International Journal of Advanced Science and Technology
Vol.111 (2018), pp.157-174
http://dx.doi.org/10.14257/ijast.2018.111.14

A Study on Factors of Information Security Investment in the Fourth Industrial Revolution

Hong Je Lee[1], Eun Hee Roh[2] and Kyeong Seok Han[3*]

[1]*Department of IT Policy Management, Soongsil University, Seoul, Korea*
[2]*Department of College of Liberal Arts & Sciences, Hansung University, Seoul, Korea*
[3*]*Department of Business Administration, Soongsil University, Seoul, Korea*
[1]*hongje.lee@nicerating.com*, [2]*ehroh@hansung.ac.kr*
[3*]*kshan@ssu.ac.kr*

Abstract

In the era of the 4th Industrial Revolution, information security threats are expanding from the cyber world to the real world, even threatening safety beyond information leakage. Recently, companies have been introducing new technologies such as mobile, wireless LAN, Big Data, Cloud, and IOT, which are key technologies of the 4th Industrial Revolution. However, the security environments are not sufficient to cope with new threats in term of information security organization, budgets, manpower, etc. In order to cope with security risks of the 4th Industrial Revolution, we analyzed information security investment factors to improve level through investments. We designed a research model to extend the UTAUT, consisted of information assets, concerns, experience and habits, social influences and facilitation conditions. For the empirical analysis, we used data from the survey on information security of Korean companies and analyzed correlation through structural equation model. The results showed that information assets, facilitation conditions have a strong influence on experience and habits, intention to investments and experience and habits, investment intention have a strong influence on the 4th Industrial Revolution security investment. Also, there were moderating effects by size, type of business, the experience of security incidents, formal information security organization and policy.

Keywords*: Information Security Investment, 4th Industrial Revolution, UTAUT, Survey on Information Security, PMT*

1. Introduction

The 4th Industrial Revolution that first appeared in the WEF (World Economic Forum) in 2016 is defined as 'the era of technology fusion where the boundaries of physical space, digital space, and biological space are blurred based on the digital revolution'. The CPS (Cyber-Physical System) will have major impacts the industrial structure and market economy model around the world. Every thing (human beings, things and things) will be interconnected and society will become more intelligent with Hyper-Connected and Hyper-Intelligent technology. In terms of technology, IoT (Internet of Things), Cloud, Big data, mobile and AI (Artificial Intelligence) will influence the development of the 4th Industrial Revolution.

However, in the era of the 4th Industrial Revolution of Hyper-connected, all devices are on the network, so there will be a lot of security problems that cannot be compared with current wired and wireless environment. Threats of the cyber world will be expanded

Received (November 15, 2017), Review Result (January 25, 2018), Accepted (January 31, 2018)
* Corresponding Author

ISSN: 2005-4238 IJAST

to the real world, and also become more sophisticated and intelligent. The advancement of digital revolution can be great opportunities, but it can also lead to catastrophic disasters in the event of new security threats. For example, the spread of IoT devices in the smart home, factory, car and city, healthcare is expected to surge 23% annually from 4.6 billion at the end of 2005 to 16 billion by 2021. Gartner predicted that by 2020, 20 percent of all security threats will be associated with IoT. IoT devices are connected to other networks and can be exploited as a cyber-attack route. Malfunctions and illegal manipulation of IoT devices within vehicles, home appliances, and healthcare may cause damages to user's body and threaten safety. Information leakage and privacy threats from IoT, Big Data, and Cloud services will also be increased

According to the KISA (Korea Internet & Security Agency)'s Survey on Information Security in 2016 (Business), the security environments (security policy establishment, organization, manpower, budget, education, *etc.*) of Korean companies are not so good. Also, 15% of businesses with more than 250 employees experienced security incidents in last year. Companies recognized 'information leakage through Cloud or IOT' as the biggest security threat of the 4th Industrial Revolution services. When IoT has been introduced, most businesses are concerned about hacking, malicious code infections, lost or stolen devices, *etc.* But, only 13.9% of companies have been investing in information security for new services, for example, 12.2% for wireless LAN security investment, 2.8% for mobile security, and 1.4% for Cloud security [27]. Threats in new services such as IoT, Big data, Cloud are increasing, but the coping environments of information security are not sufficient.

The information security of the 4th Industrial Revolution requires a change in the overall security paradigm that requires not only data protection but also safety for people and environments. For example, Gartner presented the 'New Model for digital security' that ensures confidentiality, integrity, availability of data, as well as privacy, safety, and reliability of people and environments. The purpose of this study is to analyze factors that have an influence on information security investment and to present policies for information security improvement through information security investment in the 4th Industrial Revolution. This study designed a research model for information security investment factors based on the information security risk management, protection motivation theory, UTAUT and empirical data were analyzed by structural equation analysis with statistical program AMOS.

2. Related Studies

2.1. PMT (Protection Motivation Theory)

Fear Appeal describes negative consequences of not following recommendations to users and try to change their attitude and behaviors (*e.g.* anti-dandruff shampoo, mouthwash, insurance, smoking cessation, drug prevention, *etc.*) [16, 17]. Rogers (1975) proposed the **PMT (Protection Motivation Theory)** for predicting a person's reaction to fear appeal. The PMT has explained effects of threat messages, based on assumption that the cognitive (threat and coping appraisal) processes lead to changes in the behavior to protect health [7, 17].

Threat appraisal is an individual's assessment of threatening events and consists of perceived vulnerability and perceived severity.

□ **Perceived vulnerability** - the likelihood of being exposed to threats

□ **Perceived severity** - the extent of damages to individual if threats are successful

Coping appraisal is an individual's assessment of ability to prevent and cope with loss and consists of self-efficacy, perceived response effectiveness, and perceived barriers.

□ **Self-efficacy** - individual beliefs about ability to respond to threats

□ **Perceived response effectiveness** – the effectiveness of recommended behavior in protecting against threats

□ **Perceived barriers** - factors that interfere with behavior such as financial costs, time, difficulties, side effects, *etc.*

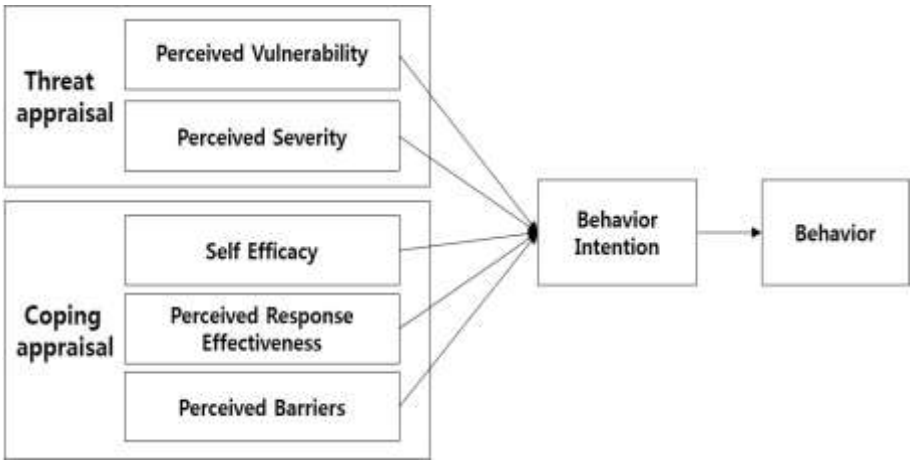

Figure 1. Protection Motivation Theory

Rogers (1975) argued that when five components are perceived at high levels, individuals become more motivated to protect themselves and eventually affect behavioral intentions, lead to behavior. Self-efficacy has been found to have the strongest effect on behavioral intention among independent variables [3, 12, 13, 14]. The PMT has been studied to explain the protection behavior of individuals in various fields such as psychology, education, *etc.* [7]. The PMT is concerned with mitigating or preventing threats [16]. Thus it is related to behavioral intent to adopt security countermeasures to threats. In the field of information security, the fear appeal or PMT have been used to explain individual information security behaviors (*e.g.* security product use and organizational security policy compliance).

2.2. UTAUT (Unified Theory of Acceptance and Use of Technology)/UTAUT2

Venkatesh, Morris, Davis, and Davis (2003) proposed the UTAUT, which integrated TRA (Theory of Reasoned Action), TPB (Theory of Planned Behavior), TAM (Technology Acceptance Model), MM (Motivation Model), MPCU (Model of PC Utilization), *etc.* UTAUT model has been a theoretical and behavioral framework for use intention of new IT systems to improve organizational productivity [20].

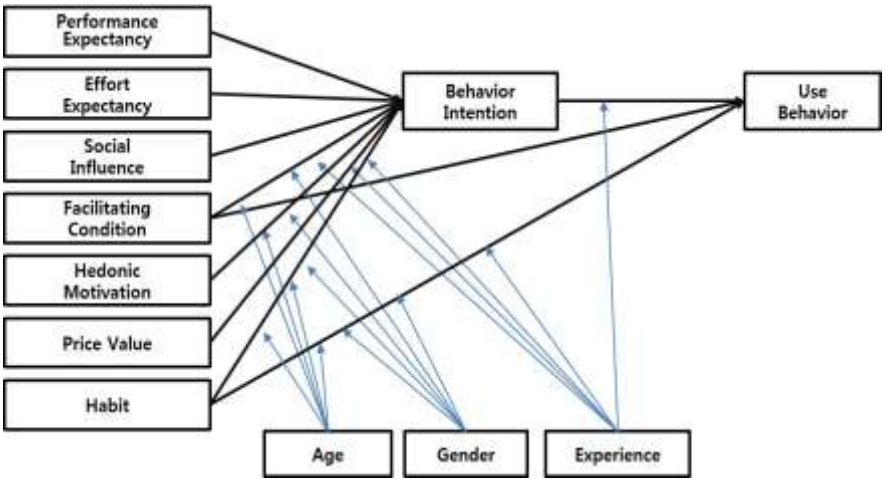

Figure 2. UTAUT2

□ **Performance expectancy** – the degree to which use of new system will help improve job performance

□ **Effort expectancy** - easy or difficult to use a new system

□ **Social influence** – the extents to which important others believe they should use a technology

□ **Facilitating conditions** - organizational resources and technical infrastructure to use a new technology

□ **Behavioral intention** - extent to which a technology is intended to be used

Performance expectancy, effort expectancy, and social influence affect behavioral intentions to use technology. The behavioral intention, facilitation conditions determine technology use. Among predictors, performance expectancy is a key driver for use and behavior. UTAUT model uses gender, age, experience, and voluntariness of use as moderating variables to account for demographic influences. Venkatesh, Morris, Davis, and Davis (2003) validated UTAUT in four business areas (public sector, telecommunications services, finance, and entertainment) and UTAUT have been useful in verifying organizational acceptance of new IT technology [20].

Venkatesh, Thong, and Xu (2012) were interested in consumer technology use and proposed UTAUT2, which extend UTAUT with adding hedonic motivation, price value, and habit predicator [21].

□ **Hedonic motivation** - fun or pleasure derived from using a technology

□ **Price value** - cognitive tradeoff between the monetary cost for using technology and the perceived benefits

□ **Habit** – the degree of tendency to automatically perform after learning

In this study, we are especially interested in the experience and habit of UTAUT2. Experience is an opportunity to use new IT technology, which is the time elapsed since the initial use of the technology. For example, Venkatesh (2003) classified the experience into three phases: after initial training, after one month, and after three months. Habits are related to automaticity, which is measured to the extent that behavior is unconsciously believed to be automatic [21]. Prior use was a strong predictor of future technology use. Habits have direct impacts on the use of technology, and feedbacks from previous experiences have impacts on various beliefs and, consequently, on behavior. Experiences can also control the relationship between facilitation conditions and intent to use. The greater experience, the greater familiarity with the knowledge that promotes user learning. Venkatesh (2012) suggested that habits should be preceded by experience in order for habits to influence on the use of technology [21].

Information security products are also a kind of IT products. Therefore the UTAUT may be applied to use new information security products. Although the UTAUT includes components for intention to use information security technologies, there is little research on IT security countermeasures based on the UTAUT model. Venkatesh (2003) did not include perceived vulnerability and perceived severity when developing UTAUT [20] since UTAUT focused on IT technologies that provide tangible benefits through IT system use. UTAUT model might be better suited to acceptance of new technologies rather than mitigating risks or avoiding losses [2]. Studies based on technology acceptance models, including UTAUT, are limited to whether or not to use IT systems and do not result in any harm even if not used [23, 25]. If users choose not to use new IT system, non-use will not cause any damage or profit. However, not using IT security controls often results in negative consequences such as denial of service attacks, information leakage, *etc.*

2.3. TAM and Information Security Investment

Johnson, A. M. (2005) proposed a research model that extended the Technology Acceptance Model (TAM) model to explain organizational motivation and decision making for information security investment [24]. The proposed model defined external variables that affect perceived usefulness and perceived ease of use of information security.

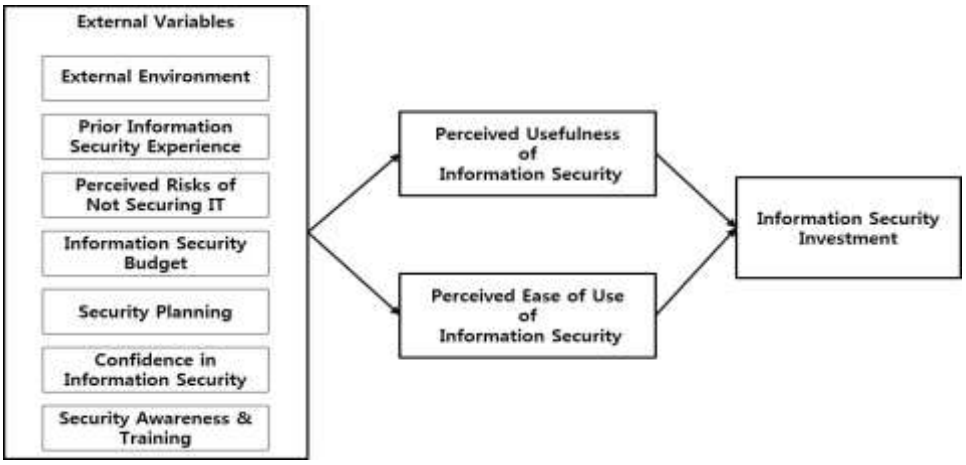

Figure 3. TAM and Information Security Investment

2.4. Related Studies Comparison

We have found similarities and differences in the research models studied in the related studies. For example, perceived risks of not securing IT of TAM and security investment model include the perceived vulnerability and perceived severity of PMT. Perceived response effectiveness of PMT and Performance expectancy of UTAUT and Perceived usefulness, Confidence in information security of TAM are similar components.

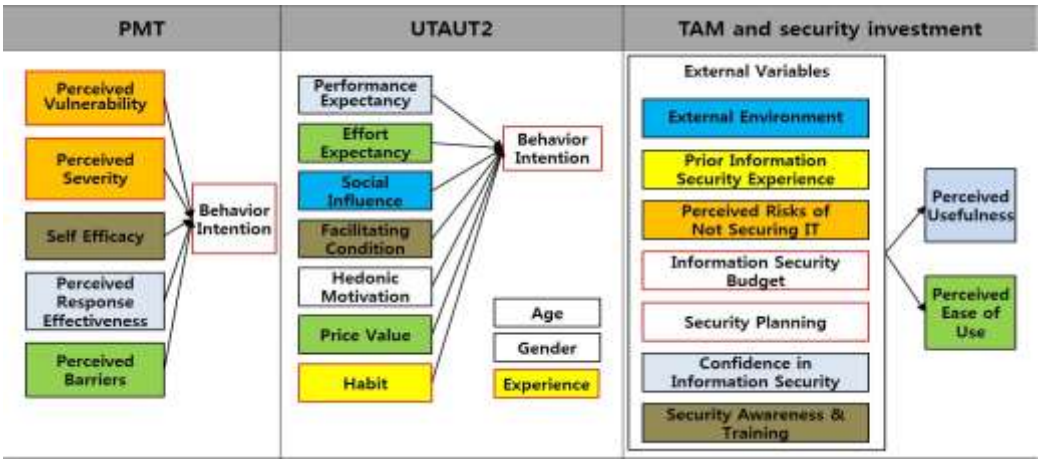

Figure 4. Model Comparison

Comparing the PMT with the UTAUT model in terms of information security technology use, UTAUT has no risk components such as perceived vulnerability and perceived severity of the PMT. The TAM and UTAUT theories have been applied to various types of IT systems but did not consider impacts of not using security countermeasures such as firewalls, anti-viruses, and so on. For example, not installing a firewall increases the likelihood that external attacks will threaten user computers. Firewalls can mitigate external attacks, but they do not provide any direct benefits in terms of improving user performance. The motivation for using security technologies is

related to mitigating negative threats rather than obtaining positive benefits. The use of information security systems reduces threats and vulnerabilities while not providing substantial benefits to users. Survey on information Security in 2016 (Business) [27] also showed that if there were no perceived threats and security incidents, security behavior would tend not to occur. Companies that did not have information security budgets were surveyed that 86.7% did not feel the necessity because there were no information security incidents. Therefore, to analyze technology acceptance of information security technologies, risks such as perceived vulnerabilities, severity would be required.

On the other hand, PMT didn't include social influence or facilitation conditions to explain internal, organizational cognitive processes. Many of technology acceptance studies have supported relationships between social influence and facilitation conditions, so hypothesis that such influences will also exist in intention to use information security technology seems to be reasonable. Survey on information Security in 2016 (Business) showed that 39.2% of companies collect personal information, which is the key information asset of companies. Companies are also collecting sensitive personal information such as social security number (47.6%), account number (22.1%), credit card number (11.8%) and credit information (6.7%). Nevertheless, the levels of technical countermeasures to secure personal information are low. It is necessary to include social influence and facilitation conditions to the research model for the preemptive response, rather than responding after security incidents. Considering a lot of information security incidents in the past, there have been a recurring vicious cycle in which security measures have taken only after security incident occurs.

In order to improve the level of information security in 4th Industrial Revolution, it is necessary to adopt new approaches through aggressive, preemptive response rather than threat based PMT or fear appeal. There are not many empirical studies applying the UTAUT model to information security. However, since UTAUT has been a generic, comprehensive technology acceptance model, it has significant advantages that there are many applicable fields. Therefore, we would extend UTAUT by integrating PMT and security investment model. The research model was designed by considering variables in terms of enterprise security investment rather than personal security behavior and analyzed impacts on the 4th Industrial Revolution information security investment.

3. Research Model and Hypothesis

3.1. Research Model

We designed a research model based on UTAUT, PMT, and information security investment to solve the following research problems.

[Research Topic #1] What are the factors that influence investment of information security in the 4th Industrial Revolution and how do they affect it? How do new threats (e.g. IoT) impact investments in information security?

[Research Topic #2] How does the experience and habits of previous information security products/services use affect information security investment in the 4th Industrial Revolution?

[Research Topic #3] Are there moderating effects on information security investment, depending on the size of the company, the type of business, and the experience of the previous year's infringement? How does the presence of security policies, formal security organization affect investment in information security?

The independent variables of the structural model consist of perceived risk (assets, new concern), social influence, facilitation conditions. We set experience and habits, information security investment intention as parameters and set 4th Industrial Revolution security investment as the dependent variable. The research model also set size (the

number of employees), type of business, security organization, security planning, the experience of security accidents in the last year as control variables.

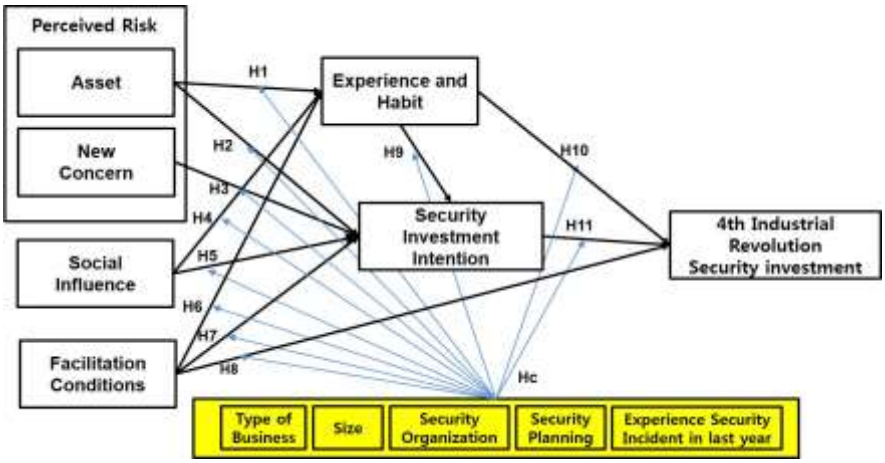

Figure 5. Research Model

The operational definition of the variables used in the study model is as follows.

□ **Information Asset -** information assets for a company to protect from risk

□ **New Concern -** the external new threats and internal vulnerabilities of assets (*e.g.* IoT threats)

□ **Experience and Habit -** experiences of using information security products, services, and periodic vulnerability inspections

□ **Social Influence –** the degree of recognition that information security is important

□ **Facilitation Conditions -** the degree to which we believe that there are an organizational resource and a technical basis for information security investment

□ **Security Investment Intention -** the degree of budget for information security investment

□ **4th Industrial Revolution Security Investment -** information security products that have invested or plan to invest in 4th Industrial Revolution technology (*e.g.* IoT, Cloud, Big Data, Mobile)

3.2. Research Hypothesis

□ **Perceived risk, Performance expectation, and information security investment**

In information security, risk refers to the possibility of unwanted incidents (natural disasters, hacking, information leakage, *etc.*), resulting in economic loss or negative reputations, customers exit, *etc.* Chenoweth (2007) pointed out that decisions about risk were based on inconsistent emotion, belief, and cognition rather than risk analysis [2]. Therefore, the proposed model adopted ISO27005 risk management, an international standard for information security risk management [26]. Information security risks are analyzed as Risks = Asset * Vulnerability * Threat. Risks may also be analyzed as Risks = Assets * Concerns without distinguishing between threat and vulnerability. ISO27005 risk identification finds assets that an organization needs to protect and also identifies the vulnerabilities of assets and possible threats within and outside the organization. Information security is an activity to control perceived risk to an acceptable level. Companies need to invest in security countermeasures to keep risk at DoA (Degree of Acceptance). Risk reduction refers to the implementation of countermeasures against significant risks that can cause harm to the organization. By strengthening security policies or investing in security products or services, an organization can reduce risk by reducing the frequency of risks, eliminating vulnerabilities within assets.

Sometimes, security technology is difficult to use, thereby reducing intention to use information security technology [6]. Although the perceived effectiveness of PMT has been found to affect security products (*e.g.* anti-spyware) or personal information protection behavior [4], Wang (2010) suggested that perceptions of outcomes resulting from non-use security technology have more influence on user attitudes and intention to use than perceived usefulness and perceived ease of use. Wang (2013) also concluded that in anti-phishing scenarios, knowledge of phishing is directly related to the intention to use the anti-phishing software. Since information security investments have effects of reducing organizational risks, risks can be considered as corresponding to performance expectations of UTAUT [22, 23]. As performance expectations increase, use of IT technology increases, so the greater are risk, the more investments in security. In related studies based on PMT, it also showed that the higher the perceived risk, the greater the information security behavior.

H_1: Information assets will have a positive impact on information security use experiences and habits.

H_2: Information assets will have a positive impact on information security investment intentions.

H_3: Perceived new concerns will have a positive impact on information security investment intentions.

□ Social influence and information security investment

Related studies showed that the higher social influence (subjective norm), the higher security behavior [7, 8]. Korean companies tend to invest in information security in order to comply with regulations such as the Personal Information Protection Act, Act on Promotion of Information and Communications Network Utilization and Information Protection, Electronic Financial Transactions Act, *etc.* The social influence (recognition of information security importance of management and employees) is considered as the important factor on information security investments. In a survey on information security in 2016 [27], companies with high information security regulations such as financial insurance, information services companies are highly aware of the importance of information security and high utilization ratios of information security products and services. The survey also showed that the purpose of investing in information security was to 'protect and enhance corporate value (36.2%)' and 'to fulfill obligations such as law (22.2%)' and the ratio of investing in information protection for compliance is also quite high.

Therefore, the following hypothesis was set up to examine the relationship between social influence and information security investment.

H_4: Social influence will have a positive impact on information security use experiences and habits.

H_5: Social influence will have a positive impact on information security investment intentions.

□ Facilitation conditions and information security investment

Facilitation conditions, such as information security organization, manpower, education, are also considered to be an important factor in information security investment. In terms of information security, organizational facilitation conditions of UTAUT are similar to self-efficacy of PMT. In many studies of protective behavior applying PMT, it has been found that there is a strong correlation between self-efficacy and protection behavioral intention [4, 7, 19]. In a survey on information security in 2016, information security budget was the most difficult factor on information security, followed by 'employment of information security professionals (34.0%)' and information security personnel management (28.1%)'. In the case of companies that do not have budgets, 'Do not know how to protect information (29.0%)' was the second. Especially,

the smaller the company size, the less information security budget. Therefore, it is reasonable to assume that the higher facilitation conditions (self-efficacy), the more information security behaviors (investment) will increase.

H_6: Facilitation conditions will have a positive impact on information security product use experience and habits.

H_7: Facilitation conditions will have a positive impact on information security investment intention.

In UTAUT, as the facilitation condition directly affected the behavior, the facilitation condition was considered to have a direct influence on the 4th Industrial Revolution information security investment

H_8: Facilitation conditions will have a positive impact on the 4th Industrial Revolution information security investment.

□ Experience and information security investment

In UTAUT, prior use was a strong predicator of future technology use and feedbacks from previous technology experiences influence behavioral intention and behavior. As information security products are considered as a part of IT products, the use experience of previous information security products will also influence the intention to use new information security products. Habits also have direct impacts on the use of security technologies. Companies will invest in information security to reduce the vulnerabilities that arise from routine vulnerability checks and internal, external security audits. Corporate information security is not a onetime ending task with security product investment, rather a systematic and continuous process-oriented activities. According to ISO27001, which is an international ISMS (Information Security Management System) standard, information security is implemented through repetitive activities of the Plan-Do-Check-Act (PDCA). ISMS consists of information security policy establishment, management, and organization, risk management, implementation of information protection measures (investment), post-management (internal audit, periodic vulnerability check *etc.*). Not securing risks are often detected through regular activities such as periodic vulnerability checks, security audits, and security consulting. Therefore, previous use experiences and periodic inspections of information security were considered to affect the investment of new information security, so added the following hypothesis.

H_9: Previous use experience and habits of information security products will have a positive impact on information security investment intention.

H_{10}: Previous use experience and habits of information security products will have a positive impact on investment on the 4th Industrial Revolution information security investment.

□ Moderating variables and information security investment

There have been statistical differences in the information security investment in Korean companies by business sector. Comparing network security products (*e.g.* firewall, IPS, Web Firewall, *etc.*) utilization rates in a survey on information security in 2016, financial insurance and information service companies are high, but agriculture, forestry, and fisheries, manufacturing and construction industry are low. Also, the larger the company size, the higher the utilization rate of information security products and services.

Companies experienced security breaches in the previous year are more likely to increase their information security investments to lower risk, depending on the degree of severity and number of security incidents.

H_{c1}, H_{c2}, H_{c3}: The type of business, size, and experience of security incidents will have a moderating effect on investment in information security.

H_{c4}, H_{c5}: The presence of security policy, security organization will have a moderating effect on investment in information security.

4. Analysis and Results

4.1. Characteristics of Data

The KISA have conducted an annual survey on the status of information security to assess the level of information security. The survey was conducted through interviews with 9,000 companies, which specialist investigators visited companies selected as samples and received responses to the survey. We collected research data from KISA's survey on information security in 2016 and the research model was verified for companies collecting personal information with more than 10 employees and exclude too small companies. The statistical characteristics of samples are as described in Table 1.

Table 1. Characteristics of Data

Type of Business	Size (employees)					*
	10~49	50~249	250~999	1000~	Total	
Agriculture, forestry and fisheries	12	5			17	
Manufacturing	6	20	34	16	76	10
Construction	3	6	4	3	16	4
Wholesale and retail	41	43	41	1	126	7
Transportation	14	17	17	3	51	11
Accommodation and restaurant	37	54	9	2	102	7
Information service industry	28	59	22	1	110	11
Financial insurance business	99	85	39	14	237	11
Real estate business and leasing	30	31	6	1	68	7
Scientific and technical services	39	44	44	6	133	26
Business facilities support	27	44	29	12	112	8
Associations and organizations	27	37	5		69	10
Etc	33	40	75	72	220	50
Total	396	485	325	131	1,337	162

* Experience security incidents in last year

The construct and measurement items of variables in this study are shown in Table 2.

Table 2. Construct and Measurement of Variables

Construct	Measurement	Source
Asset (AST)	**AST1**-Personal information (general information)	ISO27005
	AST2-Personal information (sensitive information)	
	AST3-Encrypted personal information	
	AST4-Purpose of collecting personal information	
New Concern* (CON)	**CON1**-Hacking and malware	PMT
	CON2-Information leakage	
	CON3-Information system failure	
	CON4-Lost / stolen device	
Experience and Habit (EXP)	**EXP1**-Using network security products	UTAUT2
	EXP2-Using information leak prevention products	
	EXP3-Using security management products	
	EXP4-Using security services (*e.g.* security consulting)	

	EXP5-Vulnerability check cycle and contents	
Social Influence (SOC)	**SOC1-**Importance of information security by management	UTAUT
	SOC2-Importance of personal information security by management	
	SOC3-Importance of information security by employees	
	SOC4-Importance of personal information security by employees	
Facilitation Condition (FAC)	**FAC1-**Information security organization(CISO, CPO)	UTAUT, PMT (Self-efficacy)
	FAC2-Ratio of information security personnel among IT personnel	
	FAC3-Information security education	
	FAC4-Risks included in security plan (policy)	
Security Investment Intention (INT)	**INT1-**Information security budget ratio	UTAUT (Behavior Intention)
	INT2-Budget increase / decrease degree	
	INT3-Security product/service spending in the budget	
	INT4-Ease of budget assurance	
4th Industrial Revolution Security Investment (USE)	**USE1-**Currently investing in 4th Industrial Revolution information security	UTAUT (Use Behavior)
	USE2- Plans to invest in the future in 4th Industrial Revolution information security	
	USE3-Intend to use or use 4th Industrial Revolution Technology**	

* IoT Security threats, **4th Industrial Revolution Technology: IoT, Cloud, Big Data, Mobile

4.2. Validity and Reliability Analysis

Table 3 showed factor loadings, Cronbach's α, CR, and AVE value of measurement items.

Table 3. Convergent Validity

Construct	Measurement	Factor Loading	Cronbach's α	CR	AVE
AST	AST1	.520	**.748**	**.792**	**.572**
	AST2	.714			
	AST3	.892			
CON	CON1	.847	**.832**	**.876**	**.642**
	CON2	.810			
	CON3	.727			
	CON4	.599			
EXP	EXP1	.844	**.910**	**.870**	**.573**
	EXP2	.875			
	EXP3	.879			
	EXP4	.726			
	EXP5	.726			
SOC	SCO1	.770	**.939**	**.957**	**.882**
	SOC3	.952			
	SOC4	.946			
FAC	FAC1	.980	**.862**	**.887**	**.731**
	FAC2	.936			

	FAC3	.643			
INT	INT1	.995	**.962**	**.959**	**.846**
	INT2	.952			
	INT4	.905			
USE	USE1	.788	**.809**	**.888**	**.726**
	USE2	.764			
	USE3	.861			

* Measurement items with low reliability (AST4, FAC4, SOC2, INT3) were removed.

The Cronbach's α coefficient of variables in this study was found to be greater than 0.7, so research variables are consistent and reliable. The Convergent Validity and the Discriminant Validity were verified by CFA (Confirmatory Factor Analysis). In order to verify the Convergence Validity, the standardization factor should be 0.5 or more, the CR (Composite Reliability) value should be 0.7 or more, and the AVE (Average Variance Extracted) value should be 0.5 or more. The results showed that the measurement items of variables were judged to satisfy convergent validity conditions.

To validate the discriminant validity, the AVE value between variables must be greater than the square of the correlation coefficient. The results of the analysis are shown in Table 4 and the highest correlation coefficient is .665 between security investment intention (INT) and facilitation condition (FAC). Correlation squared is 0 ~ 0.442, which is less than the range of AVE (0.572 ~ 0.882).

Table 4. Discriminant Validity

Construct	AST	CON	EXP	SOC	FAC	INT	USE
AST	**.572**						
CON	.046	**.642**					
EXP	.159	.088	**.573**				
SOC	.036	.034	.120	**.882**			
FAC	.138	.078	.422	.109	**.731**		
INT	.136	.094	.386	.037	**.665**	**.846**	
USE	.042	.047	.200	.014	.163	.210	**.726**

4.3. Path Analysis

Path analysis was conducted to analyze impacts of information assets, concerns (threats, vulnerabilities), experiences and habits, social influences, and facilitation conditions on information security investment. Hypothesis H_2 and H_8 were rejected and other hypotheses were adopted.

Table 5. Path Analysis

Hypothesis		Standardized Regression Weights	S.E	C.R.	p-value	Adopt/ Reject
H_1	AST → EXP	.350	.057	10.825	***	Adopt
H_2	AST → INT	.045	.072	1.588	.112	Reject
H_3	CON → INT	.056	.051	2.329	.020	Adopt
H_4	SOC → EXP	.154	.032	6.395	***	Adopt
H_5	SOC → INT	-.105	.044	-4.527	***	Adopt
H_6	FAC → EXP	.409	.020	15.137	***	Adopt

H_7	FAC → INT	.494	.028	18.214	***	Adopt
H_8	FAC → USE	-.052	.023	-1.356	.175	Reject
H_9	EXP → INT	.204	.046	6.393	***	Adopt
H_{10}	EXP → USE	.377	.031	10.015	***	Adopt
H_{11}	INT → USE	.170	.021	4.765	***	Adopt
χ^2=1194.422,df=235,CMIN/df=5.083,RMSEA=.063 GFI=.930,AGFI=.910,PGFI=.728,CFI=.960, NFI=.950,IFI=.953,PNFI=.809,PCFI=.817						

□ **Total Effect (Direct, Indirect Effect) Result**

In path analysis, the degree to which a variable affects other variables is called an effect, which is divided into total effect, direct effect, and indirect effect. The total effect is a sum of the effects of both direct and indirect effects. Direct effects mean the effect of one variable directly on the other, indirect effects means the effect that one variable affects the other variable, but it affects the final variable through the intermediate parameter. The total effects, direct effects, and indirect effects are shown in Table 6.

Table 6. Total Effects, Direct Effects, Indirect Effects

	Total (Direct, Indirect)					
	AST	CON	SOC	FAC	EXP	INT
EXP	**.350** (.350 .000)		**.154** (.154 .000)	**.409** (.409 .000)		
INT	**.117** (.045 .071***)	**.056** (.056 .000)	**-.073** (-.105 .031**)	**.577** (.494 .084***)	**.204** (.204 .000)	
USE	**.152** (.000 .152***)	**.010** (.000 .010**)	**.046** (.000 .046**)	**.201** (-.052 .252***)	**.412** (.377 .035***)	**.170** (.170 .000)

Experience and habits (information security products/services use) are highly affected by facilitation conditions and assets. Security investment intentions (budget) are affected by facilitation conditions, experience and habits, assets. 4th Industrial Revolution Security investment is influenced by experience and habits, investment intentions, facilitation conditions, assets. But, the impact of social influence (recognition of the importance of information security) is low, so the perception of information security of the management and employee does not lead information security investment. Assets have a greater impact on information security investments than new concerns in terms of risk.

4.4. Moderating Effects Analysis

We analyzed whether the size, type of business, and experience of security incidents, formal security organization, security planning (policy) have moderating effects with pairwise parameter comparison between constrained and unconstrained models.The determining method is that if the difference of path coefficients is larger (or smaller) than ±1.96 (α = 0.05), there is a significant difference at 95% confidence level and if it is larger than ±2.58 (α = 0.01) there is a significant difference at 99% confidence level.

Table 7 shows the results of the moderating effects by size (small and medium enterprises: less than 250 employees, major companies: 250 or more employees).

Table 7. Moderating Effects by size

Hypothesized Path	Group				Critical Ratio for differences
	Small Business (n=881)		Major Company(n=456)		
FAC→ EXP	.403	***	.289	***	-3.7
FAC → INT	.465	***	.533	***	2.78
INT → USE	.225	***	-.029	.551	-3.67
EXP → USE	.209	***	.527	***	6.14

* p<0.05, ** p<0.01, *** p<0.001

Table 8. Moderating Effects by Security Incidents and Security Organization

Hypothesized Path	Group (Did you experience security incidents in last year?)				Critical Ratio for differences
	No (=1,175)		Yes (n=162)		
FAC → EXP	.426	***	.314	***	2.53
EXP → USE	.348	***	.628	***	-2.1
INT → USE	.142	***	-.052	.567	2.34
Hypothesized Path	Group (Have formal information security organization?)				Critical Ratio for differences
	Yes (=1,081)		No (n=256)		
FAC → EXP	.271	***	.489	***	3.67
SOC → INT	-.126	***	-.004	.942	3.12
FAC → INT	.459	***	.375	***	-2.13
EXP → USE	.350	***	.242	.004	-3.41

* p<0.05, ** p<0.01, *** p<0.001

The hypotheses and the analysis of moderating effects are summarized in Figure 6.

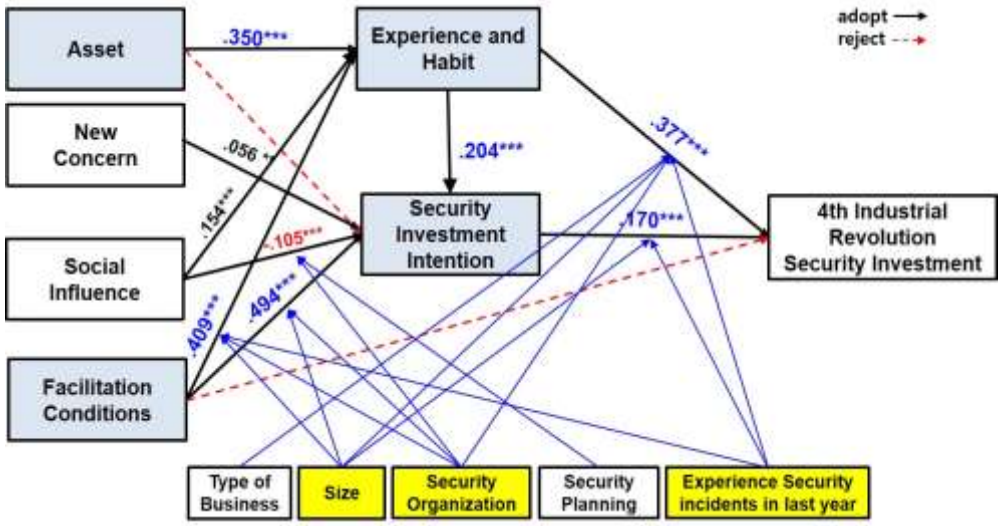

Figure 6. Path Analysis and Moderating Effects

5. Conclusion

In this study, we designed a research model to improve the level of corporate information security through security investment in order to cope with new security threats of the 4th Industrial Revolution. Also, this study analyzed the impacts of the asset, new concern, social influence, facilitation conditions on experience and habits, security investment intention and the 4th Industrial Revolution security investment.

The academic significance of this study is that most of the information security researches have been based on the PMT, but this study empirically demonstrated that UTAUT could also be applied to information security fields by applying UTAUT to the information security investment. Many information security researches also have studied the security behavior of individuals. But, this study extended UTAUT and analyzed corporate information security investment factors with corporate information security survey data. Through empirical data on the security of Korean companies, this study showed that internal factors (asset, facilitation conditions, experience and habits) have more influence on information security investment than negative external factors (threats and vulnerabilities). The result of the study indicates needs to change the paradigm of information security policies for the 4th Industrial Revolution information security. The detail implications of the policies on the information security of the 4th Industrial Revolution era are as follows.

First, perceived risk has a positive impact on experience and habits, security investment intentions, and the 4th industrial revolution security investment. In particular, assets (sensitive information) more directly or indirectly influenced information security products use experience and the 4th Industrial Revolution security investment than new security concerns. Assets are one of the key drivers of corporate security investment. On the other hand, new security concerns show a low correlation, indicating that the security threats of new services such as IoT have little impact on new security investments. Thus, it is necessary to strengthen laws and regulations according to the degree of information assets of enterprise (*e.g.* the number of personal information, the number of information systems, *etc.*). Particularly, in the era of the 4th Industrial Revolution, it is necessary to take pre-emptive countermeasures in order to cope with information leakage of Big Data, Cloud, and IoT. But, currently, many companies do not set budget (86.7%) because there are no security incidents. It is necessary to strengthen management and technical countermeasures according to the number of sensitive information * collection of data in Big Data, Cloud, IoT technology.

Second, social influence has a positive impact on experience and habits. But, social influence has a negative impact on security investment intention (budget, 4th Industrial Revolution security investment). The higher the perception of the importance of information protection, the more likely it is to use security products and services. However, the ratio of information security among IT budget is low compared to recognition of the importance of information security. Low penalty regulations may be one of the causes. In the case of Korean Personal Information Protection Act, when security incidents occur, the penalty of CEO or security officer and damage compensation are low compared to EU GDPR (General Data Protection Regulation). The GDPR imposes a higher penalty compared between 4% of annual sales and EUR 20 million in severe violation. Therefore, it will be necessary to strengthen the punishment of the manager or the responsible person in case of security breach.

Third, facilitation conditions were found to be the most influential factors in experience and habits, security investment intention. The most effective policy to improve the level of information security is to strengthen the facilitation conditions (information security

organization, security personnel, security education). But, the reality of Korean companies is low level ratio of information security organizations, security personnel, security education. In the case of public institutions and SMB (small and medium sized Business), it is difficult to employ security personnel. Low-level security organizations and personnel are the major factors that hinder information security level of the enterprise. As the 4th Industrial Revolution technology have developed, the role of security personnel will become even more important. Therefore, in order to create jobs in the information security sector of the government, it is necessary to cultivate talented manpower and to activate employment for the 4th Industrial Revolution information security. Along with the increase the security personnel ratio through new hiring, it is also necessary to expand outsourcing of information security business (security consulting, monitoring, educations, *etc.*). According to the Survey on Information Security in 2016 [27], 15.4% of companies outsourced information security, and the rate of outsourcing in security monitoring (17.2%) and security consulting (13.8%) were low. In addition, the ratio of company with cooperative channels in the case of security incidents were also low.

Fourth, experience and habits have positive effects on security investment intention and new security investment. Experience in information security products and services and periodic security vulnerability checks have positive impacts on security investment. Feedbacks from information security product and service usage positively affects security investment. Prior use of information security products and services also have a positive effect on 4th Industrial Revolution security investment. Particularly, in case of companies with a large size (more than 250 employees), experience and habit has a greater impact on 4th industrial revolution security investment than small companies. Therefore, it is necessary to promote the use of security products and services to improve information security level. In case of Korea, if companies buy information security products, tax breaks are offered. It is necessary to make more use of security products and services through expanding the tax breaks benefit (increase reduction rate and add information security service outsourcing in tax breaks items).

Acknowledgments

This paper is a revised and expanded version of a paper entitled “An Empirical Study on Investment Factors of Information Security Based on UTAUT” presented at HSST, The 5th International Conference on Interdisciplinary Research Theory and Technology (IRTT 2017), Daejeon, December 2017. This research was financially supported by Hansung University.

References

[1] S. Arekete, P. Ifinedo and B.A. Akinnuwesi, “Antecedent factors to end-users' symbolic acceptance of enterprise systems: An analysis in Nigerian organizations”, Adaptive Science & Technology (ICAST), 2014 IEEE 6th International Conference on, IEEE, **(2014)**, pp. 1-8.
[2] T. Chenoweth, R. Minch and S. Tabor, “Expanding views of technology acceptance: seeking factors explaining security control adoption”, AMCIS 2007 Proceedings, **(2007)**, pp. 321.
[3] D. Fruin, J, C. Pratt and N. Owen, “Protection motivation theory and adolescents' perceptions of exercise”, Journal of Applied Social Psychology, vol. 22, no. 1, **(1992)**, pp. 55-69.
[4] A. Gurung, X. Luo and Q. Liao, “Consumer motivations in taking action against spyware: an empirical investigation”, Information Management & Computer Security., vol. 17, no. 3, **(2009)**, pp. 276-289.
[5] C.-L. Hsu, M.-R. Lee and C.-H. Su, “The role of privacy protection in healthcare information systems adoption”, Journal of medical systems, vol. 37, no. 5, **(2013)**, pp. 9966.
[6] Q. Hu and T. Dinev, “Is spyware an internet nuisance or public menace?”, Communications of the ACM, vol. 48, no. 8, **(2005)**, pp. 61-66.
[7] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory”, Computers & Security, vol. 31, no. 1, **(2012)**, pp. 83-95.

[8] A.C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: an empirical study", MIS quarterly, **(2010)**, pp. 549-566.
[9] W. Kassa, "Information technology security professionals' knowledge and use intention based on UTAUT model", PhD Thesis, Capella University, **(2016)**.
[10] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective", Journal of the Association for Information Systems, vol. 11, no. 7, **(2010)**, pp. 394.
[11] L. Xin, L. Han, Z. Jie and J. P. Shim, "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services", Decision support systems, vol. 49, no. 2, **(2010)**, pp. 222-234.
[12] J. E. Maddux and M. A. Stanley, "Self-efficacy theory in contemporary psychology: An overview", Journal of Social and Clinical psychology, vol. 4, no. 3, **(1986)**, pp. 249-255.
[13] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change", Journal of experimental social psychology, vol. 19, no. 5, **(1983)**, pp. 469-479.
[14] S. Milne, P. Sheeran and S. Orbell, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", Journal of Applied Social Psychology, vol. 30, no. 1, **(2000)**, pp. 106-143.
[15] B.-Y. Ng, A. Kankanhalli and Y. Calvin Xu, "Studying users' computer security behavior: A health belief perspective", Decision Support Systems, vol. 46, no. 4, **(2009)**, pp. 815-825.
[16] R.W. Rogers, "A protection motivation theory of fear appeals and attitude change", The journal of psychology, vol. 91, no. 1, **(1975)**, pp. 93-114.
[17] R.W. Rogers, "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation", Social psychophysiology: A sourcebook, **(1983)**, pp. 153-176.
[18] P. Seuwou, E. Banissi and G. Ubakanma, "User Acceptance of Information Technology: A Critical Review of Technology Acceptance Models and the Decision to Invest in Information Security", International Conference on Global Security, Safety, and Sustainability, Springer, Cham, **(2017)**, pp.230-251.
[19] M. Siponen, S. Pahnila and A. Mahmood, "Employees' adherence to information security policies: an empirical study", IFIP International Information Security Conference, Springer, Boston, MA, **(2007)**, pp. 134-144.
[20] V. Venkatesh, M. G. Morris, G. B. Davis and F. D Davis, "User acceptance of information technology: Toward a unified view", MIS quarterly, **(2003)**, pp. 425-478.
[21] V. Venkatesh, James Y.L. Thong and X. Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology", MIS quarterly, vol. 36, no. 1, **(2012)**, pp. 157-178..
[22] P. A. Wang and E. Nyshadham, "Knowledge of online security risks and consumer decision making: An experimental study", System Sciences (HICSS), 2011 44th Hawaii International Conference on. IEEE, **(2011)**.
[23] P. A. Wang "Information security knowledge and behavior: An adapted model of technology acceptance", Education Technology and Computer (ICETC), 2010 2nd International Conference on. IEEE, vol. 2, **(2010)**, pp. 364-367.
[24] A.M. Johnson, "The technology acceptance model and the decision to invest in information security", Southern Association of Information Systems Conference, **(2005)**, pp. 114-118.
[25] I. Woon, G.-W. Tan and R. Low, "A protection motivation theory approach to home wireless security", ICIS 2005 proceedings, **(2005)**.
[26] ISO, "ISO/IEC 27005: ISO/IEC 27005:2011 Information technology -Security techniques-Information security risk management (second edition)", http://www.iso27001security.com/html/27005.html.
[27] KISA, "2016 Survey on Information Security Business Executive Summary", https://isis.kisa.or.kr/board/?pageId=060200&bbsId=15&itemId=60&searchKey=&searchTxt=&pageIndex=1.

Authors

Hong Je Lee, he received the BS and MS degrees in Computer Science from Korea University, Seoul, Korea in 1996, 1998. He completed his Ph.D. at Korea University's Graduate School of Information Security in 2015 and is currently a Ph.D. student at Soongsil University Graduate School of IT Policy and Management. His research interests include Information Security, Big Data, IoT, Cloud Computing.

Eun Hee Roh, she is an assistant professor at Department of College of Liberal Arts & Sciences, Hansung University, Korea. She received the Ph.D. degree in Engineering from Soongsil University, Korea in 2015, and prior to that, she earned Master of Education in 2001 from Sookmyung Women's University Graduate School. Her research interests include HTML5, Hybrid-App (Web-App), Smart Learning, Digital Contents, Information Security.

Kyeong Seok Han, he is a Professor at the School of Business Administration, Soongsil University, Korea. He received his Ph.D. degree in MIS from Purdue University, United States in 1989, and prior to that, he earned B.A. in 1979 and MBA in 1983 from Seoul National University. He formerly was a Professor of University of Houston. His major research interests include Digital Economy, Business Consulting, ERP, e-CRM, Big Data, Agent-based Simulation.