hypotheses testing, Performance Expectancy (PE) is expected to have a significant positive effect on Behavioral Intention (BI). This result implies that major driver of the organizations attempting to adopt PIMS is the improvement of the business outcome. That is, information security activities can contribute the improvement of efficiency and resource utilization of the organization by the establishment of PIMS. This also reflects the intention of organization to manage the effectiveness of PIMS with quantitative measures such as improvement of efficiency and expansion of related resources.

Next analysis results shows that Facilitating Conditions (FC) are expected to have a significant positive effect on Behavioral Intention



〈Figure 3〉 Path Analysis and Results of Hypotheses Testing

〈Table 10〉 Results of Hypotheses Testing

Hypothesis Path			non-standardized coefficient				standardized coefficient	Hypothesis	Support
			Estimate	S.E.	C.R.	P	Estimate		
PE	→	BI	0.234	0.109	2.158	0.031**	0.213	1	Yes
EE	→	BI	-0.239	0.155	-1.544	0.123	-0.166	2	No
FC	→	BI	0.903	0.167	5.399	***	0.847	3	Yes

**p < 0.05, ***p < 0.001.

(BI). This result implies that capabilities and resource of organizations are important in the establishment of PIMS. That is, in order to establish PIMS effectively, it is important to have an individual capabilities such as experience and knowledge of information security personnel and resource to implement and operate the system.

Therefore, organizations should consider a program to improve the capabilities of the information security personnel, such as training and education, and to secure resource needed for effective establishment and operations of PIMS.

The hypothesis that Effort Expectancy (EE) is expected to have an effect BI is not supported. This result implies that perceived difficulty of the establishment of PIMS is not affecting the intention to adopt PIMS. This result may be explained by the fact that most of PIMS implementation is done by external parties, such as consulting firms, in practice. However, as proven by the previous hypothesis, capability of organizations is important in the establishment of PIMS. Too much dependence on outside expertise and low capabilities of internal personnel would result in negative consequences in the operations of PMS. Therefore, it seems imperative that policies and program to develop internal capabilities to operate PIMS effectively after the initial adoption stage should be in place and enforced.

5. Discussion and Conclusions

This study analyzes the factors affecting the establishment of PIMS based on UTAUT model. Four hypotheses are established and tested. Major results of the study can be summarized as follows :

First, the major driver of the organizations attempting to adopt PIMS seems to be the improvement of the business outcomes. From this perspective, organizations adopting PIMS intend to manage PIMS with quantitative measures, such as improvement of efficiency and expansion of related resources.

In addition, considering the business outcomes from another perspective, the benefit of fine/penalty reduction in the event of breach of related laws provided to certified organization may be an important driver for the establishment of PIMS. In fact, PIMS is being recognized as a tool not only to improve the business outcomes, but also to minimize the damage from potential privacy accidents.

Another point is the importance of organizational capability and resource in the establishment of PIMS. In order to establish PIMS effectively, it is required to secure appropriate capabilities and resource. In other words, for the effective establishment of PIMS, individual capabilities such as experience and knowledge of information security personnel are needed. In addition, unlike general IT security, which mainly focuses on IT infrastructure of organization, PIMS incorporates life cycle controls over general activities dealing with PIs. In this regard, PIMS needs additional resource such as dedicated personnel for PIMS, and resource required for operations and maintenance of the system.

Therefore, organizations should strive to improve the capabilities of the information security personnel, and to secure sufficient re-

source needed to not only establishment but also operations and maintenance of the system.

Finally, the perceived difficulty of the establishment of PIMS is not affecting the intention to adopt PIMS. This result may be explained by the fact that most of PIMS implementation is done utilizing the external consulting firms, and organizations do not care much about the degree of difficulty. However, as proven by the previous hypothesis, capability of organizations is important in the establishment of PIMS and heavy dependence on outside expertise and low capabilities of internal personnel would result in negative consequences. Therefore, organizations should establish and operate a program to develop internal capabilities.

At the early stage, most of organizations adopting PIMS regard it as a tool to publicly announce that they are performing information security activities appropriately. However, after going through the implementation and operations stages and understanding the real benefits of PIMS, organizations begin to recognize that the system can be a tool to foster and reinforce information security throughout the organization. It is usually difficult to obtain support from management and business personnel for the information security activities, and to secure and maintain the momentum to operate and continually improve PIMS. Since PIMS is a system based on legal requirements, information security officers should utilize PIMS as a tool to address the challenges faced by them in practice.

The limitations of the study and future research directions are as follows : the ultimate dependent variable of UTAUT model is the Use Behavior, that is, the actual adoption and/or implementation of PIMS. However, the history of PIMS in Korea is quite short (less than 3 years), and the number of organizations which have already established PIMS is less than 20. Therefore, intention rather than actual adoption of PIMS is analyzed. As the area matures, future research should be performed including the Use Behavior construct.

Because of the failure to establish validity and reliability of the Social Influence construct, this study cannot test the effect of the management support and others' opinion about the importance of PIMS on the adoption process. Even though it was not tested in this study, management agreement and support is always an important driver for the success of information system, and it should be emphasized that management support should be obtained for the effective operations and improvement of the system.

The scope and level of information security activities of an organization depend on the relevant laws and regulation. In addition, importance of PIMS differs by industry. However, this study is not able to consider all these environmental factor into consideration. Detailed research taking these external factors into consideration is expected in the future.

In developed countries, U.S. for example, although public authorities publish privacy related standards and guidelines, actual implementation and operations of the management system are left to self-regulated environment in which practical information security activities are performed

by each organization or industry. On the other hand, in case of Korea, most of the personal information security standards are set by the government authority, and essential security controls are forced by law [Kim, 2008]. Since data for this study are collected from Korean respondents, these domestic conditions, perceptions and culture are either assumptions or limitations of the study. In this regard, cross-cultural study among different legal environments could be a good future research topic.

Even though this study focuses on the adoption of PIMS, more important and useful research topic in this area includes performance of PIMS. Ideal research would employ longitudinal approach comparing performances before and after the adoption of PIMS.

Considering the need for and importance of personal information security, establishment of PIMS is one of the critical issues in the organizations. The establishment of PIMS should be encouraged to strengthen the competitiveness of businesses and to enhance the security level of the entire nation. It is expected that this study may contribute to developing plans and policies for establishment of PIMS in practice, and to providing a foundation for further research in this area.

References

[1] Abushanab, E. and Pearson, J. M., "Internet Banking in Jordan : The Unified Theory of Acceptance and Use of Technology (UTAUT) Perspective," *Journal of Systems and Information Technology*, Vol. 9, No. 1, 2007, pp. 78-97.

[2] Agarwal, R. and Prasad, J., "The Role of Innovation Characteristics and Perceived Voluntariness in The Acceptance of Information Technologies," *Decision Sciences*, Vol. 28, No. 3, 1997, pp. 557-587.

[3] Agarwal, R. and Karahanna, E., "Time flies when you're having fun : Cognitive absorption and beliefs about information technology usage," *MIS Quarterly*, Vol. 24, No. 4, 2000, pp. 665-694.

[4] Agarwal, R. and Prasad, J., "The role of innovation characteristics and perceived voluntariness in the acceptance of information technologies," *Decision Sciences*, Vol. 28, No. 3, 1997, pp. 557-582.

[5] Ajzen, I., "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, 1991, pp. 179-211.

[6] Bandyopadhyay, K. and Fraccastoro, K. A., "The Effect of Culture on User Acceptance of Information Technology," *Communications of the Association for Information Systems*, Vol. 19, 2007, pp. 552-543.

[7] Barclay, D. W., Thompson, R., and Higgins, C., "The partial least squares (PLS) approach to causal modeling," *Technology Studies*, Vol. 2, No. 2, 1995, pp. 285-309.

[8] BSI(British Standard Institution), "BS10012," 2010.

[9] Chae, S., "Social Science Research Methodology," Hakhyungsa, 2004.

[10] Churchill, G., Marketing Research : Methodological Foundations, 7th Ed. Dryden Press, USA, 1999.

[11] Davis, F. D., Bagozzi, R. P., and Warshaw, P. R., "User acceptance of computer technology : A comparison of two theoretical models," *Management Science*, Vol. 35, No. 8, 1989, pp. 982-1003.

[12] Fishbein, M. and Ajzen, I., "Understanding attitudes and predicting social behaviour," New Jersey; Prentice-Hall, 1975.

[13] Hennington, A. H. and Janz, B. D., "Information Systems and Healthcare XVI : Physician Adoption of Electronic Medical Records : Applying the UTAUT Model in a Healthcare Context," *Communications of the Association for Information Systems*, Vol. 19, 2007, pp. 60-80.

[14] Hong, K., "A Study on the Effect of Information Security Controls and Processes on the Performance of Information Security," Graduate School of Kookmin University, 2003.

[15] Hsiu-Yuan Wang and Shwu-Huey Wang, "Predicting mobile hotel reservation adoption : Insight from a perveived value standpoint," *International Journal of Hospitality Management*, Vol. 29, 2010, pp. 598-608.

[16] Hung, S. Y., Chang C. M., and Yu, T. J., "Determinants of user acceptance of the e-Government services : The case of online tax filing and payment system," *Government Information Quarterly*, Vol. 23, 2006, pp. 97-122.

[17] Im, Il, Hong, S., and Kang, M., "An international comparison of technology adoption," *Information and Management*, Vol. 48, 2011, pp. 1-8.

[18] Jang, S., Shin, S., and Noh, B., "A Study of the ISCS(Information Security Check Service) on performance measurement model and analysis method," *Korea Institute of Information Security and Cryptology*, 2010.

[19] Jeon, S., Park, N., and Lee, C., "Study on the Factors Affecting the Intention to Adopt Public Cloud Computing Service," *Entrue Journal of Information Technology*, Vol. 10, No. 2, 2011, pp. 97-112.

[20] Nohl, K. and Evans, D., "Quantifying information leakage in tree-based hash protocols," CS-2006-20, *Computer Science Department*, University of Virginia, 2006.

[21] Kim, G., AMOS 18.0 Structural Equation Model, Hannarae Publishing Co., 2010.

[22] Kim, B. and Yoon, M., "Customer Acceptance and Usage Behavior for Airline e-Services by Using UTAUT model," The *Korea Academic Society of Tourism and Leisure*, Vol. 23, No. 6, 2011, pp. 471-491.

[23] Kim, J., "Management System and Governance for Personal Information Security," 2008, pp. 1-2.

[24] Kim, K., Shin, H., Park, S., and Kim, B., "A Study on the Effects of the Information Asset Protection Performance on the Organization Performance : Management Activity and Control Activity," *Korea Society for Information Management*, Vol. 40, No. 3, 2009, pp. 61-77.

[25] Kim, M., "A Study of Factors Influencing Social Media Acceptance for Office Professionals," *Korean Association of Secretarial Science*, 2011.

[26] Korea Communications Commission(KCC) and Ministry of Public Administration and Security and Ministry of Knowledge Eco-

nomy, “Information Security White Book,” 2011.

[27] Korea Communications Commission(KCC), “PIMS(Personal Information Management System,” 2011.

[28] Korea Internet and Security Agency(KISA), “National Information Security Evaluation Indices and It’s Implications, 2007,” *Information Security Issue Report*, 2008.

[29] Korea Internet and Security Agency(KISA), “Personal Information Management System (PIMS) Certification,” 2011, 2012.

[30] Kwon, O., “An Empirical Study on Potential Smartphone Users,” *Internet and Information Security*, Vol. 1, No. 1, 2010, pp. 55-83.

[31] Lee, D., Lim, G., and Jang, S., “A Comparative Analysis on the Usage of Internet Banking Users in Korea and China : Based on the UTAUT Theory,” *Journal of Information Systems*, Vol. 19, No. 4, 2010, pp. 111-136.

[32] Lee, J. and Lee, H., “Evaluating Information Security Investment using TCO-based Security ROI,” *Korea Information Processing Society* 27th, Vol. 14, No. 1, 2007.

[33] Loo, W. H., Yeow, P. H. P., and Chong, S. C., “User Acceptance of Malaysian Government Multipurpose Smartcard Applications,” *Government Information Quarterly*, Vol. 26, No. 2, 2009, pp. 358-367.

[34] MK Business News, “http://news.mk.co.kr/newsRead.php?year=2012&no=255168,” 2012.

[35] Moon, J. and Kim, Y., “Extending the TAM for a World-Wide-Web context,” *Information and Management*, Vol. 28, No. 4, 2001, pp. 217-230.

[36] Oh, J., “Factors of Internet Service Acceptance : A Revaluation of UTAUT Model,” *Korean Academic Society of Business Administration*, Vol. 39, No. 1, 2010, pp. 55-79.

[37] Suh, H., “The Effect of IT Investment by Business-IT Strategic Alignment and IT governance maturity on the IT Performance,” *Seoul School of Integrated Sciences and Technologies*, 2009.

[38] Sun, H., “Impacts of Information Security Policies and Organizations on the Information Security Performance in Korean Enterprises,” *Kookmin University Seoul Korea*, 2005, pp. 1087-1095.

[39] Venkatech, V. and Davis, F. D., “A theoretical extension of the technology acceptance model : Four longitudinal field studies,” *Management Science*, Vol. 46, No. 2, 2000, pp. 186-204.

[40] Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D., “User acceptance of information technology : Toward a unified view,” *MIS Quarterly*, Vol. 27, No. 3, 2003, pp. 425-478.

[41] Yang, K., “Determinants of US Consumer Mobile Shopping Services Adoption : Implications for Designing Mobile Shopping Services,” *Journal of Consumer Marketing*, Vol. 27, No. 3, 2010, pp. 262-270.

[42] Yoo, H., Kim, M., and Kwon, O., “A Study of Factors Influencing Ubiquitous Computing Service Acceptance,” *Society for e-Business Studies*, Vol. 13, No. 2, 2008, pp. 117-147.

Author Profile

Young-soo Seo

Young-Soo Seo is a Director in the Enterprise Risk Services of Deloitte Seoul office. He is currently in the Master's program in Graduate School of Information, Yonsei University. His research interests include Enterprise Risk management, Enterprise Security and Privacy.

Seong-il Lee

He is currently a security consultant at Department of ERS, Deloitte Anjin LLC. He received Ph.D. from Dongguk University, MA. from Chungang University. His research interests include Information Security Strategy, Information Security Governance and Information Security Management System(ISMS).

K.T. Hwang

He is currently a professor at Department of MIS, Dongguk University. He received Ph.D. from State University of New York at Buffalo, M.B.A from George Washington University, and Bachelor of Economics from Yonsei University. His research interests include Information Strategy, IT Governance and IT Service Management (ITSM).

◈ 이 논문은 2012년 08월 07일 접수하여 2012년 09월 11일 게재확정되었습니다.