J. Korea Saf. Manag. Sci. Vol. 23 No. 2 June 2021
http://dx.doi.org/10.12812/ksms.2021.23.2.053
ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

ICT Adoption and Cyber Security of Korean SMEs

Jeyong Jung*
*Department of Police Science, University of Ulsan

중소기업의 ICT 도입과 사이버 안전에 관한 연구

정 제 용*
*울산대학교 경찰학과

Abstract

Small and medium-sized enterprises(SMEs) continue to adopt ICT to gain an edge in organizational innovation and competition. This has a management advantage, but it also brings vulnerabilities as to cyber security. Therefore, the purpose of this study is to conduct an exploratory study on the cyber security situation of SMEs. A survey was conducted on Korean SMEs to determine how well they are connected to ICT and how much they are exposed to cyber security threats. The results suggest two things. First, Korean SMEs are well connected to ICT, but there is a gap between the actual adoption and human recognition of its importance. Second, security threats and breaches affect the majority of SMEs, but several problems including costs have not been properly evaluated. The results of this study are expected to help improve the cyber security management system of Korean SMEs.
Keywords : Cyber security, SMEs, ICT adoption, Threats and breaches, Survey

1. Introduction

It was estimated that 3.2 billion people around the world and more than 80% of people in developed nations were using the Internet by the end of 2015[1]. In particular, mobile-broadband penetration rates were expected to reach 47% in 2015, about four times as high as they were 5 years previously[2]. This growth of Internet and wireless communication has changed the behaviour of end users in terms of how people interact with one another and engage in social activities. South Korea has highly innovative ICT infrastructures and people in both countries have relatively advanced computer skills and knowledge compared to those in other countries[2, 3].

Not only individuals, but also organisations, have had to adapt to a new environment dependent on internet-based communication networks. In order to maximize profits and reduce costs, companies of all sizes have attempted to take advantage of ICTs. As an increasing number of people use social networking services as a venue for communication and information sharing, the massive spread of virtual social interactions creates an opportunity for businesses to open up new markets. Additionally, ICTs help businesses manage themselves in a variety of ways, such as improving performance, sharing business information, and reducing costs. In this sense, ICTs have become increasingly essential in business operations on a daily basis[4]. The adoption of ICTs is now one of the crucial prerequisites for increasing competitive edge in business[5].

The rise of cloud computing, Internet of Things, and social media platforms has contributed to a very great increase in data sets. Using Big Data analytics, companies carry out data-driven decisions rather than intuition-driven ones. The technological revolution has changed business communication and management.

† This paper was rewritten based on part of Chapter 5(Quantitative Findings) of the author's unpublished PhD thesis.
† Corresponding Author : Jeyong Jung, Department of Police Science, University of Ulsan, 93, Daehak-ro, Nam-gu, Ulsan, E-mail: pancon@ulsan.ac.kr
Received April 13, 2021; Revision June 14, 2021; Accepted June 22, 2021

However, there is a problem. The Internet - as the core part of ICT – acts as a playground for cyber criminals[6]. The South Korean Police has reported that cybercrimes have significantly increased by about 31% from 116,961 in 2011 to 153,075 in 2016[7, 8]. In a similar vein, in the UK, the number of cybercrime offences and online fraud cases were estimated to be about, respectively, 2 million and 3.6 million in the 12 months[9]. The rapid growth of ICTs has provided grounds which generated new types of risks and threats. As far as businesses are concerned, an increasing reliance upon those devices has exposed SMEs(Small and Medium-sized Enterprises) to various cyber security threats. This has given rise to cyber security breaches (e.g., hacking, theft of business or customer information, and system disruption) which have caused major economic and social losses to companies, at least temporarily.

This research is aims to explore cyber security risks and threats of SMEs. Using a survey method, this study intends to examine quantitative findings and delivers an assessment of SMEs' current situation by using descriptive statistics, chi-square tests and *t*-tests.

2. Literature Review

Some studies[10, 11] attempted to identify organisational factors which contribute to the vulnerability of SMEs in relation to cyber security. Firstly, the size of an organisation is associated with various aspects of cyber security. In most cases, the number of employees and the volume of assets increase proportionately. When it comes to cyber security, a large company is more likely to use risk assessment tools[12] or to accept cyber security management by depending on its resources such as IT specialists and budgets. On the contrary, small companies do not have such resources to address the threats[11, 12]. This makes small companies unequipped and unprepared. [10] asserted that there was a significant difference in countermeasures between large companies and small ones. For example, in the case of cloud computing, a large company is capable of managing cloud-related risks with the support of sophisticated risk management and experienced IT teams[13]. Some small owners who are aware of these risks are hesitant to adopt cloud computing in spite of its potential benefits due to privacy, security, and data integrity reasons.

Secondly, decision-making dynamics in small companies are highly leveraged by the owners[14, 15]. Large companies have a hierarchical structure with several layers of management to manage resources efficiently[16]. Their decision-making is undertaken through functional departments (e.g., marketing, finance, accounting, human resource, and IT). Though top-level strategic decisions are conducted by a CEO or board members, most of the functional and operational decisions derive from managers. Therefore, decision-making is carried out via known, formal, and hierarchical channels. However, small companies have a relatively flat organisational structure with an absence of bureaucracy. Their management structure is not formalised and changeable based on organisational and external influences. This structure may bring in more flexibility, but the downside is that this can produce overly reactive and short-term decisions[17]. In fact, SMEs' decision-making mechanisms are dominated by few decision-makers[16]. Decision-making mechanisms are centralised and dependent upon the owners[14]. In this case, knowledge and attitude of the owners and senior managers are greatly important factors to produce effective decisions.

However, SME owners and managers had an insufficient understanding of the security risks and were not aware of possible measures to mitigate the risks[18]. The owners therefore were not capable of undertaking an intensive evaluation of cyber security decisions. This can pose a serious challenge against SMEs in that professional competencies are not available to them. [15] stated that when it comes to risks, small owners were more concerned about financial risks or profits, and that risk assessment itself was subjective because of the strong influence of ownership over management. He also asserted that the framing of risks was not research-based or data-driven, but based on the owner's experience

ISSN 1229 - 6783(Print)
ISSN 2288 - 1484(Online)

and knowledge derived from informal networks. In addition, preoccupation with daily issues made owners demonstrate a lack of concern towards security issues[19]. These justify why business owners need to be educated on cyber security risks.

For businesses, cybercrime is a potential source of security risk that could have a disruptive impact. Cybercrime can be a reliable proxy measure of cyber security threats although cybercrime rates cannot represent all potential risks. The UK government has announced its first esimation of the scale of cybercrime in 2015. In 2016, the survey reported that the volume of online fraud and cybercrime cases were about 3.6 million and 2 million, respectively[9]. It was noted that traditional crimes were on the decline. All these figures represented that online crimes occurred on the similar magnitude with offline crimes (5.6 million versus 6.2 million cases). It highlighted that cyber fraud were more serious than expected. Common types of cyber fraud were bank and credit account/card fraud, theft of personal information on bank accounts, misuse of credit card details, along with online shopping scams.

According to the Cyber Security Breaches Survey[20] , nearly 47% of small businesses and 64% of medium businesses in the UK suffered a security breach in the past 12 months. The survey also suggested a large discrepancy in breach cost by business size. The average breach cost estimates were higher among medium and large businesses compared to small businesses. Across all breaches, micro/small businesses' mean cost was estimated to be 894 pounds, while medium businesses' mean cost was calculated as 8,180 pounds. These UK survey results indicate that SMEs were targeted by cybercriminals and that the damage was serious enough to merit further attention. A security breach could cause problems including minor inconvenience, reputational damage, loss of customer data, fines, and, in the worst case, company closure. Damage from a breach may have more serious consequences on SMEs than large corporations because SMEs generally have no emergency recovery plans and capacity to mitigate the damage.

3. Research method

This study is built on the survey of IT managers and owners in SMEs. Using convenience sampling method, emails which contained research introduction and the survey link were sent to 5,028 SMEs in nine administrative areas. A total of 352 SMEs returned the questionnaires online for a response rate of 7%. The survey data were collected for about two months from 28 October 2016. Although 352 samples were collected, 24 samples were discarded because of the poor quality of responses.

The number of missing responses was very small: five (1.5%) in the question on business sector and two (0.6%) in the question on business size. There was much variation among business sectors. Only 0.9% of SMEs were in the transportation and storage or the real estate sectors but as many as 38.1% in the manufacturing sector. In this chapter we reduce this variation by also grouping businesses according to the orientation of their services: (1) services largely directed at the public, (2) services largely directed at organisations, (3) public services and (4) manufacturing and construction.

In terms of business size, 40 more samples of small businesses (184 cases) were collected than medium businesses (142 cases). However, the proportion gap between small businesses (56.1%) and medium businesses (43.3%) is not disproportionately large. <Table 1> presents the types of groupings within the sample.

<Table 1> Sample profiles by business sector categories and business size

	Small firms	Medium firms	Missing	Total	Percentage
Services largely directed at public	42	16	1	59	18.0%
Services largely directed at organisations	39	27	0	66	20.1%
Public services	27	22	0	49	14.9%
Manufacturing and construction	73	75	1	149	45.4%
Missing	3	2	0	5	1.5%
Total	184	142	2	328	100%
Percentage	56.1%	43.3%	0.6%	100%	

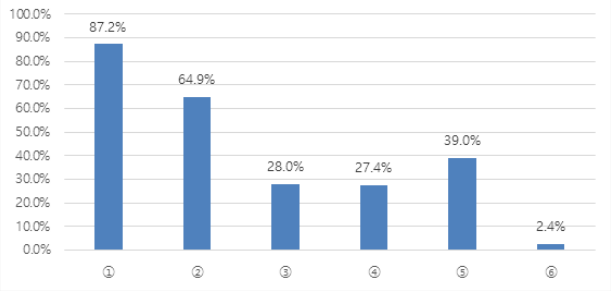
4. Results and analysis

In the survey, questions were categorised into two groups which represent differing themes. Overall, these categories are intended to explore the current cyber security context in which SMEs operate their business. The objective of the survey is to have an awareness of cyber secuirty arrangements surrounding SMEs because there is an obvious lack of situational assessment on SMEs in South Korea. These are the two categories: (1) business connectedness to ICTs and their significance and (2) incidence and impact of cyber security breaches.

4.1 Business connectedness to ICTs and their significance

The vast majority of Korean SMEs adopted online services in some form [Figure 1]. 'Email addresses for organisation or employees' (87.2%) was identified as the most prevalent online service, followed by 'a website or blog' (64.9%) and 'online business bank account' (39.0%). There was a noticeable distinction in the use of online services. Most businesses used online services for communications (i.e., email addresses) and advertising (i.e., website or blog and accounts on social media sites) purposes. By contrast, online services for business transactions (i.e., ordering or booking by customers) and financial transactions (i.e., bank accounts) were used by around a third of businesses (respectively, 27.4% and 39.0%).

1. Which of the following, if any, does your company currently have or use? (multiple choice)



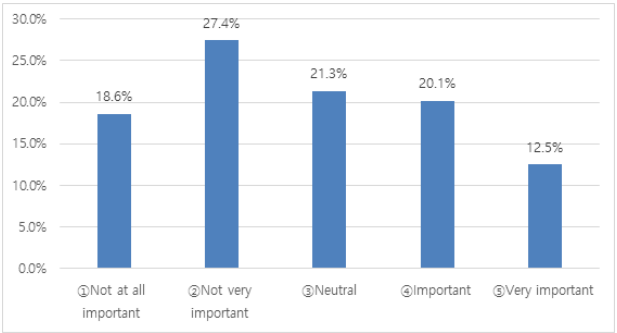
[Figure 1] Types of online services that SMEs use

Keys

①	Email addresses for your company or its employees
②	A website or blog
③	Accounts or pages on social media sites (e.g., Facebook or Twitter)
④	The ability for customers to order, book or pay for products or services online
⑤	An online business bank account your company pays into
⑥	Other

About a third (32.6%) of the respondents replied that online services were either 'important' or 'very important' elements in their businesses [Figure 2]. On the other hand, approximately half (46.0%) of the SMEs did not consider online services as a core part of their business offering (i.e., 'not at all important' or 'not very important'). About a fifth (21.3%) gave a neutral reply. There were 44 more negative responses than positive ones, which was translated into a 13.4 percentage point difference. The fact that negative answers outnumbered positive ones may be counterintuitive when considering that South Korea is one of the most connected societies in the world[2, 21]. However, it highlights that SMEs did not recognise their business dependence upon online services as much as they actually used them [Figure 1].

2. To what extent, if at all, are online services a core part of the goods or services your company provides?



[Figure 2] SMEs' perception on online services

The extent to which SMEs considered online elements within their businesses varied considerably by business size. Medium firms were more likely to

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

consider online services as significant business elements than small firms. While slightly less than a fifth (19.0%) of medium firms recognised online services as 'very important', only 7.6% of small firms viewed in the same way. Similarly, a 14.1 percentage point more of medium firms answered 'important' than small firms did (28.2% versus 14.1%). The *t*-test in <Table 2> showed that medium and small businesses had a significantly different perception of online services (p<0.001).

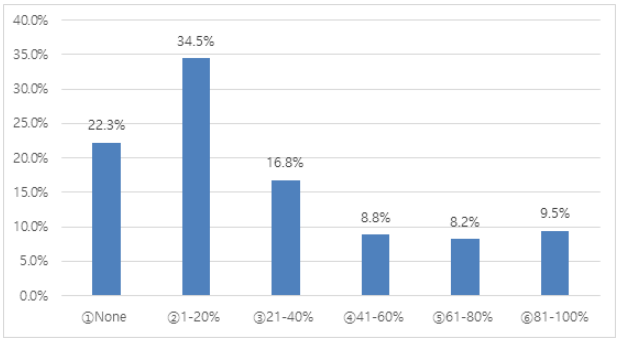
<Table 2> *t*-test statistics on the perception on online services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.54	0.09	1.21	2.36	2.71
Medium	142	3.16	0.11	1.34	2.94	3.38
diff	326	-0.62	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0		*t* value	*df*
			.000		-4.41	324

The use of personally-owned devices for regular work within a firm is a widespread phenomenon in Korea. Although the widespread use of personally-owned devices at work brings convenience to staff, this also means that firms face another set of cyber security risks. Staff in the overwhelming majority (77.7%) of businesses used their own devices to some extent [Figure 3]. However, it was notable that the median in the proportion of staff who used their own devices was '1-20%' and this proportion went down as the value went up. The results highlight that the extent of actual use of personally-owned devices by staff was not considerably high within a firm.

3. How many employees in your company use personally-owned devices such as smartphones, tablets, home laptops or desktop computers to carry out regular business-related activities?

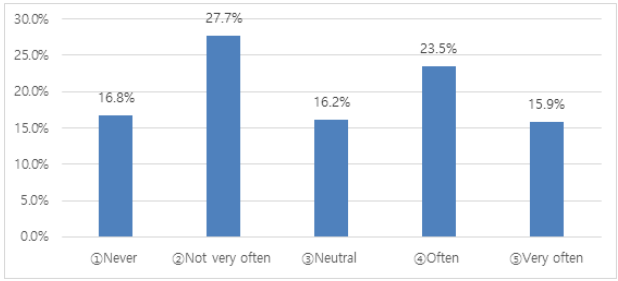
Also, there was a difference by business sector. Over half (58.3%) of businesses in the financial and insurance sector and less than half (41.4%) of businesses in the information and communication sector replied that more than 80% ('81-100%') of



[Figure 3] Proportion of staff who use personally-owned devices for regular work

staff used their own devices at work. On the contrary, manufacturing and construction sectors showed the opposite tendency. Over a fifth (23.2%) and a half (50.0%) of businesses, respectively, in manufacturing sector and construction sector answered that no staff used their own devices at work. Cloud computing was widely adopted by Korean businesses, with about four fifths (83.2%) of businesses using some sort of externally-hosted web services [Figure 4]. Only a minority (16.8%) of businesses did not use them in any form. Over a third (39.4%) of the SMEs used them either 'often' or 'very often'.

4. Does your company currently use any externally-hosted web services, for example to host your website or corporate email accounts, or for storing or transferring data?



[Figure 4] SMEs' use of externally-hosted web services

The use of cloud computing differed by business size. Medium companies were more likely to use externally-hosted services for any reason than small companies. Less than a third (27.2%) of small companies used these services more than 'often', compared to over half (55.6%) of medium companies.

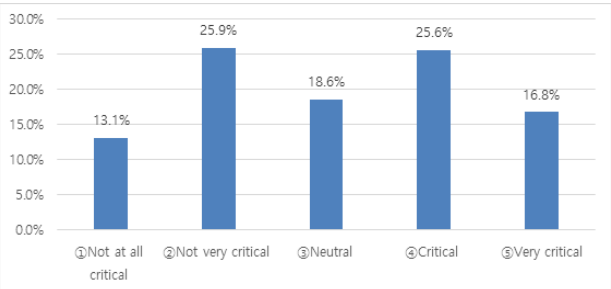
According to the *t*-test result in <Table 3>, medium businesses used externally-hosted web services more often than small businesses (p<0.001), which supports the argument that cloud computing tends to be more acceptable as the company size grows[11].

<Table 3> *t*-test statistics on the use of externally-hosted web services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.55	0.10	1.30	2.37	2.74
Medium	142	3.45	0.10	1.25	3.25	3.66
diff	326	-0.90	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0 .000		*t* value -6.28	*df* 324

Less than half (42.4%) of businesses considered externally-hosted web services were more than 'critical' to their businesses. It should be noted that the frequency distribution of answers in [Figure 5] was quite similar to that of answers in [Figure 4]. The similar pattern of the frequency distribution graphs may imply that these two variables were associated. As a proof of the association, the correlation value between these two variables was .65 which was statistically significant at the .05 level. This indicates that the perception of whether these externally-hosted web services were critical to the respondents' companies [Figure 5] was highly related to the actual use of these services [Figure 4].

5. How critical, if at all, are these externally-hosted web services to your company?



[Figure 5] Criticality of ex

Perception on the criticality of cloud computing services varied by size band. Over half (53.5%) of medium firms viewed these services as more than 'critical' to their businesses, compared to about a third (34.2%) of small firms. The *t*-test analysis in <Table 4> confirmed that the criticality of cloud computing services increased as business size expanded (p<0.001).

<Table 4> *t*-test statistics on criticality of externally-hosted web services by business size

Group	Obs	Mean	Std. Err.	Std. Dev.	95% Conf. Interval	
Small	184	2.81	0.09	1.28	2.63	2.99
Medium	142	3.43	0.11	1.26	3.22	3.64
diff	326	-0.62	0.14			
diff = mean(Small) - mean(Medium)			Ha: diff < 0 .000		*t* value -4.37	*df* 324

4.2 Incidence and impact of cyber security breaches

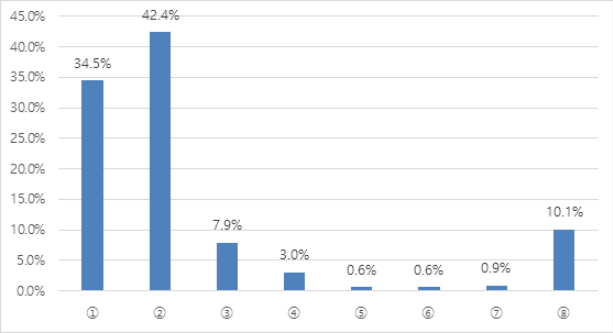
Over half (55.4%) of the SMEs have experienced one or more cyber security breaches in the last 12 months. Among the affected businesses (n=182), the vast majority (76.4%) suffered fewer than 5 breaches and the proportion of the affected businesses went down dramatically as the number of breaches increased. As a consequence, SMEs can be formed into two broad groups: (1) a group which did not suffer any breaches and (2) a group which suffered a few breaches.

In addition, it is worth mentioning that a tenth (10.1%) of the respondents did not know whether their businesses experienced cyber-attacks. Businesses which answered 'Don't know' consisted of 18 small firms (9.8% of the total small firms) and 15 medium firms (10.6% of the total medium firms), which did not show any meaningful difference.

6. Approximately, how many cyber security breaches or attacks have you experienced in total over the last 12 months?

Overall, there was a negative relationship between breach experience and the size of a firm <Table 5>.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



[Figure 6] Experience of cyber security breaches or attacks

Keys

①	None	⑤	15 to fewer than 20
②	Fewer than 5	⑥	20 to fewer than 50
③	5 to fewer than 10	⑦	50 or more
④	10 to fewer than 15	⑧	Don't know

The incidence of breaches was found to be significantly different by business size, with over two thirds (68.1%) of small firms and about half (52.8%) of medium firms having experienced breaches over the last 12 months. The association between breach experience and business size was statistically significant (p=.008). STATA showed that tau-b was -.160, which showed a weak relationship. The asymptotic standard error (ASE) for tau-b was .058. And if tau-b is divided by this estimated standard error, the z test value is obtained. Here, z=-.160/.058=2.76. This z value was significant at the .05 level. It means that the weak relationship was statistically significant.

<Table 5> Cross-tabulation of cyber security breach experience and business size

	Cyber security breach experience		
	No	Yes	Total
Small	53	113	166
Medium	60	67	127
Total	113	180	293
Pearson chi2(1) = 7.124		Pr=.008	
Kendall's tau-b = -.156		ASE=.058	

Among those SMEs (n=132) which claimed online services were 'not very important' and 'not at all important' to their business offer, less than two thirds (64.4%) experienced any form of breach. On the contrary, among businesses (99 SMEs) that considered online services were 'important' and 'very important' to their business offer, about half (53.5%) have experienced breaches. A t-test in Table 6 confirmed that businesses which had no breach experience considered online services as more essential than businesses which had breach experience (p=.025).

<Table 6> t-test statistics on the perception on online services by breach experience

	Group	Obs	Mean	Std. Err.	Std. Dev	95% Conf. Interval	
Breach experience	No	113	3.02	0.13	1.33	2.77	3.26
	Yes	182	2.71	0.10	1.30	2.52	2.90
	diff	295	0.31	0.16			
diff = mean(No) - mean(Yes)				Ha: diff > 0		t value	df
				.025		1.97	293

Another factor related to breach experience was the business sector that a firm belonged to <Table 7>. A chi-square test showed that cyber breach experiences and categories of business sectors were associated (p=.008). Businesses that provided 'public services' were either more targeted by offenders or unprepared for cyber threats than businesses in other sectors. The opposite interpretation could be given to businesses that provided 'services largely directed at organisations'.

<Table 7> Cross-tabulation of cyber security breach experience and categories of business sector

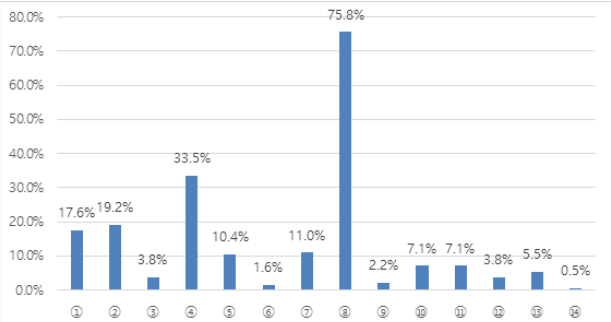
			Categories of business sector				
			1	2	3	4	Total
Cyber breach experience	No	Frequency	22	30	8	51	111
		Expected frequency	20	23	17	51	111
	Yes	Frequency	31	29	36	83	179
		Expected frequency	33	36	27	83	179
		Total	53	59	44	134	290
Pearson chi2(3) = 11.704 Pr=.008							

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

The most common type of breaches experienced [Figure 7] were infections with viruses, spyware or malware (75.8%, 138 out of 182) and stealing money through fraudulent emails or fake websites (33.5%). There was a very large gap between the two. Other noticeable types were unauthorised access (19.2%) and denial-of-service attacks (17.6%). [Figure 7] was comparable to the fact that the most prevalent source of the breach was reported as emails, email attachments, or websites, followed by malware authors. This reaffirmed that Korean SMEs were plagued by massive viruses and malware via email attachments or websites[22]. Against this backdrop, malware authors were seen as the main source of these attacks. Considering that the vast majority of the SMEs used emails and websites for their business [Figure 1], it was clear that they were constantly exposed to cyber security breaches.

7. Which of the following have happened to your company in the last 12 months? (multiple choice)



[Figure 7] of breaches experienced

Keys

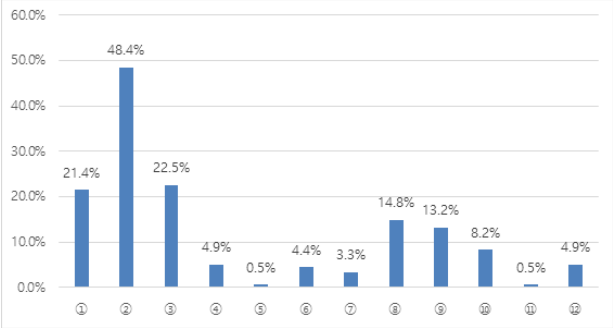
①	Denial-of-service attacks
②	Access to computers, networks or services without permission (i.e., hacking)
③	Money stolen electronically (e.g., through online banking)
④	Money stolen through fraudulent emails or fake websites
⑤	Personal information (e.g., customer data) stolen electronically
⑥	People damaging or stealing software from your computers or network
⑦	People downloading unlicensed/stolen software to computers or network
⑧	Computers becoming infected with viruses, spyware or malware
⑨	Theft of intellectual property
⑩	Others impersonating company in emails or online
⑪	Breaches from personally-owned devices
⑫	Breaches from externally-hosted web services
⑬	Breaches on social media
⑭	Other

Slightly under half (48.4%) of breaches were detected by anti-virus or anti-malware software. As these software are regularly updated by providers, they provide convenience for business users at low cost. These software are a one-size-fits-all approach, as once installed no further configurations or efforts are needed. The second and third most prevalent ways for detection were disruption to business (22.5%) and by accident (21.4%). These ways are reactive rather than proactive. Being aware of attacks upon disruption to business may be the worst scenario in that damage from a breach has already occurred. The fact that a fifth (21.4%) of businesses identified breaches by accident indicates that there were a large number of attempted attacks which were not detected. All the aforementioned detection methods did not involve any internal control mechanisms or security management processes.

On the other hand, identification by reports from staff or contractors (14.8%) and routine internal security monitoring (13.2%) are more proactive methods. These methods indicate that there is an organisational structure for cyber security. In other words, internal control mechanisms are, to some extent, active in a company. It is expected that a business will be willing to adopt these proactive methods as their business management becomes more structured. Adopting proactive methods is recommended in that they are more likely to detect not only breaches but also attempted attacks earlier than reactive methods.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

8. How was the breach or attack identified? (multiple choice)



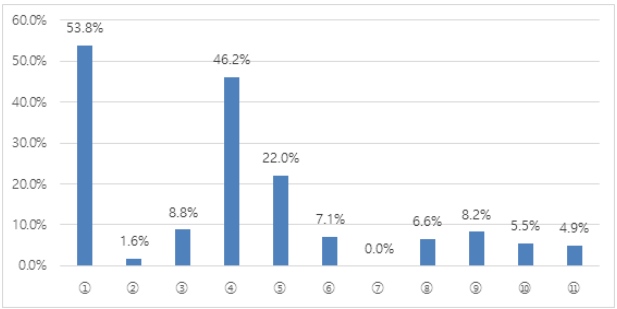
[Figure 8] Methods for identifying breaches or attacks

Keys

①	By accident
②	By antivirus/anti-malware software
③	Disruption to business/staff/users/ service provision
④	From warning by government/law enforcement
⑤	Our breach/attack reported by the media
⑥	Similar incidents reported in the media
⑦	Reported/noticed by customers/customer complaints
⑧	Reported/noticed by staff/contractors
⑨	Routine internal security monitoring
⑩	Other internal control activities not done routinely (e.g., reconciliations, audits)
⑪	Other
⑫	Don't know

Regarding the impact of breaches, there was a considerable variety in replies [Figure 9]. Two impacts that stood out were stopping staff from carrying out their day-to-day work (53.8%) and any other repair or recovery costs (46.2%). These impacts are direct consequences of disruption to business continuity. In addition, implementing new measures for protecting against future attacks (22.0%) is a necessary follow-up response after the business disruption. These impacts are classified as direct or short-term impacts which require organisational responses within a short period of time. In contrast, some respondents did not think their firms experienced indirect or long-term impacts such as loss of revenue (1.6%), fines from regulators (0.0%), and reputational damage (6.6%) as often as direct or short-term impacts.

9. Thinking of all the breaches or attacks experienced in the last 12 months, have these impacted your company in any of the following ways? (multiple choice)



[Figure 9] Types of the impact of breaches or attacks

Keys

①	Stopped staff from carrying out their day-to-day work
②	Loss of revenue or share value
③	Additional staff time to address the breach, or to inform customers or stakeholders
④	Any other repair or recovery costs
⑤	New measures needed to prevent or protect against future breaches or attacks
⑥	Lost or stolen assets
⑦	Fines from regulators or authorities, or associated legal costs
⑧	Reputational damage
⑨	Prevented provision of goods or services to customers
⑩	Discouraged you from carrying out a future business activity you were intending to do
⑪	Other
⑫	Don't know

Even though 'reputational damage' (6.6%) was not recognised as a crucial impact on overall businesses, it was perceived differently depending on business size. Medium firms were more likely to suffer reputational damage than small firms (6.3% versus 1.6%). And, the association between reputational damage and business size was statistically significant in Table 8 (p=.025). However, no association was found between reputational damage and business sector categories in <Table 9> (p=.903).

<Table 8> Cross-tabulation of reputational damage and business size

		Business size		
		Small	Medium	Total
Reputational damage	Yes	3	9	12
	No	181	133	314
	Total	184	142	326
Pearson chi2(1) = 5.010 Pr=.025				

<Table 9> Cross-tabulation of reputational damage and categories of business sector

		Categories of business sector				
		1	2	3	4	Total
Reputational damage	Yes	2	3	1	6	12
	No	57	63	48	143	311
	Total	59	66	49	149	323
Pearson chi2(3) = 0.569 Pr=.903						

Keys

①	Services largely directed at public	③	Public services
②	Services largely directed at organisations	④	Manufacturing and construction

5. Conclusion

The results show that Korean SMEs were highly connected to ICTs, but perception of their significance did not correspond to the actual adoption of ICTs. A sizable majority of Korean SMEs relied upon online services in some form. The adoption of online services was mainly for communications and advertisement rather than business or financial transactions. Online services were used not only by business-owned devices, but also via personally-owned devices at work (77.7%). In particular, the use of externally-hosted web services was a widespread phenomenon in Korea. However, SMEs' perception of ICTs' significance did not necessarily match the high extent of actual usage of them. A 13.4 percentage point more of businesses replied negatively when asked whether their online services were a core part of their business offering. In addition, the number of positive answers (42.4%) was almost equal to that of negative answers (39.0%) when asked whether externally-hosted web services were critical to their business.

Despite the significance of the ICT adoption, cyber security breaches affected all kinds of SMEs and costs were not clearly measured. It was notable that one in two businesses (55.4%) have experienced cyber security breaches, the majority attributed to viruses and malware (75.8%). Most of them were funnelled through emails, email attachments, or websites (53.8%). Two features of cyber-attacks using viruses and malware are the indiscriminate nature as to victim selection and low cost[6]. Business disruption (53.8%) and direct costs (i.e., repair or recovery costs: 46.2%) were found to be the most crucial impacts of cyber-attacks on businesses.

This study shed a light on the vulnerabiilty of SMEs by investigating the situation of SMEs as to ICT connections and cyber security. Considering the lack of research and awareness of the SMEs' cyber security threats, this empirical study will contribute to knowledge in the field of cyber security management of businesses. The results here are expected to act as a fundamental work which facilitates future studies. Future works need to closely delve into the dynamics of businesses concerning the management of cyber security.

6. References

[1] International Telecommunication Union(2015a), ICT facts & figures.

[2] International Telecommunication Union(2015b), Measuring the information society report.

[3] United Nations(2014), E-government survey. Retrieved from https://publicadministration.un.org/egovkb/portals/egovkb/documents/un/2014-survey/e-gov_complete_survey-2014.pdf

[4] Z. A. Soomro, M. H. Shah, J. Ahmed(2016), "Information security management needs more holistic approach: A literature review." International Journal of Information Management, 36(2):215-225.

[5] J. Hashim(2015), "Information Communication Technology(ICT) adoption among SME owners in Malaysia." International Journal of Business and Information, 2(2):221-240.
[6] D. Wall(2007), Cybercrime. Cambridge: Polity.
[7] National Police Agency(2012), National police white paper. Seoul: TSO.
[8] National Police Agency(2017), National police white paper. Seoul: TSO.
[9] Office for National Statistics(2017), Crime in England and Wales: Year ending Sept 2016. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016
[10] A. Gupta, R. Hammond(2005), "Information systems security issues and decisions for SMEs: An empirical examination." Information Management & Computer Security, 13(4):297-310.
[11] D. Truong(2010), "How cloud computing enhances competitive advantages: A research model for SMEs." The Business Review, 15(1):59-65.
[12] J. M. Bauer, W. H. Dutton(2015), The new cyber security agenda: Economic and social challenges to a secure internet. World Bank' World Development Report, No. 102965.
[13] D. Organ(2015), "Trust through certification in SME Cloud adoption." In P. R. J. Trim, & H. Y. Youm (Eds.), Korea-UK collaboration in cyber security: From issues and challenges to sustainable partnership (pp. 32-46). Seoul: British Embassy in South Korea.
[14] R. Blackburn(2012), Segmenting the SME market and implications for service provision: A literature review. London: Advisory, Conciliation and Arbitration Service, Research Paper Ref: 9/12.
[15] B. Herbane(2010), "Small business research: Time for a crisis-based view." International Small Business Journal, 28(1):43-64.
[16] A. Ghobadian, D. Gallear(1997), "TQM and organization size." International Journal of Operations & Production Management, 17(2):121-163.
[17] K. Grant, D. Edgar, A. Sukumar, M. Meyer(2014), "'Risky business': Perceptions of e-business risk by UK small and medium sized enterprises (SMEs)." International Journal of Information Management, 34(2):99-122.
[18] M. Harris, K. Patten(2014), "Mobile device security considerations for small and medium-sized enterprise business mobility." Information Management & Computer Security, 22(1):97-114.
[19] D. Bhattacharya(2011), "Leadership styles and information security in SMEs." Information Management & Computer Security, 19(5):300-312.
[20] Department for Digital, Culture, Media and Sport (2018), Cyber security breaches survey 2018. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018
[21] Organisation for Economic Co-operation and Development(2017), Fixed and wireless broadband subscriptions per 100 inhabitants.
[22] Symantec(2017), Internet security threat report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

저자 소개

정 제 용
울산대학교 사회과학대학 경찰학과 조교수
관심분야 : 중소기업의 보안관리, 사이버범죄 등