Asia Pacific Journal of Information Systems
Vol. 30 No. 2 (June 2020), 308-327

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2020.30.2.308

Comparing the Effects of Two Methods of Education (Online versus Offline) and Gender on Information Security Behaviors

Minjung Park[a], Sangmi Chai[b,*]

[a] *Ph.D. Candidate, School of Business, Ewha Womans University, Korea*
[b] *Associate Professor, School of Business, Ewha Womans University, Korea*

ABSTRACT

The importance of information security is increasing, and various efforts are being made to improve users' information security behaviors. Among these various efforts, information security education is mainly aimed at providing users with information security knowledge and improving information security awareness. This study classified the types of information security education into offline and online to examine the effects of each education method on attitudes toward information security (perceived severity, vulnerability, self-efficacy and response-efficacy) and information security behaviors. A survey was conducted for users with information security education experiences. The results obtained by comparing the differences in the path coefficients of personal information security behaviors according to information security education experiences showed that security behaviors were more significant in the online experience group than the offline group. In addition, gender differences were analyzed, and it was found that females had a greater impact on information security attitudes than males. This study also found that among Internet users with online information security education experience, females tend to have more information security behavior than males, but there were contrasting results among users with offline information security education experiences. The results of this study finally address the necessity of reflecting users' personalities in the systematic design of information security education in the future. Furthermore, the results of this study support the need for an appropriate education system that sufficiently understands education types to maximize the effects of information security education.

Keywords: Gender Difference, Information Security, Information Security Behaviors, Offline Education, Online Education, Protection Motivation Theory

Ⅰ. Introduction

Early IT companies around the world have been operated by men and have low proportions of women. As a result, most IT companies have been predominantly formed by male-centered cultures, and most

*Corresponding Author. E-mail: smchai@ewha.ac.kr

women perceive that they are not treated equally to men. This sentiment was due to the relatively high proportion of women who felt relatively deprived due to wage discrimination, although men and women performed the same tasks, or due to the proportion of women among all executives being low. Based on the results of a number of studies in which men were reported to have significantly higher wage rates than women, gender-based pay gaps increasingly exist in society (Kim, 2017). Due to these impacts, gender issues in IT companies have expanded and affected the entire IT industry. Recently, however, these barriers to gender issues have been broken down. Google, the global leader among IT companies, has been working to bridge the gender pay gap since 2012. In 2017, women's average wages at Google were finally higher than men's; although it looked like there was reverse discrimination, the company reportedly made various official efforts to bridge the gender wage gap (Fortune, 2019). In addition, Apple, Amazon, and Intel have maintained gender wage ratios of 99.6%, 99.0%, and 100%, respectively, thereby alleviating gender-based pay gaps (QUARTZ, 2016). The proportion of women in other IT sectors, including computer programming, is still quite low, although the gender wage gap has decreased.

Despite the advances in the IT and information security areas, where the latest technology is most rapidly accessed, there are still notable gender differences in those fields. In a cybersecurity environment, perceived gender stereotypes of career and willingness to continue a work career had a negative relationship (Chai and Kim, 2012). A number of studies have been performed to compare the habits and frequencies of the personal information security behaviors of online users based on gender. Female users have a tendency to have more negative feelings toward data leaks and privacy infringements, are more risk-averse than male users, and tend to have more active information security behaviors (Garbarino and Strahilevitz, 2004; Murphy and Tocher, 2011; Suh and Hee, 2002). It is known that females are more prone to information security behaviors because they are highly concerned about situations such as data breaches or leakage (Gilbert et al., 2003; McCormac et al., 2017). To protect personal information, males mainly adopt methods such as installing firewalls and performing frequent data backups, while female users tend to improve their information security awareness by taking information security education or training programs and obtaining related news (Hazari et al., 2008). It can be inferred that there are various differences in the information security behaviors that users adopt in information security environments due to their personal characteristics including gender. Based on these prior studies, this study assumed that there would be a difference in the effects of information security education by gender.

As information security education programs has increased due to the recent growth of importance of information security, this study intends to identify whether there is a gender difference in the effectiveness of information security education. We will also investigate the differences of information security attitudes based on gender. The result of this study finally suggests that the necessity of reflecting individual characteristics as gender, in the process of designing information security education or training programs. Furthermore, this study measures the effectiveness of education on information security behaviors according to the education type (i.e., online and offline education). This study defines offline courses as being conducted by educational facilities that have limited space, including public and private

institutions, universities, etc. In addition, all education that occurs through the Internet is classified as online education. Accordingly, this study finally raises the following research questions.

1. *Do significant differences exist in users' education effectiveness (= information security behaviors) depending on the type of information security education and gender?*
2. *Do significant differences exist in users' attitudes toward information security (perceived severity, perceived vulnerability, self-efficacy, and response-efficacy) depending on the type of information security education and gender?*

Ⅱ. Theoretical Background

2.1. Information Security Education and Gender

As the social importance of information security education increases, legal regulations are being set up around the world that mandate information security education for public institutions and firms. Article 28 of the Personal Information Protection Act in Korea compels that firms provide regular education and training for their staff members that treat personal information at least once a year to ensure the proper processing of personal information. Similarly, Article 4f, paragraph 3 of Germany's Privacy Act requires that data controllers participate in training to maintain the specialized knowledge that is necessary to fulfill their obligations.

A numerous study related on information security education is actively being performed, in the recent. The research on information security education can be summarized as reviews on the impacts on information security behavior and compliance with information security policies. The studies on the impacts of information security education on security behaviors have mixed results. First, the establishment and operations of well-designed information security education and training programs in firms or organizations have been found to induce information security behaviors in their employees or members (Park et al., 2011; Puhakainen and Siponen, 2010). Thus, organizations have been considered to be the best approach to conducting information security education for their members or employees in order to maintain information security (Arachchilage et al., 2016; Le Compte et al., 2015). In other words, the completion of an information security education program by an organizational member has a direct impact on increasing their security behaviors (Arachchilage et al., 2016; Kirlappos et al., 2011; Schneier, 2000). Second, the information security education and training programs of firms have been shown to positively influence employees' intentions to comply with information security policies and to enhance their expertise in information security (Siponen et al., 2014). In contrast, a few previous studies also have identified that information security education does not always significantly affect an individual's information protection behavior (D'Arcy et al., 2009; Dinev and Hu, 2007). These findings indicate that information security education does not always directly stimulate personal information protection behavior. These results can be drawn that information security education is not a negative countermeasure such as penalty or wage cuts, rather, is a positive countermeasure that raises the information protection awareness among employees (Lebek et al., 2013).

There are a number of studies that have identified the factors affecting the effectiveness of information security education; these studies found that information security education has varied effects on security behavior and compliance with information

security policies. As a result of examining individual characteristics such as gender, age, education level, and personality, it was found that there is a significant difference between information security attitudes and completed information security education according to gender (Anwar et al., 2017; Ifinedo, 2014; McCormac et al., 2017; Vance et al., 2012). Since females are more likely to perceive information security risks than males, security behaviors, have also been reported to be higher among females (McCormac et al., 2017). These differences in information security attitudes by gender are inferred from the fact that females are more likely to experience 'technophobia', which refers to a fear of advanced technology, than males and that the proportion of females who perceive information security concerns is relatively higher than that of males (Gilbert et al., 2003). Therefore, this study intends to clarify the differences among the effects of personal information security behaviors according to information security education by gender.

2.2. Protection Motivation Theory

Protection motivation theory (PMT) was first applied in the health sciences field to judge the response of a patient to the diagnosis of a disease but has recently been widely used in the information security field. This theory has been developed to explain fear based on expectancy- value theory and cognitive-processing theory, as well as how an individual perceives and responds to risks (Maddux and Rogers, 1983). In health sciences, PMT has been developed to explain behavioral changes that can protect one's health by using protection motives based on the cognitive evaluation processes of the threat appraisal and coping appraisal (Ifinedo, 2012; Rogers, 1975).

A threat appraisal consists of the perceived vulnerability and perceived severity from an individual's assessment of a threatening event. Perceived vulnerability refers to the degree of likelihood that a threat occurs, and perceived severity indicates the severity of the damage that may be caused by the potential negative consequences (Liang and Xue, 2010; Lim et al, 2017; Rogers, 1975). A coping appraisal is a confidence of an individual's ability to prevent and cope with the losses resulting from a threat and consists of self-efficacy and response-efficacy (Son et al., 2014). Self-efficacy refers to your ability to prevent and respond to threats (Bandura, 2010). Response-efficacy is a measure of the belief that threats can be reduced by acting on threats (Prentice-Dunn et al., 2009). This study examines the effects of the experience of information security education on the perceived vulnerability, severity, self-efficacy, and response-efficacy based on protection motivation theory. In particular, the four factors that were presented above are will be compared by using each path coefficient in order to identify the differences according to the type of information security education and gender, respectively.

Ⅲ. Hypothesis Development

3.1. Type of Education and Achievement

With the development of IT technology, various web-based learning programs have been instituted that can educate individuals without time and spatial limitations (Hubalovsky et al., 2019; Salloum et al., 2019). A web-based learning program is different from existing classroom-based programs that are conducted in a limited space at a predetermined time. In recent years, online learning programs have been actively generated and utilized by both private educa-

tional institutions and public institutions (Lee and Park, 2018). Online lectures involve education that is conducted by using communication media when a teacher and students are physically separated from each other, and this type of education is widely referred to as distance education, online learning, online education, and e-learning (Lee and Kim, 2018). As online education courses have become more popularized and their demand increase, many empirical studies have been conducted that compare two education methods (online vs offline) with regard to learning achievements (Ahn and McEachin, 2017; Chingos and Schwerdt, 2014; Hubalovsky et al., 2019; Hwang et al., 2012; Miron and Urschel, 2012; Thirunarayanan and Perez-Prado, 2001; Yu, 2013). There was a difference between students' academic achievements in the two education types: traditional offline courses and online courses. Most studies identify that online education has no significant impact on academic outcomes compared to offline education (Ahn and McEachin, 2017). Students who took online classes received lower grades on standardized tests than those who completed the same contents in traditional classroom-based courses for both regular curriculum and one-time education programs (Ahn and McEachin, 2017; Chingos and Schwerdt, 2014). Despite the same contents being delivered to students at the same time, it could be inferred that the effect of the education was different due to the spatial limitations and the delivery method. As a result, it can be summarized that regardless of class contents that were offered, the effectiveness of online training has been reported to be lower than that of offline training (Ahn and McEachin, 2017; Chingos and Schwerdt, 2014). Furthermore, the academic achievements from online education were lower than those of offline education, regardless of the nation, economic status and social status of the students (Miron and Urschel, 2012). However, the intentions to retake a course according to the students' satisfaction with the lectures was higher among the students who took online courses than that for those who took offline courses (Yu, 2013).

The variety of online and offline information security education programs that are managed by corporations and public and private educational institutions has recently increased. They organized education and training programs to educate users on how to protect their information and to improve the awareness and importance of information security that users perceive. In particular, as online lectures are popularized, online lectures on information security are being actively designed and conducted to educate users. Most prior studies emphasize the need for operating information security education and training programs; however, there are no studies that examine the effects of security behaviors on the method or the type of education. Therefore, this study aims to identify whether there are significant differences in the educational outcomes of online and offline education methods for information security. Additionally, this paper also identifies differences in the impact of information security education experiences on security behaviors by gender. We also investigate the difference in the effects of information security behaviors according to the type of information security education and gender.

H1: Users' information security experiences will have a positive impact on information security behaviors.

H1a: Among users who have online information security education, there will be a significant difference of information security behaviors depended by gender.

H1b: Among users who have offline information security education, there will be a significant difference of information security behaviors depended by gender.

H1c: Depending on the type of information security education (online vs offline), there will be a significant difference in the effect between educational experiences and information security behaviors.

H1d: Depending on gender, there will be a significant difference in the effect between educational experiences and information security behaviors.

3.2. Perceived Severity

The perceived severity of information security for an individual is the degree of their perceived fear of damages, including financial loss and invasion of privacy, that can occur as a result of his or her personal information being leaked (Johnston and Warkentin, 2010). The perceived severity of users improves their willingness to protect their PCs from external threats by taking security measures such as installing antivirus software (Lee and Larsen, 2009). Therefore, the perceived severity of information security for individuals is a major factor in complying with an organization's information security policies or increasing security behaviors in order to maintain a secure information security environment (Johnston et al., 2015; Woon et al., 2005). The severity of the penalties and sanctions that are imposed by individuals for noncompliance with information security policies reduces the intentions to exploit IS (D'Arcy et al., 2009).

The SETA (security, education, training, awareness) program, which collectively refers to a variety of education programs that provide general information security knowledge and develop the procedures and skills that are required to maintain a secure information environment, is reported to positively impact security cultures (Chen et al., 2015). However, depending on how information security education is conducted, the information security related knowledge or skills that individuals can acquire is different. The possibility of eliminating various external threats, which reduces the perceived severity, depends on the type of education that an individual completes. Therefore, this study assumes there will be statistically significant differences in the perceived severity of an individual depending on the type of information security education.

Female users perceive higher privacy concerns than males in both Internet contexts and non-Internet contexts (Fogel and Nehmad, 2009; Sheehan, 1999). Accordingly, the perceived severity of the loss of privacy in the online purchasing process was also higher in female users than in male users (Garbarino and Strahilevitz, 2004). Therefore, based on these previous studies, this study suggests the following hypotheses that the information security behavior that is caused by information security education experience will vary according to gender and its type.

H2: Users' information security education will have a positive impact on the perceived severity of information security.

H2a: Depending on the type of information security education (online vs offline), there will be a significant difference between educational experiences and the perceived severity of information security.

H2b: Depending on gender, there will be a significant difference between educational experiences and the perceived severity of information security.

3.3. Perceived Vulnerability

The perceived vulnerability to information security is the degree of awareness of the risks and possibilities of exposing personal information through illegal access and improper collection (Rogers, 1975). The potential for the loss or disclosure of personal in-

formation arises due to a variety of reasons, including insider negligence in the online environment, users' unwanted information leaks, and hacking (Dinev and Hart, 2004). Thus, how high a user evaluates the likelihood of such a risk makes the individual aware of the vulnerability of information security.

A previous study found that the perceived vulnerability to disease was higher in female patients than in male patients, with a statistically significant gender difference in the perceived vulnerability to disease (Duncan et al., 2009). Therefore, this study suggests the following hypothesis stating that there will be statistically significant differences in the effects of educational experiences on the perceived vulnerability of information security according to gender.

H3: Users' information security education experiences will have a positive impact on the perceived vulnerability of information security.

H3a: Depending on the type of information security education (online vs offline), there will be a significant difference between educational experiences and the perceived vulnerability of information security.

H3b: Depending on gender, there will be a significant difference between educational experiences and the perceived vulnerability of information security.

3.4. Self-efficacy

The self-efficacy of an individual with respect to information security has been studied as a representative criterion for determining or evaluating an individual's information security behavior (Bulgurcu et al., 2010; Hoque et al, 2015; Rhee et al., 2009; Siponen et al., 2014). Self-efficacy is the belief in a user's ability to execute the necessary behaviors (Stajkovic and Luthans, 1998). The user's self-efficacy is the confidence in the individual's ability to protect various data, including personal information, in the information security context (Chai et al., 2009; Johnston and Warkentin, 2010). As a result, an individual's belief in their ability to protect against unwanted information leaks or information disclosures without their personal consents can be explained as his or her self-efficacy (Rhee et al., 2009).

Many studies have been conducted to examine the effect of the self-efficacy of employees on intentions to comply with information security policies and information security behaviors in organizations or groups. In most studies, self-efficacy has a positive effect on employees' information security behaviors (Bulgurcu et al., 2010; Van Bavel et al., 2019). Nevertheless, depending on the complexity of the behavior, there may be a negative impact on information security behaviors (Bélanger et al., 2017).

Self-efficacy affects overall learning attitudes including motivations to participate in education and learning self-regulation (Schunk and DiBenedetto, 2016; Schunk and Usher, 2012). Students' self-efficacy in training programs and voluntary motivations to participate in them had a positive relationship (Zimmerman, 2000). This study assumes that the self-efficacy of individuals for information security will be affected by the user's information security education because computer self-efficacy is mainly affected by users' computer experiences of education (Beyer, 2014). Furthermore, as there is a difference in self-efficacy by gender for the same information system security (Beyer, 2014; Phelps, 2005), this study shows that there is a difference in self-efficacy according to information security education and gender. Therefore, we posit the following hypotheses.

H4: Users' information security education experiences will have a positive impact on the self-efficacy of information security.

H4a: Depending on the type of information security education (online vs offline), there will be a significant difference between educational experiences and the self-efficacy of information security.

H4b: Depending on gender, there will be a significant difference between educational experiences and the self-efficacy of information security.

3.5. Response-efficacy

The response-efficacy of a user to information security is his or her belief that he or she has the ability to prevent personal infringement incidents from external intrusions or to minimize the damage when an infringement occurs (Siponen et al., 2014). In other words, response-efficacy can be explained by an individual's assessment of how well the proposed countermeasures can reduce losses and control the situation, which is an evaluation of the threat countermeasures (Floyd et al., 2000). The effectiveness of a user's response-efficacy increases when he or she judges to have a more effective ability to control the threat than the level of the individual's perceived threat, such as information on the threat or how to prevent damage (Rogers, 1975). The higher the response-efficacy level that is perceived by an individual, the better the adoption of technology that enhances their privacy protection (Chenoweth et al., 2009; Crossler, 2010) and the higher their intentions are for continued use of such implements (Lee and Larsen, 2009). Therefore, this study hypothesizes that education experiences related to information security and privacy prevention methods will influence the response-efficacy, which is effective for perceived risk management. In addition, each hypothesis posits that the differences in response-efficacy according to educational experiences will differ by gender and the type of education.

H5: Users' information security education experiences will have a positive impact on the response-efficacy of information security.

H5a: Depending on the type of information security education (online vs offline), there will be a significant difference between educational experiences and the response-efficacy of information security.

H5b: Depending on gender, there will be a significant difference between educational experiences and the response-efficacy of information security.

Ⅳ. Research Methodology

4.1. Data Collection

This study used data collected by the leading Internet survey firm in Korea. The Internet survey firm electronically distributed the questionnaires to randomly selected Internet users. The company has approximately one million panels, and among them, those who fit the purpose of our research were used in the final analysis. A screening question was used to select those who have experienced information security educations. Based on the screening question, 648 respondents were selected among a total of 836 respondents participated in this survey, with ages ranging from 20 to above 60 years old. This online survey was performed in November 2018. Details of the respondents' demographic characteristics are presented in <Table 1>.

4.2. Data Analysis

We adopted the measurement scales from previous studies, and slightly modified them to reflect the purpose of this study. The items for perceived severity and perceived vulnerability were revised mainly based

<Table 1> Descriptive Statistics of Respondents

Construct	Items	Number (%)
Gender	Male	281 (43.4)
	Female	367 (56.6)
Age	20 ~ 29	124 (19.1)
	30 ~ 39	199 (30.7)
	40 ~ 49	210 (32.4)
	50 ~ 59	66 (10.2)
	Over 60	49 (7.6)
Education	Less than high school	164 (25.3)
	High school graduate	118 (18.2)
	Bachelor or diploma	314 (48.5)
	Postgraduate Degree	52 (8.0)
Daily hours spent	under 1 hour	74 (11.4)
	1 ~ 3 hours	106 (16.4)
	3 ~ 5 hours	176 (27.2)
	5 ~ 7 hours	121 (18.6)
	more than 7 hours	171 (26.4)
Total		648 (100)

on the items of Ifinedo (2012) and Bulgurcu et al. (2010), respectively. In addition, the measures for self-efficacy and response-efficacy were adopted from Compeau and Higgins (1995) and Ifinedo (2012). The items for all the constructs were measured on a seven-point Likert scale ranging from (1) strongly disagree to (7) strongly agree. In addition, questionnaires related to information security education methods ("How did you take the information security training?") were included throughout the questionnaire to compare the experience of online and offline information security educations courses among users.

Prior to the hypothesis test, confirmatory factor analysis was performed to verify the reliability and validity of the measurement items of the variables used in this study. Therefore, the measurement items were assessed through internal consistency reliability, convergent validity and, discriminant validity. First, to verify reliability, composite reliability (CR) and average variance extraction (AVE) were calculated. If the value of CR of the structural equation model is 0.7 or more, it is judged that there is no problem in reliability. The AVE of each construct is higher than 0.5, therefore, we can conclude that convergent validity was ensured (Fornell and Larcker, 1981). To access the internal consistency of our constructs, we examined Cronbach's *a*. The Cronbach's *a* and all factor loadings of all constructs are greater than 0.70, which is higher than the recommended minimum value of 0.70 (Chin, 1998). Therefore, all questionnaire items presented strong reliability and validity. <Tables 7> ~ <Tables 11> demonstrate that the square roots of each constructs' AVE is higher than the correlation with any other construct, and indicator loadings are higher than all of its cross loadings (Fornell and Larcker, 1981). Finally, we can conclude that all of the questionnaire items in this study have suitable construct discriminant validity.

<Table 2> Convergent Validity Testing Results

Construct	Std. loading of each item	AVE	CR	Cronbach's α
Perceived severity (PS)	0.79, 0.87, 0.75, 0.83	0.66	0.88	0.83
Perceived vulnerability (PV)	0.74, 0.71, 0.80, 0.86	0.61	0.86	0.81
Self-efficacy (SE)	0.78, 0.78, 0.84, 0.82	0.65	0.88	0.82
Response-efficacy (RE)	0.83, 0.85, 0.84, 0.84	0.71	0.91	0.86
Information security behavior (ISB)	0.79, 0.86, 0.78, 0.78	0.65	0.88	0.82

<Table 3> Convergent Validity Testing Results for Online Group

Construct	Std. loading of each item	AVE	CR	Cronbach's α
Perceived severity (PS)	0.79, 0.88, 0.70, 0.77	0.69	0.85	0.81
Perceived vulnerability (PV)	0.74, 0.75, 0.85, 0.88	0.60	0.81	0.75
Self-efficacy (SE)	0.70, 0.77, 0.84, 0.86	0.64	0.87	0.81
Response-efficacy (RE)	0.83, 0.86, 0.79, 0.83	0.68	0.90	0.85
Information security behavior (ISB)	0.75, 0.84, 0.83, 0.76	0.63	0.87	0.81

<Table 4> Convergent Validity Testing Results for Offline Group

Construct	Std. loading of each item	AVE	CR	Cronbach's α
Perceived severity (PS)	0.81, 0.94, 0.74, 0.79	0.67	0.89	0.86
Perceived vulnerability (PV)	0.79, 0.70, 0.93, 0.80	0.60	0.81	0.74
Self-efficacy (SE)	0.77, 0.79, 0.86, 0.82	0.66	0.88	0.83
Response-efficacy (RE)	0.84, 0.86, 0.87, 0.84	0.73	0.91	0.88
Information security behavior (ISB)	0.82, 0.80, 0.90, 0.74	0.67	0.89	0.83

<Table 5> Convergent Validity Testing Results for Males

Construct	Std. loading of each item	AVE	CR	Cronbach's α
Perceived severity (PS)	0.81, 0.87, 0.71, 0.81	0.64	0.87	0.83
Perceived vulnerability (PV)	0.72, 0.75, 0.94, 0.90	0.63	0.76	0.79
Self-efficacy (SE)	0.75, 0.80, 0.87, 0.82	0.66	0.88	0.83
Response-efficacy (RE)	0.82, 0.85, 0.82, 0.80	0.68	0.89	0.84
Information security behavior (ISB)	0.80, 0.79, 0.85, 0.75	0.64	0.87	0.81

<Table 6> Convergent Validity Testing Results for Females

Construct	Std. loading of each item	AVE	CR	Cronbach's α
Perceived severity (PS)	0.79, 0.94, 0.75, 0.76	0.63	0.87	0.83
Perceived vulnerability (PV)	0.79, 0.83, 0.92, 0.90	0.67	0.86	0.78
Self-efficacy (SE)	0.83, 0.86, 0.84, 0.85	0.64	0.87	0.81
Response-efficacy (RE)	0.85, 0.86, 0.84, 0.85	0.72	0.91	0.87
Information security behavior (ISB)	0.77, 0.84, 0.88, 0.75	0.66	0.89	0.83

<Table 7> Descriptive Statistics and Correlations between Latent Variables

	PS	PV	SE	RE	ISB
PS	***0.81***				
PV	0.53	***0.78***			
SE	0.07	0.12	***0.80***		
RE	-0.02	0.10	0.66	***0.84***	
IPB	0.24	0.28	0.63	0.57	***0.80***

Note: Leading diagonal shows the square root of AVE of each construct

<Table 8> Descriptive Statistics and Correlations Between Latent Variables for Online

	PS	PV	SE	RE	ISB
PS	***0.77***				
PV	0.59	***0.77***			
SE	0.07	0.08	***0.80***		
RE	0.01	0.01	0.68	***0.83***	
IPB	0.28	0.30	0.58	0.53	***0.80***

Note: Leading diagonal shows the square root of AVE of each construct

<Table 9> Descriptive Statistics and Correlations between Latent Variables for Offline Group

	PS	PV	SE	RE	ISB
PS	***0.82***				
PV	0.52	***0.78***			
SE	0.09	0.16	***0.81***		
RE	-0.02	0.02	0.59	***0.85***	
IPB	0.22	0.25	0.59	0.52	***0.82***

Note: Leading diagonal shows the square root of AVE of each construct

<Table 10> Descriptive Statistics and Correlations between Latent Variables for Males

	PS	PV	SE	RE	ISB
PS	***0.80***				
PV	0.31	***0.73***			
SE	0.05	0.11	***0.81***		
RE	0.01	0.07	0.59	***0.82***	
IPB	0.26	0.31	0.54	0.50	***0.80***

Note: Leading diagonal shows the square root of AVE of each construct

<Table 11> Descriptive Statistics and Correlations between Latent Variables for Females

	PS	PV	SE	RE	ISB
PS	***0.79***				
PV	0.46	***0.82***			
SE	0.11	0.14	***0.80***		
RE	-0.02	-0.02	0.28	***0.85***	
IPB	0.23	0.25	0.44	0.45	***0.81***

Note: Leading diagonal shows the square root of AVE of each construct

4.3. Hypothesis Tests

The hypothesis tests in this study are analyzed using the path coefficient of the PLS (Partial Least Squares) structure equation model. For all respondents with experience in information security education, we examined the effects of their information security educational experiences on their perceived severity, vulnerability, self-efficacy, and response-efficacy, respectively. The results showed that information security education experience increased the individual's perceived self-efficacy, response-efficacy, perceived severity and vulnerability, as well as information security behaviors, and the detailed results are presented in <Table 12>.

We performed independent sample t-tests for identifying the difference of users' information security behaviors between the gender and types of their experiences of information security education. The results showed that there was a significant statistical difference in information security behaviors according to the type of information security education and gender. Female users had a more tendency of conducting information security behaviors than males, among users those who took online information security education (H1a supported). Among the users who took offline information security education, on the contrary of the online education users, males showed higher information security behaviors than females (H1b supported).

Additionally, the significance of the difference between two groups was compared by using the path coefficient comparison formula that is shown in [Equation 1] (Chin, 1998) to find the differences in the influences of variables according to gender and the type of information security education.

$$t = \frac{path_{sample1} - path_{sample2}}{\sqrt{\frac{(m-1)}{(m+n-2)} \times SE^2_{sample1} + \frac{(n-1)}{(m+n-2)} \times SE^2_{sample2}} \times \sqrt{\frac{1}{m} + \frac{1}{n}}}$$

[Equation 1]

$path_{sample i}$: *subsample − specific path coefficients*

m, n: the sizes of the each subsample

SE: path coefficient standard errors as resulting from bootstrapping

t: t-distributed with m+n-2 degrees of freedom.

As shown in <Table 13> and <Table 14>, H1a (EDU → ISB), H4a (EDU → SE), H5a (EDU → RE), H1b (EDU → ISB), H2b (EDU → PS), H4b (EDU → SE), and H5b (EDU → RE) of the differences in the path coefficients were statistically significant at the 5% significance level.

Note the sign of the difference between the two path coefficients in the statistically significant group differences. As shown in <Table 13>, we can find out that online group the more conduct information security behaviors than the group of offline, when the difference of path coefficients among two groups toward information security behaviors show positive

<Table 12> Path Coefficients and Results of the Hypothesis Test

Hypotheses paths	β	*SE*	*T*-value	Remarks
EDU → ISB (H1)	0.37	0.03	10.94***	*supported*
EDU → PS (H2)	0.18	0.04	4.67***	*supported*
EDU → PV (H3)	0.15	0.04	4.06***	*supported*
EDU → SE (H4)	0.41	0.03	12.24***	*supported*
EDU → RE (H5)	0.38	0.03	11.15***	*supported*

values. Furthermore, among the personal information security education experiences, the online information security education experience group had higher self-efficacy and response-efficacy than the offline experience group. In addition, the information security behaviors according to the educational experi-

<Table 13> Independent Sample t-test for Gender and Type of Education

Hypotheses	Dependent Variable	males (n = 281)		females (n = 367)		t	Remarks
		Mean	*SD*	Mean	*SD*		
(H1a) online education (n = 339)	ISB	4.79	0.98	4.82	1.01	-.234*	Supported
(H1b) offline education (n = 309)		4.62	1.05	4.57	1.06	.341*	Supported

Note: *significant at 0.05

<Table 14> Multi-group Comparison Test Results (Online vs Offline)

(edu_style) hypotheses paths	items	offline (n = 309)	online (n = 339)	Path Coefficients-diff (online - offline)	Results
EDU → ISB (H1a)	Path Coefficients	0.39	0.31	0.81***	online > offline
	STDEV	0.05	0.05		
EDU → PS (H2a)	Path Coefficients	0.23	0.17	0.85	ns
	STDEV	0.05	0.04		
EDU → PV (H3a)	Path Coefficients	0.23	0.17	1.52	ns
	STDEV	0.05	0.05		
EDU → SE (H4a)	Path Coefficients	0.43	0.43	3.34***	online > offline
	STDEV	0.05	0.05		
EDU → RE (H5a)	Path Coefficients	0.38	0.38	1.89*	online > offline
	STDEV	0.05	0.05		

Note: *significant at 0.05, **significant at 0.01, ***significant at 0.001

<Table 15> Multi-group Comparison Test Results (Males vs Females)

(gender) hypotheses paths	items	males (n = 281)	females (n = 367)	Path Coefficients-diff (females - males)	Results
EDU → IPB (H1b)	Path Coefficients	0.39	0.19	5.05***	males < females
	STDEV	0.04	0.05		
EDU → PS (H2b)	Path Coefficients	0.31	0.10	5.77*	males < females
	STDEV	0.05	0.10		
EDU → PV (H3b)	Path Coefficients	0.24	0.10	3.84	ns
	STDEV	0.05	0.08		
EDU → SE (H4b)	Path Coefficients	0.42	0.23	6.05***	males < females
	STDEV	0.04	0.06		
EDU → RE (H5b)	Path Coefficients	0.42	0.12	8.91**	males < females
	STDEV	0.04	0.11		

Note: *significant at 0.05, **significant at 0.01, ***significant at 0.001

ence are also more prevalent in the online education group than those of the offline group, and it can be finally inferred that the effect of online education is relatively high. This finding is in contrast to the results of most previous studies that higher academic achievements were obtained by the offline education group than the online education group.

Gender resulted in significant differences in the group path coefficients for all variables except for the perceived vulnerability of individuals. The perceived severity, self-efficacy, and response-efficacy of the female users were all significantly higher than those of the male users. This result can confirm that information security education has a greater effect on the information security attitudes and behaviors of female users than male users. It is possible to confirm that the information security education effect is more prominent among females since the security behaviors from the information security education experience are greater in female users than in male users.

Ⅴ. Discussions

5.1. Conclusions

This study examined the effects of an individual's information security education on the individual's perceived severity, vulnerability, self-efficacy, and response-efficacy in the context of information security. The results suggested that the perceived severity, vulnerability, self-efficacy and response-efficacy of users all had significant impacts on information security behaviors. Furthermore, the increased information security behaviors from educational experiences were higher in the users who took online courses than the group who completed the offline information security education courses. This finding is different from a number of previous studies in which the completion of offline courses from educational institutions including schools and private institutions results in higher learning achievements than e-learning or online learning. The results of this study also suggest the need to focus on the characteristics of information security when information security education is designed.

5.2. Theoretical Implications

Except for the perceived vulnerability of users, it was confirmed that there were statistically significant differences in the path coefficients according to gender. This means that there are differences in the effectiveness of information security education by gender. So far, significant differences in the information security environment by gender have been only revealed in terms of the intentions to adopt information security technologies due to privacy concerns. Since female users are likely to be aware of the severity of information leaks than men, information security behaviors are also higher among female than male users (Fogel and Nehmad, 2009). Therefore, the results of this study also suggest that personal characteristics including gender should be incorporated when developing information security education. Until now, information security education has been systematically organized only based on the level of information security knowledge, but in the future, it is necessary to incorporate various personal characteristics of online users.

Most previous studies focused on enhancing information security behavior according to educational experiences. However, this study is different in that it discovers whether there is a difference in personal information protection behavior according to the

information security education method and gender. This result suggests that improving personal information security behavior, which is the effect of education, depends on the characteristics of the users.

E-learnings appeared in the early 2000s, when the Internet began to spread. Currently, its content quality and the provided services have improved compared to the past. However, the studies related to online education that have been actively conducted are limited to the time when online learning emerged, and there has been limited follow-up research. In other words, few studies have been conducted on improving online education outcomes or finding ways to advance online education compared to the past. This study draws on the field of information security education, which has experienced higher achievements from online education than offline education; and has highlighted the necessity of further research on the effects of online learning not only information security but also in various fields. This study also provides a foundation to the design and spread of blended learning for information security education, which combines the features of offline and online learning, by emphasizing the effects of online education.

5.3. Practical Implications

It is worth noting that the online education group showed better information security behaviors than the offline education group. This result can be inferred as follows. The number of users who want to take relevant education courses based voluntarily on the increased interest in information security and the need for data protection has increased, in the recent. This change in the social environment seems to have increased the number of online courses that are easily accessible to users, and educational achievements have been amplified by the completion of voluntary education. These results suggest that the effect of education amplifies, if the user voluntarily takes the education, even if it is not the offline education, which is mainly known as higher achievement.

Since most information security-related incidents, such as personal information infringements and data leaks, occur frequently online, it would be made a difference of achievements depended by which types of educations users adopt. In other words, the outcomes of training on how to prevent or overcome various information security incidents that frequently occur online may be maximized through online education, which is the same context as that in which the incident happened. Therefore, future information security education should have an aim to understand the exceptionally vulnerable online environment of information security incidents. Overall, it can be deduced that online education has a greater educational effect than offline as education is conducted in a similar environment where various information security incidents occur.

Finally, it is necessary to take full advantage of the effect of information security education by overcoming the following weaknesses that are associated with online compared to offline education. Many previous studies found that the main limitations of online education are students' low levels of concentration and weak motivations to voluntarily participate compared to offline approaches (Gelly and Silver, 2007). Therefore, online-information security education should seek to overcome the weaknesses of online lectures while also reflecting the characteristics of information security, such as the state-of-the-art online environment and the latest information intrusion technology.

There are still some limitations that should have been taken into account when conducting this study,

but which have not been addressed sufficiently. First, this study mainly identified the differences in the effects of information security education experiences by considering gender as an individual characteristic, but future studies will examine more diverse perspectives, including the cultural characteristics of individuals. Second, we divided the education method into offline and online education mainly based on the place where the education was conducted, but a future study will examine the differences in the education effect according to whether tuition is paid or not and whether the classes are required or not. Based on that we will consider additional factors of education methods and characteristics of individuals in a further research model for providing a deeper understanding of information security.

<References>

[1] Ahn, J., and McEachin, A. (2017). Student enrollment patterns and achievement in Ohio's online charter schools. *Educational Researcher, 46*(1), 44-57.

[2] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

[3] Arachchilage, N. A. G., Love, S., and Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197.

[4] Bandura, A. (2010). *Self-efficacy*. The Corsini Encyclopedia of Psychology, 1-3.

[5] Bélanger, F., Collignon, S., Enget, K., and Negangard, E. (2017). Determinants of early conformance with information security policies. *Information and Management, 54*(7), 887-901.

[6] Beyer, S. (2014). Why are women underrepresented in Computer Science? Gender differences in stereotypes, self-efficacy, values, and interests and predictors of future CS course-taking and grades. *Computer Science Education, 24*(2-3), 153-192.

[7] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

[8] Chai, S., and Kim, M. (2012). A road to retain cybersecurity professionals: An examination of career decisions among cybersecurity scholars. *Journal of the Korea Institute of Information Security & Cryptology, 22*(2), 295-316.

[9] Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., and Upadhyaya, S. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182.

[10] Chen, Y., Ramamurthy, K., and Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11-19.

[11] Chenoweth, T., Minch, R., and Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. Paper presented at *the 2009 42nd Hawaii International Conference on System Sciences*.

[12] Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research, 295*(2), 295-336.

[13] Chingos, M. M., and Schwerdt, G. (2014). Virtual schooling and student learning: Evidence from the Florida Virtual School. *Program on Education Policy and Governance Working Papers Series*, No.PEPG 14-02. Cambridge, MA: Harvard Kennedy School.

[14] Compeau, D. R., and Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

[15] Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. Paper presented at *the 2010 43rd Hawaii International Conference on System Sciences*.

[16] D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its

impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

[17] Dinev, T., and Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

[18] Dinev, T., and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

[19] Duncan, L. A., Schaller, M., and Park, J. H. (2009). Perceived vulnerability to disease: Development and validation of a 15-item self-report instrument. *Personality & Individual Differences, 47*(6), 541-546.

[20] Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

[21] Fogel, J., and Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160.

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

[23] Fortune (2019). At Google, a Rarity: Men Were Shorted by the Pay Gap, 2019.03.05. Retrieved from https://fortune.com/2019/03/04/google-gender-pay-gap-underpaying-men-wages/.

[24] Garbarino, E., and Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research, 57*(7), 768-775.

[25] Gelly, S., and Silver, D. (2007). Combining online and offline knowledge in UCT. Paper presented at *the Proceedings of the 24th International Conference on Machine Learning*.

[26] Gilbert, D., Lee-Kelley, L., and Barton, M. (2003). Technophobia, gender influences and consumer decision-making for technology-related products. *European Journal of Innovation Management, 6*(4), 253-263.

[27] Hazari, S., Hargrave, W., Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security, 4*(4), 3-20.

[28] Hoque, M. R., Ali, M. A., and Mahfuz, M. A. (2015). An empirical investigation on the adoption of e-Commerce in Bangladesh. *Asia Pacific Journal of Information Systems, 25*(1), 1-24.

[29] Hubalovsky, S., Hubalovska, M., and Musilek, M. (2019). Assessment of the influence of adaptive E-learning on learning effectiveness of primary school pupils. *Computers in Human Behavior, 92*, 691-705.

[30] Hwang, G. J., Wu, P. H., and Chen, C. C. (2012). An online game approach for improving students' learning performance in web-based problem-solving activities. *Computers & Education, 59*(4), 1246-1256.

[31] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

[32] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79.

[33] Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

[34] Johnston, A. C., Warkentin, M., and Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134.

[35] Kim, Y. K. (2017). Interaction effect of working in general information communication technology or computer security fields and permanent or temporary on wage, job and workplace satisfaction. *Asia Pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, 7(12)*, 91-100.

[36] Kirlappos, I., and Sasse, M. A. (2011). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy, 10*(2), 24-32.

[37] Le Compte, A., Elizondo, D., and Watson, T. (2015). A renewed approach to serious games for cyber security. Paper presented at *the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*.

[38] Lebek, B., Degirmenci, K., and Breitner, M. H. (2013). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. Proceedings of *the 19th Americas Conference on Information Systems, Association for Information Systems(AIS)*, 1-8.

[39] Lee, E., and Park, I. (2018). The Effect of Video Types on Learning Satisfaction and Academic Achievement in accordance with Visual Cue Presentation. *The Journal of Research in Education, 31*, 129-153.

[40] Lee, S. C., and Kim, J. A. (2018). Factors that affect student satisfaction with online courses. *Korean Journal of Educational Administration, 36*, 115-138.

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

[42] Liang, H., and Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

[43] Lim, S. H., Sung, J., Kim, D., and Kim, D. J. (2017). A study of consumers' perceived risk, privacy concern, information protection policy, and service satisfaction in the context of parcel delivery services. *Asia Pacific Journal of Information Systems, 27*(3), 156-175.

[44] Maddux, J. E., and Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

[45] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

[46] Miron, G., and Urschel, J. (2012). *Understanding and improving full-time virtual schools*. National Education Policy Center.

[47] Murphy, G. B., and Tocher, N. (2011). Gender differences in the effectiveness of online trust building information cues: An empirical examination. *The Journal of High Technology Management Research, 22*(1), 26-35.

[48] Park, J. K., Kim, B. S., and Cho, S. W. (2011). Primary factors affecting corporate employees' attitudes toward information security. *Korean Management Review, 40*(4), 955-985.

[49] Phelps, D. C. (2005). *Information system security: Self-efficacy and security effectiveness in Florida Libraries*. Doctoral Dissertation. Florida State University.

[50] Prentice-Dunn, S., Mcmath, B. F., and Cramer, R. (2009). Protection motivation theory and stages of change in sun protective behavior. *Journal of Health Psychology, 14*(2), 297-305.

[51] Puhakainen, P., and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757-778.

[52] QUARTZ (2016). The Amazon says there's no pay gap for women and minorities among its US workfor ce, Ashley Rodriguez, 2016.03.24. Retrieved from https://qz.com/646389/amazon-says-theres-no-pay-gap-for-women-and-minority-workers-among-its-us-workforce/.

[53] Rhee, H. S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

[54] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

[55] Salloum, S. A., Al-Emran, M., Shaalan, K., and Tarhini, A. (2019). Factors affecting the E-learning

acceptance: A case study from UAE. *Education & Information Technologies, 24*(1), 509-530.

[56] Schneier, B. (2000). *Semantic attacks: The third wave of network attacks*. Crypto-Gram Newsletter, October 2000.

[57] Schunk, D. H., and DiBenedetto, M. K. (2016). Self-efficacy theory in education. In K. R. Wentzel, and D. B. Miele (Eds.), *Handbook of motivation at school* (pp. 34-54). Rotledge.

[58] Schunk, D. H., and Usher, E. L. (2012). Social cognitive theory. In T. Urdan, K. R. Harris, and S. Graham (Eds.), *APA educational psychology handbook (Vol. 1)*. American Psychological Society.

[59] Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24-38.

[60] Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

[61] Son, M. J., Yoon, T. Y., and Lee, S. C. (2014). General quality research: Clinical information protection behavior in a medical institution: Based on health psychology theories. *Journal of the Korean Society for Quality Management, 42*(2), 153-163.

[62] Stajkovic, A. D., and Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin, 124*(2), 240-261.

[63] Suh, M. S., and Hee, K. S. (2002). The effect of consumer's emotion experienced during internet shopping according to gender. *Journal of Global Academy of Marketing Science, 9*(1), 101-128.

[64] Thirunarayanan, M., and Perez-Prado, A. (2001). Comparing web-based and classroom-based learning: A quantitative study. *Journal of Research on Technology in Education, 34*(2), 131-137.

[65] Van Bavel, R., Rodríguez-Priego, N., Vila, J., and Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39.

[66] Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

[67] Woon, I., Tan, G. W., and Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.

[68] Yu, J. G. (2013). A study of educational service quality in university: Focus on online/offline lectures. *Journal of Korea Service Management Society, 14*(3), 79-104.

[69] Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. *Contemporary Educational Psychology, 25*(1), 82-91.

◆ About the Authors ◆

Minjung Park

Minjung Park is a Ph.D. candidate in the School of Business at Ewha Womans University in Korea. She has a master's degree in Data Analytics from Ewha Womans University in Korea. Her research interests include information security, privacy and blockchain.

Sangmi Chai

Sangmi Chai is an associate professor in the School of Business at Ewha Womans University in Korea. Before joining Ewha Womans University, she was an assistant professor in College of Business, Information and Social Sciences, Slippery Rock University, PA, USA. She received her PhD in MIS from School of Management, State University of New York at Buffalo. She graduated from MBA in Seoul National University and received BS in the Ewha Womans University. Her research interests include information privacy and cybersecurity, blockchain, knowledge management, and IT investment.

Submitted: October 24, 2019; 1st Revision: December 23, 2019; 2nd Revision: February 27, 2020; Accepted: March 3, 2020