2018

Determinants of Personal Information Protection Activities in South Korea

Pilku Kang
University of Kentucky

Determinants of Personal Information Protection Activities in South Korea

Pilku Kang

PA 681

Advisor: Dr. Petrovsky

Table of contents

Executive Summary

The purpose of this paper is to investigate how people's awareness and ways to obtain relevant materials of personal information have influenced individual's information privacy protection activities. This study uses the data of a 2016 survey on information security published by Korea Information and Security Agency.

The dependent variables of this study are preventive measures for the security of a Personal Computer (PC) and preventive measures against personal information breach. I classify independent variables into four types. They are internet users' perception about information privacy, such as awareness of the importance of protecting one's personal information, and awareness of information privacy threats and their severity, channel of information collection and education, the experience of security incidents and personal information breach, and demographic factors. I use multiple regressions to estimate the effects of the independent variables.

The result of this study shows that the level of awareness of the importance of information privacy is positively correlated with information privacy protection activities. Also, it demonstrates that the more people think the information privacy threat is severe, the more they engage in information privacy protection activities. In addition, it shows that internet users who obtained relevant information from watching TV, reading the newspaper, or browsing internet are more likely to have engaged in information privacy protection activities. In order to encourage people to raise their information privacy protection activities, the South Korean government should consider factors identified in this study.

1. Introduction

The development of information and communication technologies, such as the Internet of Things, has triggered the emergence of a hyper-connected society in which people, the internet, and the physical world are all connected by a network (Choi, 2014; Dutta & Bilbao-Osorio, 2012). Such connectivity has expanded horizons and opened new doors in the digital age, especially by providing corporations with new business models and individuals with convenient services. However, as the reliance on the network has grown, so has the exposure to the risk of cyber-attack for both organizations and individuals increased. Data, such as personal information, is collected, analyzed, and used to activate these services. If such data is misused or accessed illegally by third parties, then it can be exploited for cybercriminal activities including hacking, identity theft, and spam. Cybercrime is not only costly but also increasingly common. Cybersecurity Ventures (2017) has estimated that the annual cost of damages caused by cybercrime worldwide will reach $6 trillion by 2021. At the same time, the leakage and the misuse of personal information can cause privacy breaches as well. In 2016, 84.2 percent of internet users in South Korea recognized the severity of personal information leakage and the infringement of privacy (KISA, 2017). Consequently, more than ever before, personal information protection has become a more critical element for sustainable economic growth.

To protect personal information online, the South Korean government has enacted legal and institutional measures for information protection in order to ensure the security of personal information systems and to minimize personal information collection. Through the amendment of related laws, the Korea Communications Commission (KCC), which is responsible for regulating personal information management of Internet Service Providers(ISPs), raised the level of sanction for ISPs that fail to adopt adequate technical or

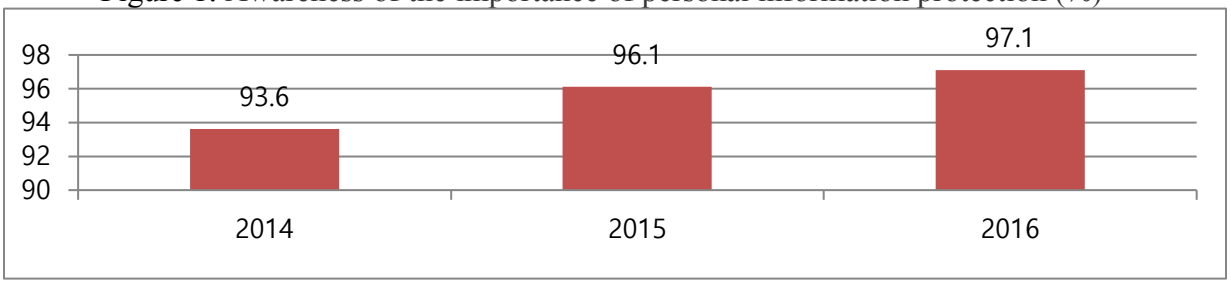
managerial measures in place to protect personal information (KCC, 2015). Also, to prevent the unnecessary storage of personal information by ISPs, if customers don't use the internet service for one year, ISPs are required to destroy their personal information or store it separately (KCC, 2016).

However, personal information cannot be protected solely by regulation of corporations. Hackers have targeted their attacks increasingly on personal computers (Gercke, 2012). For example, 86.87 percent of ransomware attacks in 2015 and 2016 aimed at home users (Kaspersky Lab, 2016). Also, human factors are significant elements to be addressed in information security (Parsons et al., 2010). First, by installing information security products, cyber-attacks can be prevented only to a limited extent. The development of information security technologies is slow compared to the rapid development of cyber-attack methods (KISA, 2010). It is also impossible to prevent personal information leakage and economic loss caused by social engineering attacks, such as phishing and pharming, by using information security products (KISA, 2010). Second, most infections of malicious code occur by visiting untrusted websites, clicking on URLs attached to emails, and downloading suspicious files. It is possible to avoid such infections by abstaining from such activities in advance. For example, according to South Korea's Ransomware Computer Emergency Response Team Coordination Center (2017), 70 percent of ransomware infections in 2016 occurred when internet users surfed the internet and clicked on the infected websites, and 25 percent of infections happened when internet users clicked on links in emails. Finally, violations of privacy can occur when internet users create or publish content, as well as post or share personal information, which includes their names, photos, and email addresses, on their social media. Therefore, it is critical for individuals to take precautionary measures to store and manage information securely on their own.

As part of the efforts to protect personal information, the KCC has implemented various policies to raise South Koreans' awareness of personal information protection, so that they can take preventive measures to protect their own information by themselves. It offered collective education for students by using a variety of educational tools, including presentation, leaflets, and videos (KCC, 2017). It also provided online platforms so that schools could independently operate educational courses addressing personal information protection (KCC, 2017). In addition, the KCC has also organized the annual "Guardian of My Information Protection Campaign," in which a TV celebrity advertises policies and strategies related to personal information protection in daily life on social media and mass media such as radio, outdoor advertisement boards, and major subway stations (www.i-privacy.kr).

In the meantime, the level of awareness related to personal information protection has increased significantly (Figure 1). Nevertheless, citizens' actual practices to protect their personal information remain limited. Research has indicated a gap between awareness of personal information protection and voluntary protective practices in South Korea (KISA, 2015). A 2014 Survey on Information Security pointed out that even though most internet users regard information protection as important, it is not sufficient to carry out personal information protection activities on their own (KISA, 2015). Therefore, I will empirically analyze how awareness of personal information protection affected activities for personal information protection. Furthermore, according to the 2013 Information Security Survey by KISA, 36.4 percent of internet users had obtained materials about information security and personal information protection; among them, most had accessed such information via the internet (45.6 percent), TV (29.6 percent), or newspapers (10.1 percent). Therefore, I will also examine the impacts of such media on increasing personal information protection activities.

< Figure 1: Awareness of the importance of personal information protection (%) >



< Source: 2016 Survey on Information Security(KISA) >

2. Literature Review

2.1. Definitions of personal information

Personal information, commonly referred to as personal data, is defined as information that can identify individuals. Its scope of definition differs across different countries (UNCTAD, 2016). The OECD Guidelines use personal data instead of personal information, and define it as "any information relating to an identified or identifiable individual."[1] In South Korea, personal information is defined as information that identifies a specific person with a name, a national identification number, or similar data in the form of code, letters, etc[2]. Even though one person cannot be identified by only a single piece of information, if the person can be identified by combining various pieces of information, it is regarded as personal information.

Personal information is often discussed along with the concept of privacy, leading to the creation of the concept of information privacy. Information privacy is defined as "the ability of the individual to personally control information about oneself" (Stone et al., 1983). While personal information is an object to be protected, information privacy implies active rights that can determine when, how and to what extent personal information is to be provided or used.

[1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
[2] Act on Promotion of Information and Communications Network Utilization and Information Protection. Art.2

2. 2 Personal information protection behaviors

The infringement of information privacy occurs in various forms in the life cycle of personal information. Solove (2006) categorizes information privacy infringements according to the information flow in four stages: (1) collection, (2) processing, (3) dissemination, and (4) invasion of information privacy. In order to cope with those infringements, personal information protection behaviors also have existed in various forms.

Researchers have used information privacy protection activities in accordance with their research purposes. For example, periodic password changes (Park, 2015), and the use of information security products such as antispyware (Chenoweth et al., 2009; Johnston & Warkentin, 2010) are listed as information privacy protection activities. In particular, the emergence of various internet services, such as social media and location-based services, confronted internet users with new forms of information privacy protection activities. For example, individuals should change their settings on social media platforms to better protect their profile and location information, control what photographs they upload, and what information they share. Therefore, such activities also have been viewed as personal information protection activities in many studies (Alqubaiti, 2016; Kamp, 2016).

2.3. Factors influencing personal information protection activities

Perceived importance of information privacy

Many studies have shown that attitudes and behaviors are influenced by the level to which people think a particular behavior or issues as important. Prior research has shown that the perceived importance of ethical issues has a significant impact on ethical judgment (Robin et al., 1996; Haines et al., 2008). Regarding information privacy, Chai et al. (2009) demonstrated that people who consider information privacy important tend to better protect personal information.

Education and training are essential elements in raising the awareness of particular behaviors. Coers et al. (2010) investigated undergraduate's group development process, and showed that its knowledge increased the perceived importance of group work skills. With regard to information security, Danuvasin et al. (2008) explained that training raises the users' security awareness. They stated that training allows users to recognize the level of threats and to provide ways to respond to security threats on their own.

Threat appraisal

R.W. Rogers proposed protection motivation theory in 1975 to explain fear appeal and its influence on the intention of behavioral change (Rogers, 1975). A core element of the theory is threat appraisal, which is an evaluation of the threatening events (Rogers, 1983; Kaspar, 2015). Threat appraisal consists of the perceived vulnerability (the likelihood that threatening events will occur), the perceived severity (the severity of threatening events) and the perceived benefits (rewards from doing risky behavior) (Rogers, 1983; Kaspar, 2015).

The majority of studies suggest that the perceived vulnerability and severity have a significant impact on changing intention and behavior of information privacy protection. Chenoweth et al. (2009) showed that perceived vulnerability and severity influence the undergraduate students' intention to utilize anti-spyware. Lee & Larsen (2009) found that the perceived vulnerability and severity affects the intention to adopt antimalware software in small and middle business. Adhikari & Panda (2018) found that perceived vulnerability and severity have a significant effect on enhancing users' privacy concerns, and ultimately change their activities. However, studies regarding perceived rewards showed different results. Youn (2009) showed that the perceived benefits offered by providing information decreased information privacy concerns. In contrast, Adhikari & Panda (2018) showed that rewards don't have a significant effect on users' information privacy concerns.

Self-efficacy

Self-efficacy is referred to as an "individual's beliefs about the ability to successfully carry out an action" (Youn, 2009). Different views exist on the effect of self-efficacy on personal information protection activities (Adhikari & Panda, 2018). Self-efficacy has been regarded as one of the most important factors that lead to individual behavior change (Maddux & Rogers, 1982; Compeau et al., 1999). However, Chenoweth et al (2009) showed that self-efficacy did not have a statistically significant effect on the intention to use the anti-spyware software as a protective technology. Also, Kamp (2016) reported that self-efficacy did not directly affect online privacy protection behavior, but affected the user's privacy concerns and social skills, and ultimately changed information protection behaviors.

Experience of learning and hearing about information privacy

Prior research has shown that changes in awareness, attitude, and behavior related to information privacy are possible with education and exposure to knowledge of information privacy. According to Chai et al. (2009), individuals who are exposed to materials on information privacy through school, parents, or media, increase their likelihood of practicing online information privacy behaviors. In particular, they demonstrated that external concerns from parents, teachers, and peers have a significant impact on increasing online information protection behaviors. Johnston & Warkentin (2010) showed that "social influence," such as guidance or surrounding people's opinion within the workplace, affects behavioral intentions of information protection activities. Kim (2010) has also shown that the more people received information from education, articles, campaigns, and advertisements, the more people actively participate in information privacy-related activities. Lee (2008), in a study of high school students' behavior, showed that the more information privacy related education students received, the more they will engage in information protection behaviors.

The National Institute of Standards and Technology (2003) classified components of learning about information security as a hierarchical structure of awareness presentation, training, and education. It explained that the purpose of awareness presentation is simply to raise attention on information security (NIST, 2003). Namely, it allows users to recognize the threats of information security so that they can cope with them accordingly. Based on such awareness and basic security knowledge, the training program will teach users, who are involved with the IT system, specific skills. Education is described as producing specialists and professionals with various security skills and competencies. Peltier (2005) stated that taking a short and simple message to users is the most important factor in raising awareness because most people are annoyed at the prospect of reading all the documents about information security. Also, the study emphasized that it is necessary to use video and other visual stimuli that are familiar to users in order to reinforce the message.

Experience of security incidents and personal information breach

Regarding individuals' experience with a security breach, prior research has shown different results. Christofides et al. (2012) demonstrated that the past negative experience with privacy breaches on social media was significantly correlated with knowledge of information privacy protection. They showed that people who had a negative experience on social media were more likely to know about and use the site's privacy settings for information disclosure. However, Chai et al. (2009) have conversely revealed that a past negative experience can negatively affect users' information protection behavior and self-efficacy. Namely, since students who experienced privacy breaches have low self-efficacy, and consequently reduce protection behaviors on the internet. As a result, they may be likely to experience a security breach again. Also, Cho (2007) reported that privacy breach and economic loss do not have a significant effect on information privacy protection behaviors.

Demographic characteristics

Prior research on information privacy has shown that gender, age, and education are correlated with information privacy protection behaviors. Dommeyer & Cross (2003) found that younger people and men are more likely to be aware of privacy-protection behaviors than older people and women. Also, Milne et al. (2004) added that those who have a higher level of education, males, and younger people are more likely to participate in information protection activities online actively.

3. Research Design

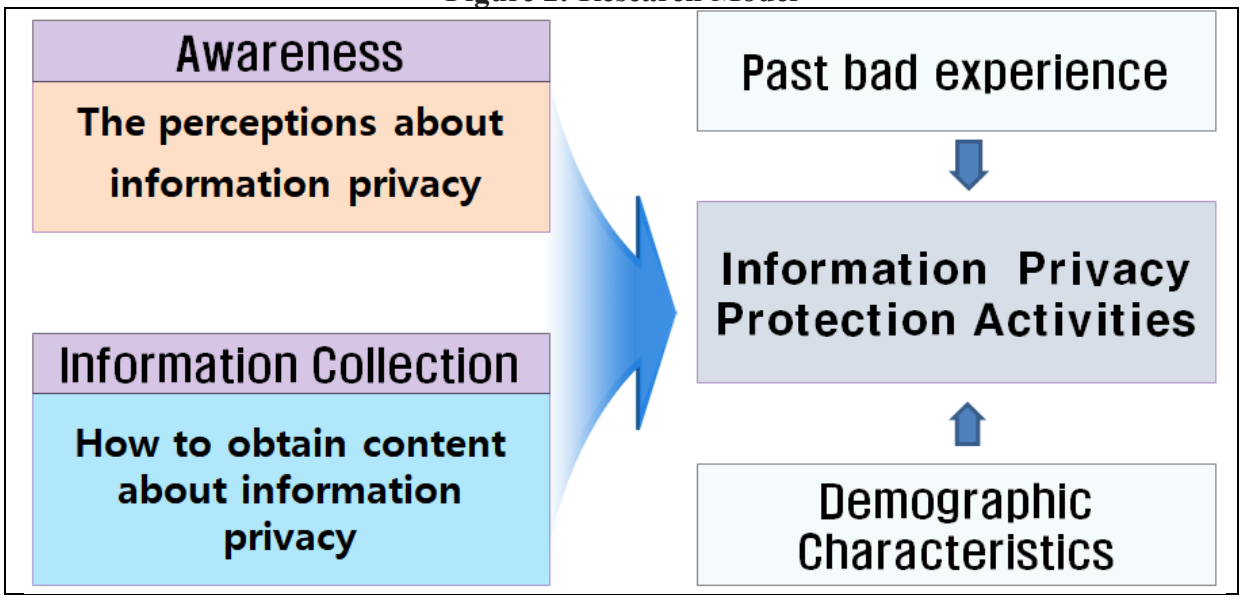
Research Question

The Korea Communications Commission has implemented policies to enhance South Koreans' awareness of protection of information privacy, so that internet users could voluntarily protect their personal information. Accordingly, I will empirically analyze how people's awareness of the importance of protecting one's personal information, and awareness of information privacy threats and their severity, have influenced individual's information privacy protection activities. In addition, according to the 2013 Information Security Survey published by KISA, 36.4 percent of internet users saw materials of policies or campaigns about information security and personal information protection, and the primary routes to obtain these materials were the internet (45.6 percent), TV (29.6 percent) or newspapers (10.1 percent). Therefore, I intend to investigate whether behaviors of personal information protection may be influenced by the media, such as the internet, TV and newspaper, and other forms of communication.

Research Model

Various factors may affect information privacy protection activities at individual level. They typically do not require a high level of information technology skills and knowledge. For example, there are simple and easy strategies that can be followed by anyone, such as not visiting unfamiliar websites, and not opening suspicious emails sent by unknown individuals or organizations. Therefore, I assume that personal information protection activities are mainly determined by internet users' perception about information privacy, such as their awareness of the importance of information privacy, and simple knowledge and information about strategies that should be used to protect one's personal information that can be acquired from media, internet, and other forms of communication. Also, I include past experiences of security incidents and personal information infringement because they have the potential to change perceptions and behaviors regarding personal information protection activities. Finally, I include demographic characteristics such as age, gender, and educational level as control variables. I use multiple regressions to estimate the effect of independent variables on the dependent variables. The detailed research model is shown in Figure 2.

< Figure 2: Research Model >



4. Data Description

4.1 Data sample

The data used in this study is collected from the "2016 Survey on Information Security" conducted by the Korea Internet & Security Agency (KISA). The survey investigated people's information security awareness, their activities related to personal information protection, and collected respondents' demographic characteristics such as gender, age, and education. In the year 2016, 4,000 Internet users aged between 12 and 59 years were surveyed among those who used the Internet for the last one month (KISA, 2017). The survey used multi-stage stratified sampling by region, gender, and age, and used face-to-face interviews by visiting selected households (KISA, 2017). The anonymized microdata is open to the public through the MicroData Integrated Service (MDIS) of the Korean Statistical Information Service (KOSIS).

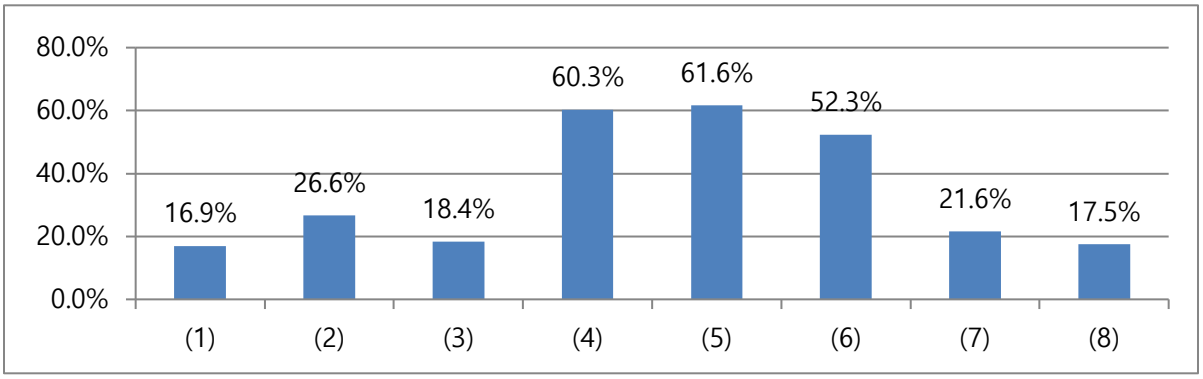
4.2 Dependent Variables

I classified the major information privacy protection activities into two categories. The first consists of preventive measures for the security of a PC. It is necessary to use information protection products to protect one's PC from viruses such as malicious code or external attacks. However, it is critical to prevent viruses and other infections in advance by using precautionary measures as mentioned before. Second, the secure management and monitoring of personal information are essential to avoid the personal information from being exposed and used for malicious purposes such as identity theft. Therefore, I also select measures designed to avoid infringement of personal information.

Preventive measures for the security of a PC

In the survey, there are eight activities to protect the information security of the PC and Network : (1) Security updates for applications (Adobe Flash, etc.); (2) Using encrypted USB thumb drives and others; (3) Designating an account for each user if multiple users use one PC; (4) Not opening attachments to suspicious e-mails; (5) Not accessing unknown websites; (6) Not downloading files from unknown websites; (7) Checking for unnecessary additional programs when installing applications; (8) Opting out of share settings for files and folders. Respondents are asked to select all activities in which they have engaged. Information protection activities and their prevalence are listed in Figure 3. Although each activity has a different degree of execution, I will assume that all activities have the same value because each action is indispensable to information security, so that I use the number of each behavior for information security as a dependent variable. The possible range of this variable is from 0 to 8.

< Figure 3: Preventive measures for the security of a PC, Multiple answers (%) >



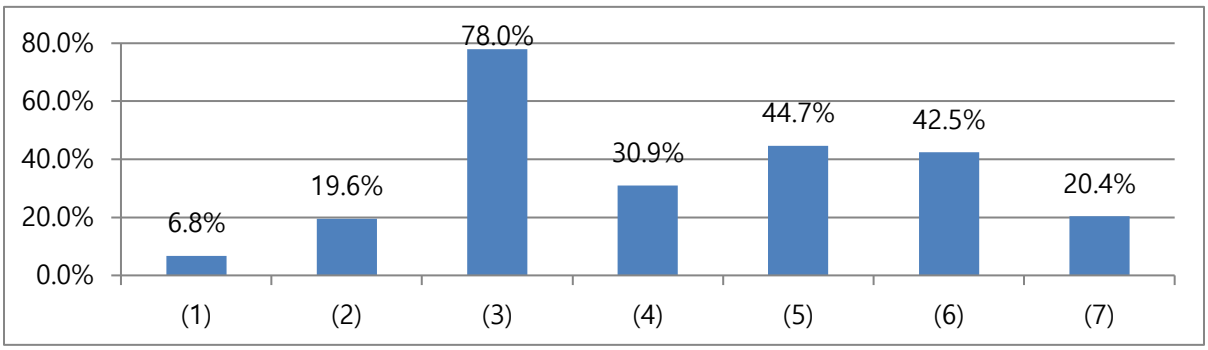
*weights are not applied.

Preventive measures against personal information breach

In the survey, there are seven preventive measures against personal information breach : (1) Check whether my personal information was used or not from time to time by using e-

clean service[3]; (2) Check if someone is using my personal information by using identity theft notification service; (3) Carefully manage personal information, not revealing it to others; (4) Be careful not to store your personal information in the shared folder; (5) carefully manage financial information not to be exposed in financial transactions; (6) Take caution in downloading suspicious material from internet; (7) Store a authentication certificate to personal portable storage only. Preventive measures for personal information protection and their prevalence are listed Figure 4. Although each activity has a different degree of execution, I will assume that all activities have the same value because each action is essential to avoid the personal information from being exposed and used for malicious purposes, so that I use the number of each personal information protection behavior as a dependent variable. The possible range of this variable is from 0 to 7.

< Figure 4: Preventive measures against personal information breach, Multiple answers (%) >



* weights are not applied.

4.3 Independent variable

The first major explanatory variable is the perception of the importance of information security and personal information protection because the more people who think that information privacy is important, the more they are willing to engage in information privacy protection activities (Chai et al., 2009). The variable is a Likert scale of perception with five

[3] E-clean service allows internet users to check history of authentication used to sign up for websites by using their information. Therefore, it is possible to check whether or not their personal information is stolen and used.

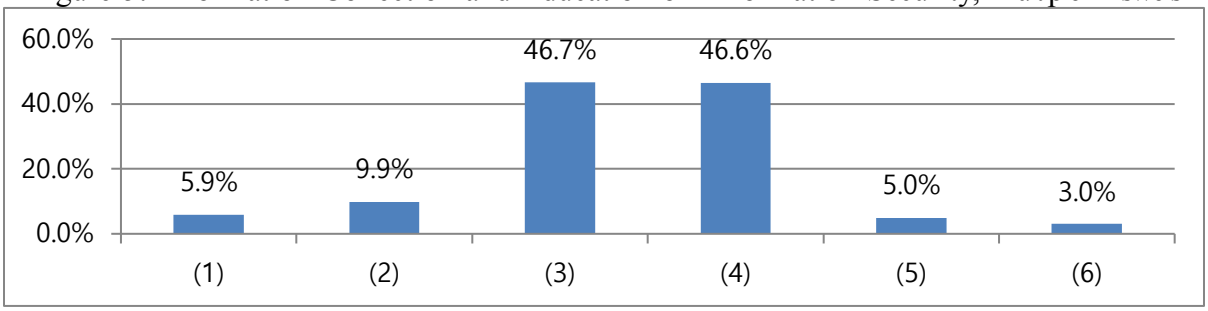
values (Not important =1 ~ important =4, very important =5). More than 95 percent of internet users said information security and personal information protection are important (important + very important) (KISA, 2017). In order to protect information privacy, protection of information system and protection of personal information should be combined. Therefore, I will assume the average value of two perceptions as perceived importance of information privacy (Chronbach's alpha=0.76).

The second set of explanatory variables covers awareness of information security threats and their severity. As mentioned in the literature review, the perceived severity of information privacy threat influences on personal information protection activities. These variables indicate the level of how well people know about the infringement of information security threats and their severity. The variables are a Likert scale of perception with five values (very low=1 ~ very high =5). In the survey, people are asked how well they know about the threats and severity of the five items: (1) Leakage of personal information and violation of privacy; (2) Damage from malware infection (virus, adware, spyware); (3) Financial damage from phishing, pharming and smishing; (4) Financial damages from credit or debit card fraud, or illegal payments; (5) Damages from ransomware infection. I will assume the average value of the response of above five items as the perceived threat (Chronbach's alpha=0.63) and their severity (Chronbach's alpha=0.81).

The third variable is the channel of information collection and education on information protection, because exposure to materials about information privacy through external environment increases awareness and knowledge on information privacy, and can lead to increase information privacy protection activities, as mentioned in literature review. It is reported that 65.6% of Internet users collect information and learn about information security (KISA, 2017). In this survey, there are six types of channels for acquiring information.

Respondents are asked to select all actions they are currently taking to collect information and learn about information security. Six types of channels are (1) Inquiries about information protection to public institutions; (2) Inquiries about information protection to private companies such as vaccine companies; (3) Information search through TV, newspaper, and internet (4) Information acquisition from acquaintances, friends, and colleagues; (5) Purchasing print materials such as books, educational SW and contents; (6) Taking classes such as internet lectures, seminars and academic conferences. I transformed the responses into dummy variables (yes = 1, No = 0) for each activity. The channels of information collection and education are shown in Figure 5.

< Figure 5: Information Collection and Education on Information Security, Multiple Answers >



*weights are not applied.

The fourth set of explanatory variables cover whether or not people experienced security incident and personal information breach in the previous year. In the case of security incidents, the total value for each type of accident was set as a variable. The types of accident are (1) damage from malicious code, (2) personal information theft and privacy violation, (3) Financial damages due to phishishing/pharming/smishing, (4) Financial damages due to credit card or debit card fraud, or illegal transactions, (5) damage from ransomware infection. The range of possible value of this variable is 0 to 5. However, in the case of a personal information breach, I consider whether the person experienced personal information breach or not. During 2015, 17.4 percent of users experienced security incidents, and 7.6 percent experienced personal information breaches (KISA, 2017).

Finally, I will include the demographic characteristic such as gender, age, and education level. Demographic characteristics are listed as shown in Table 1.

< Table 1: Demographic characteristics >

Categories	Scale
Gender	Female =0, Male=1
Age	12-19 =1, 20s=2, 30s=3, 40s=4, 50s=5
Education	No schooling=0, ~K6 =1, ~K9=2, K12=3, College~ =4

The descriptive statistics of the dependent and independent variables mentioned above are shown in Table 2.

< Table 2: Descriptive statistic >

VARIABLES	N	mean	sd	min	max
Dependent variables					
Preventive measures for a PC security	4,000	2.751	1.211	0	8
Preventive measures against information breach	4,000	2.429	1.324	0	7
Awareness					
Perceived importance	4,000	4.516	0.528	2	5
Perceived threat	4,000	4.019	0.536	1	5
Perceived severity	4,000	4.172	0.621	1	5
Channel of information collections					
Inquires to public institutes	4,000	0.059	0.235	0	1
Inquiries to private companies	4,000	0.099	0.298	0	1
Information search through TV or internet	4,000	0.467	0.499	0	1
Acquisition from friends, acquaintance	4,000	0.466	0.499	0	1
Purchasing printed materials	4,000	0.050	0.217	0	1
Taking classes	4,000	0.030	0.171	0	1
Past bad experience					
Experience of security incidents	4,000	0.235	0.631	0	5
Experience of personal information breach	4,000	0.068	0.251	0	1
Demographic characteristics					
Age	4,000	3.094	1.380	1	5
Gender	4,000	0.511	0.500	0	1
Education	4,000	3.476	0.632	0	4

5. Analysis and Findings

Preventive measures for the security of a PC

Most importantly, regression results (Table 4) show that the more people think information privacy is important, the more activities they engage in to protect the security of a PC (Coefficient=0.187, p-value <0.01). Also, the more people think the information privacy

threat is severe, the more activities they engage in to keep a PC secure (Coefficient=0.0822, p-value < 0.05). Additionally, the degree of awareness of the threat increases PC security activities (Coefficient=0.305, p-value <0.01). Second, this study shows that internet users who inquired to the private companies (Coefficient=0.365, p-value<0.01) or conducted an information search through TV, newspaper, or internet (Coefficient=0.106, p-value<0.01) increased their activities for the security of a PC. Third, the experience of security incidents is negatively related to preventive activities for a PC safety (Coefficient=-0.135, p-value<0.01). This result may be caused by reverse causality. In other words, those who have taken fewer actions for the security of a PC may experience security incidents, and vice versa. Also, this is because the security incidents were minor and were not expected to have a significant effect on changing their perceptions and behaviors. Finally, activities for information privacy protection are affected by demographic characteristics. Younger people, those with higher education level, and men are more likely to be engaged in protecting their PC.

Preventive measures against personal information breach

To begin with, regression results (Table 4) show that the more people think information privacy is important, the more activities they engage to prevent personal information infringement (Coefficient=0.195, p-value <0.01). Also, the more people think the information privacy threat is severe, the more they engage in preventing personal information infringement (Coefficient=0.384, p-value <0.01). However, the degree of awareness of the threat does not show a statistically significant relationship with activities for preventing personal information infringement. Second, this study shows that internet users who inquired to a private company (Coefficient=0.339, p-value <0.01) or conducted an information search through TV, newspaper, or internet (Coefficient=0.326, p-value <0.01) or collected information from acquaintances, friends, or colleagues (Coefficient=0.315, p-value <0.01)

increased their use of preventive measures to prevent personal information infringement. Third, the experience of a personal information breach increases preventive measures to avoid personal information infringement (Coefficient=0.205, p-value <0.05). Finally, younger people, those with higher education level, and men engage in greater activities for protecting personal information.

< Table 4: Regression results >

VARIABLES	Preventive measures for a PC security	Preventive measures against personal information breach
Awareness		
Perceived importance	0.187***	0.195***
	(0.0343)	(0.0383)
Perceived threat	0.305***	-0.0769
	(0.0469)	(0.0531)
Perceived severity	0.0822**	0.384***
	(0.0398)	(0.0419)
Channel of information collections		
Inquires to public institutes	0.137	0.0736
	(0.0864)	(0.0938)
Inquiries to private companies	0.365***	0.330***
	(0.0734)	(0.0679)
Information search through TV or internet	0.106***	0.326***
	(0.0386)	(0.0398)
Acquisition from friends, acquaintance	0.0373	0.315***
	(0.0382)	(0.0394)
Purchasing printed materials	0.00233	-0.0103
	(0.0876)	(0.0893)
Taking classes	0.240*	0.228*
	(0.141)	(0.121)
Past experience		
Experience of security incidents	-0.135***	-0.0217
	(0.0311)	(0.0309)
Experience of personal information breach	0.176*	0.205**
	(0.100)	(0.0940)
Demographic characteristics		
Age	-0.0678***	-0.0312**
	(0.0130)	(0.0137)
Gender	0.139***	0.0774**
	(0.0367)	(0.0388)
education	0.256***	0.412***
	(0.0287)	(0.0306)
Constant	-0.511***	-1.472***
	(0.215)	(0.223)
Observations	4,000	4,000
R-squared	0.105	0.163

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

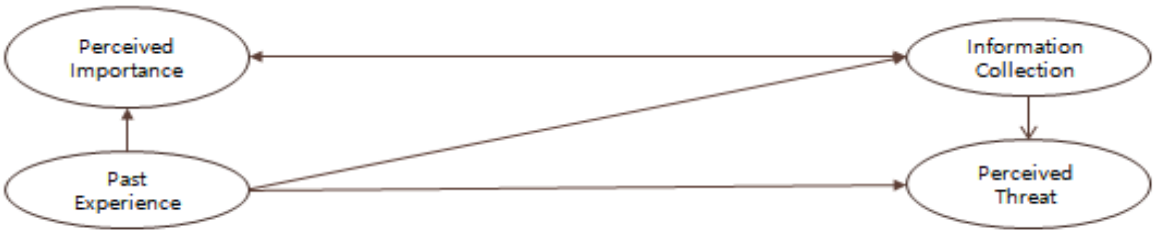
6. Limitations

This study is a cross-sectional analysis using one year's (2016) survey data, which may lead to omitted variable bias. This study did not consider the capacity of internet users to use the internet, such as the ability to use computers, as one of factors in personal information protection activities. As mentioned in the literature review, internet users with more knowledge and self-efficacy have engaged in more personal information protection activities. If internet users feel it is difficult to use the computer or lacks overall knowledge of computer software, there is a possibility to affect personal information protection activities adversely. Also, this study did not consider the type of activities that internet users perform online. Personal information protection behaviors may be different depending on the type of internet usage such as financial transaction, entertainment, or news and information search. In addition, this study did not consider the costs and benefits of doing personal information activities. This aspect should also be taken into consideration because opportunity costs such as time and money arise to protect personal information. Furthermore, this study can cause bias because it considers only whether internet users collect and learn from various routes or not. The amount of time and efforts spent in collecting information and learning can be an important determinant of information security activities.

Moreover, I considered only the direct effect of independent variables on dependent variables. However, the key independent variables are influenced by each other. For example, the more people think personal information protection is important, the more they will obtain information through internet and media, and vice versa (Figure 7). Also, the more information users obtain about information about the severity of personal information infringements, the more likely they will feel that threat of such infringement is serious. In addition, those who have experienced an infringement on personal information may have a higher tendency to

think that personal information protection is important, and that the threat from breach of personal information is serious, and may collect more information.

< Figure 7: Possible relationships between independent variables >



7. Policy implications

In this study, I have found that awareness of the importance of information privacy protection increases activities for information privacy protection. Raising awareness of the importance of information privacy is possible through learning such as training and education programs, as mentioned in the literature review. Therefore, the government should increase opportunities for people to experience such programs on information privacy. Also, information privacy protection activities are influenced by the awareness of the severity of the threat. Therefore, material, which addresses the severity of consequences that may result from not doing personal information protection activities, as well as the content about information privacy threats should also be provided.

In addition, this study shows that those who searched for information through the internet, TV, or newspapers are more likely to be engaged in information privacy protection activities. Therefore, it is necessary to use such media to make available as much information as possible about personal information protection, so that internet users can recognize its significance. Also, the government should look for ways to improve access to material dealing with information privacy on such media. For example, the government can cooperate

with internet portal sites to make it easier to search for information about information privacy and to expose relevant information to internet users as much as possible. Furthermore, internet users who have collected information from acquaintances, friends or colleagues tend to engage in more activities to prevent personal information infringement. This result suggests that personal information protection activities are affected when people are exposed to information that people in their environment have provided. Therefore, it is vital to create a culture of considering information privacy protection as important to strengthen the practice of personal information protection activities. In particular, as mentioned in the literature review, an effective way to raise awareness is to convey related content through simple and easy messages. According to the Korea Internet & Security Agency (KISA) in 2016, 33.2 percent of internet users said that information privacy-related terms are difficult to understand, and 31 percent of internet users think that such content is complicated and the knowledge is too vast to comprehend. Therefore, the government needs to make an effort to improve the understanding of the general public by simplifying, and easily explaining the content of policies. In particular, 20.1 percent of internet users feel that there is little material that is required for personal information protection. Therefore, it is necessary to develop customized content according to individual users' characteristics.

Finally, older people are less likely to perform activities for the protection of information privacy. Therefore, it is necessary to find ways to increase opportunities of education and training programs for older people.

Reference

Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Global Marketing, 1-15.

Alqubaiti, Z. Y. (2016). The Paradox of Social Media Security: A Study of IT Students' Perceptions versus Behavior on Using Facebook.

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

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on (pp. 1-10). IEEE.

Cho Jae sung (2007). Research for personal response against the experience and the concern of the disclosure of personal information and the invasion of privacy.

Choi, A. J. (2014, November). Internet of things: Evolution towards a hyper-connected society. In Solid-State Circuits Conference (A-SSCC), 2014 IEEE Asian (pp. 5-8). IEEE.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. Journal of adolescent research, 27(6), 714-731.

Coers, M., Williams, J., & Duncan, D. (2010). Impact of group development knowledge on students' perceived importance and confidence of group work skills. Journal of Leadership Education, 9, 101-121.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. MIS quarterly, 145-158.

Cybersecurity Ventures (2017). 2017 Cybercrime Report : Cybercrime damages will cost the world $6 trillion annually by 2021.

Danuvasin C., Murali R. and Lorne O. Improving End User Behaviour in Password Utilization: An Action Research Initiative. Systemic Practice and Action Research, Vol. 21, No. 1, pp. 55–72, 2008

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. Journal of Interactive Marketing, 17(2), 34-51.

Dutta, S., & Bilbao-Osorio, B. (2012). The Global information technology report 2012: Living in a hyperconnected world. World Economic Forum.

Gercke, M. (2012). Understanding Cybercrimes: Phenomena, Challenges and Legal Response. International Telecommunication Union.

Haines, R., Street, M. D., & Haines, D. (2008). The influence of perceived importance of an ethical issue on moral judgment, moral obligation, and moral intent. Journal of Business Ethics, 81(2), 387-399.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566.

Kamp, M. H. (2016). Determinants of privacy protection behavior on social network sites: the role of privacy beliefs, social norms and internet skills (Master's thesis, University of Twente).

Kaspar, K. (2015). An embodiment perspective on protection motivation theory: the impact of incidental weight sensations on threat-appraisal, coping-appraisal, and protection motivation. Studia Psychologica, 57(4), 301

Kaspersky Lab (June 2016). KSN REPORT: RANSOMWARE IN 2014-2016.

Kim Jihye (2010). An analysis of the consumer privacy protection behavior in online based on protection motivation theory.

Korea Internet and Security Agency (2010). The study on the public promotion related to the information security.

Korea internet and Security Agency (2014). 2013 Survey on Information Security (individual).

Korea Internet and Security Agency (2015). 2014 Survey on Information Security (individual),

Korea Internet and Security Agency (2017). 2016 Survey on Information Security (individual).

Korea Communications Commission (2016). 2015 Korea Communications commission annual reports.

Korea Communications Commission (2017). 2016 Korea Communications commission annual reports.

Lee, Y., & 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.

Lee Yoonsun (2008). A Study on Factors Influencing the Preventive Efforts toward Personal Information Privacy.

Maddux, J. E., & 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.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217-232.

NIST. Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, edited by Wilson M.: 2003. National Institute of Standards and Technology.

Org. for Econ. Co-operation & Dev.,. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Park Geon-U (2015). A Study on the Determinants of the Internet Privacy Protection Behavior: Focused on the Net Users' Characteristics.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment (No. DSTO-TR-2484).

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. Information Systems Security, 14(2), 37-49.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology: A sourcebook, 153-176.

Robin, D. P., Reidenbach, R. E., & Forrest, P. J. (1996). The perceived importance of an ethical issue as an influence on the ethical decision-making of ad managers. Journal of Business Research, 35(1), 17-28.

Solove, D. J. (2005). A taxonomy of privacy. U. Pa. L. Rev., 154, 477.

South Korea's Ransomware Computer Emergency Response Team Coordination Center (2017). 2017 Ramsomware Infringement Analysis Report. Retrived from http://img.innotium.com/newsletter/rans_201702/rancert_analysis_report_1702.pdf

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of applied psychology, 68(3), 459.

United Nations Conference on Trade And Development (2016). Data protection regulations and international data flows: Implications for trade and development.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special publication, 800(50), 1-39.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer affairs, 43(3), 389-418.