Participatory Educational Research (PER)
Vol. 6(2), pp. 51-64, December, 2019
Available online at http://www.perjournal.com
ISSN: 2148-6123
http://dx.doi.org/10.17275/per.19.12.6.2

A Perceptional Analysis of BYOD (Bring Your Own Device) for Educational or Workplace Implementations in a South Korean Case

Hasan Tinmaz
Technology Studies - Endicott College of International Studies - Woosong University - Daejeon, South Korea

Jin Hwa Lee*
Global Healthcare Management - Sol International School - Woosong University - Daejeon, South Korea

Article history

Received:
28.08.2019

Received in revised form:
24.09.2019

Accepted:
27.09.2019

Key words:
BYOD; Bring Your Own Device; Education; Workplace; South Korea; Security; Policy

As the communication and information technologies (especially mobile devices) have become a central part of our daily lives, people have started to bring their own devices to schools, universities, companies and other types of organizations. Bearing in mind the difficulty of stopping people from carrying these devices, Bring Your Own Device (BYOD) represents a paradigm shift, presenting new ways for organizations to function and offering several advantages to businesses, notably a reduction in hardware costs. Although BYOD (allowing people to bring their technological devices to schools or workplaces) sounds simple in words, BYOD implementations come with their own challenges (security related problems being the first). This study aims to analyze the perceptions of a group of South Korean undergraduate and master students (n=110 in total) of BYOD implementations in schools and in workplace separately. The study instrument had three sections; (i) basic demographics (age, gender and currently attending education level), (ii) 12 survey items on a Likert scale for BYOD perception at school questions, and (iii) 12 survey items on a Likert scale for BYOD perception at workplace questions. After the analyses of demographics, separate independent sample t-tests were applied in order to check if each set of 12 items for BYOD at school and at workplace significantly differ for gender and education level variables. While no significant difference was revealed based on gender variable, education level demonstrated differences on certain items. At the end, the 12 items for BYOD at school and BYOD at workplace were compared by applying paired samples t-tests to the dataset where significant differences were also observed for some items. The general results showed that participants supported BYOD in schools more than BYOD at workplace. Besides, master students showed more trust than undergraduate students on cyber-security both at school and at workplace.

*Correspondency: jlee4986@wsu.ac.kr / jlee4986@yahoo.com

Introduction

Last two decades have witnessed the integration of different communication and information technologies into people's daily lives. Computers or mobile technologies are not perceived as luxuries anymore. When people decide to go out, they check their mobile phones, even before their wallets. Thus, it is becoming more difficult to convince people not to bring their own technological devices to schools or workplace. The continuing mobile technology revolution will promote that the situation has turned out to be even stronger than before (Garba, Armarego & Murray, 2015). Therefore, it is indispensably vital to discover innovative ways to overcome that challenge. That is where BYOD approach will enlighten many organizations.

In a workplace context, BYOD can be described "… as an environment that allows employees to use their own personal device to have access to an organization's resources to perform their work" (Putri & Hovav, 2015, p. 1). Furthermore, BYOD in an instructional context could be described as "allowing pupils/students to bring their own devices, especially tablets and other suitable personal devices, into classrooms to support improving student learning outcomes" (Bring your own Device (BYOD) for Learning, 2017, p. 1). BYOD approach is actually a paradigm change in how organizations function within their structure (Ubene, Agim, & Umo-Odiong, 2018).

When the definitions are considered, BYOD implementations look very simple. On the other hand, many BYOD supporting organizations (such as Bring your own Device (BYOD) for Learning (2017) from Ireland or BSI Group (2015) from USA) strongly underline that BYOD also comes with its own unique challenges affecting how the organization functions. BSI Group specifically remarks that BYOD brings difficulties to IT staff of the organization: they need to re-think about the sustainability of security, updating, and many other technology related processes. Additionally, by considering the security and privacy related challenges of BYOD approach, the administrative bodies of any organization must develop policies for the effective integration of BYOD.

'Bring your own Device (BYOD) for Learning' (2017) lists the possible contribution of BYOD for learners as: providing more learner-centered context; offering more chances for active learning experiences; giving more responsibilities to the learners about their learning processes; increasing levels of participation through the familiarity of the devices; users having a stronger sense of taking care of the devices; and suggesting a framework to finalize class assignments or homework out of the class time. Moreover, students' informal learning processes could be transferred to formal learning (and vice versa) with the help of BYOD implementations.

The BYOD approach has been incorporated not only into educational institutions, but also into business. Many corporations have realized the financial (such as reduction in hardware expenditures) and personal advantages (increase in productivity and efficiency) of BYOD for their organizations. Although these corporations have also been well aware about the possible risks of BYOD policy in their organizations, online security related issues have still been underestimated (Downer & Bhattacharya, 2015; Putri & Hovav, 2014).

Downer and Bhattacharya (2015) list BYOD security challenges in the workplace under four major categories; (i) deployment related challenges (infusion of BYOD approach into the organization schema including to what extent BYOD should be integrated), (ii) technical issues (control of access rights including security measures, controlling network connections

and data circulation, and security of cloud based storage), (iii) policy and regulation related problems (governmental and legal arrangements and ethical matters), and (iv) human resource related challenges (training provided to employees and their reactions toward BYOD policies).

BYOD-implementing educational institutions must also be ready for challenges. The major concerns for schools include device and/or network resource compatibility, possible security problems, and ethical issues. BYOD offers a solution to schools whose budgets do not allow extensive alterations to their IT infrastructure (Ubene, Agim, & Umo-Odiong, 2018). Beyond these important issues, if there is a digital divide among learners (i.e. inequalities toward accessing and using technological devices), it would be unrealistic to imagine that BYOD would bring success to that context (Bring your own Device (BYOD) for Learning, 2017). Therefore, many scholars and organizations (Bring your own Device (BYOD) for Learning, 2017; Cheng, 2016; Downer & Bhattacharya, 2015; Garba, Armarego & Murray, 2015; Harris, Patten & Regan, 2013; McLean, 2016; Putri & Hovav, 2015) highlighted that BYOD implementations into different contexts still require further study to be successfully deployed.

South Korea is a well-known country of production, integration and utilization of different information and communication technologies (especially mobile devices), therefore it is not surprising that the country has been paying relatively more attention to BYOD approach in the schools or workplaces. However, possession of these technologies does not necessarily mean that public is ready to bring their devices to these contexts. Therefore, this study aims to unfold readiness levels of a group of South Korean students for the integration of BYOD in their schools and in their prospective workplaces.

Literature Review

There has been an ongoing effort to implement information and communication technology (ICT) in education. The use of computer and mobile devices brought significant changes to traditional classrooms as it enabled to facilitate online learning. In accordance with these changes, educational researchers have studied the impact of ICT on teaching and learning. For example, it was reported that mobile phones and mobile tablet technologies can support collaborative learning in both conventional and online learning environments (Falloon, 2015). Additionally, ICT also has a potential to develop self-determined learning and thusly a learner-centered environment (Blaschke, 2018).

So as to be able to maximize the potential benefits that ICT carry, it has become vital for learners to have one-to-one access to ICT devices. However, it often puts financial pressure on educational institutions to purchase and maintain necessary devices for all students (Cardoza & Tunks, 2014) in that sense. To address and overcome this challenge, Bring Your Own Device (BYOD) approach has been implemented in classes where students bring their own technological devices to supplement their own learning (McLean, 2016).

The BYOD approach has a number of benefits for both educational institutions and students. It can relieve schools lifting the cost pressure and responsibility for maintaining computers or tablets (Cardoza & Tunks, 2014). Depending on the school policy, there might be a partial responsibility such as software installation yet schools are not fully responsible for purchasing necessary devices.

Another benefit of BYOD includes a high level of student engagement through creating

interactive and student-centered learning environment. A study conducted by Song (2014) suggested that BYOD helps students advance their content knowledge and develop positive attitude towards learning. This study involved grade six primary school students in Hong Kong and they were asked to use their own mobile devices to explore the anatomy of fish. It was witnessed that students exhibited a sense of ownership and control over their own learning which was lacking in previous studies where learning devices were provided by school.

BYOD can also help keep up with rapid changes in technological trends. As the learners will continuously update or upgrade their own devices, educational tools can catch up with technological advances. This implies that learners are equipped with most up-to-date skills and knowledge through BYOD. In fact, studies have reported that BYOD could contribute to the development of in-demand twenty-first century skills such as digital literacy and fluency, critical thinking, problem solving and collaboration (Clifford, 2012; Hopkins, Sylvester, & Tate, 2013; Rackley & Viruru, 2014).

BYOD can also be utilized for professional development of education providers. A study conducted by Kong and Song (2015) combined BYOD and a flipped classroom model to train twenty-six in-service teachers at a higher education institute in Hong Kong. Participants were allowed to use their own devices to access learning resources and facilitate discussions in class. Devices were used to access the Edmodo (online learning platform for teachers and students) application, read online articles, and then participate in peer discussions outside class. The results of this study showed that a hybrid approach incorporating BYOD within a flipped classroom could advance professional knowledge and induce reflective inquiry for professional development.

BYOD is also gaining popularity in workplaces. As the use of personal devices allows employees to gain access to their work materials anytime and anywhere, the amount of work related activity will naturally increase. In fact, Beckett (2014) reported that companies observed a boost in work activity during holiday leave as employees could not resist the compulsion of checking easily accessible emails and the flow of information. In response to this trend, global companies such as Google and Apple have been working on software development which can facilitate the division of work-related and personal data on their devices (Beckett, 2014).

Although BYOD can certainly bring many benefits to both educational institutions and workplaces, studies also reported several concerns with its implementation. Since learners are familiar with their own devices, there are many factors that can potentially distract them from learning. These include entertainment or social networking applications, pop-up alerts and also digital games.

Students can also be distracted from learning due to the small screen size, short battery life, limited processing power and memory capacities of their devices (Cheng, 2016). That is to say the varying performance of students' devices can influence the learning process itself as well as user acceptance of BYOD. This might potentially create issues of digital disparity between economically affluent and disadvantaged students (Taneja, Fiore, & Fischer, 2015).

Another concern with BYOD is security. Security of information is the topmost priority of any organization's management (Ubene, Agim, & Umo-Odiong, 2018). Education institutes or companies usually implement system configuration based on the need to monitor data

usage and detect misuse or hacking attempts. However, it is difficult to force BYOD users to implement security policies on their personal devices and thus security risks will increase in an inevitable fashion (Dhingra, 2016).

In addition to these, users' lack of responsibility for security can accumulate risks belonging to BYOD. Harris, Patten and Regan (2013) conducted a survey on 131 college students in the United States in which 76% of the students believed that it is the employer's responsibility to provide security software for BYOD equipment. Their study also highlights other important issues related to BYOD security. For example, students' self-reported ratings at securing their devices were high but adequate installation of antivirus and firewall was poorly executed (Harris, Patten & Regan, 2013).

A number of studies have suggested possible solutions to BYOD security issues. For example, mobile device management tools can be used to remotely reset or delete the partitions of data from a BYOD user's device (Dhingra, 2016). However, terms and conditions of using these program tools must be agreed between the organization and employees or students, being the relevant parties involved. Another possible solution was suggested by Armando, Costa and Merlo (2013). Their study described a security framework wherein only applications complying with the security policy could be installed on the registered devices. This framework mediates access to the application store and informs the user with which applications can be installed safely. In another quantitative study (n=600 employees) by Putri and Hovav (2015), the success of effective BYOD strategies are related with the existence of IT security awareness programs and IT support staff in the organization.

As the BYOD approach has benefits and risks at the same time, it is vital to create right educational or organizational policies for its successful implementation. This requires careful investigation of BYOD user opinions or perceptions. In fact, a study conducted by Cheng (2016) investigated user acceptance of BYOD involving forty-four undergraduate students and two teachers at the Hong Kong Polytechnic University. Participating students were asked to complete pre and post-user acceptance questionnaires at the beginning and at the end of a 13-week semester. Focus group interviews were also carried out for deeper understanding of student and teacher views on BYOD. The results of this study showed that the participants generally supported the implementation of BYOD though several concerns raised. One of the concerns was the possible distraction caused by digital devices as described above. It was also mentioned that education institutions should include BYOD related activities or practices in the curriculum and support professional development of teachers. As such, it is suggested that BYOD related policy should aim to reduce the distraction of learners and foster the pedagogical practices of teachers.

'Bring your own Device (BYOD) for Learning' (2017) suggests critical steps for developing an effective BYOD related policy; (i) it is very important to include all stakeholders into the policy design, development and implementation phases, (ii) a strong communication mechanism among stakeholders is vital, (iii) a core team should be organized to maintain all phases of BYOD policy, (iv) the inevitable challenges and issues throughout the policy development phases must be perceived as an opportunity for improvement, (v) it is better to have a pilot implementation rather than a rapid change in the organization, and lastly (vi) the ideas of other organizations which are implementing BYOD in their bodies should be collected and implemented, if possible.

A recent study conducted by Weeger, et al. (2018) highlights undergraduate students'

perceptions of BYOD at workplace. It involved 476 students from European, Asian and American universities in their final year of undergraduate studies with relevant work experience. Through an online survey, this study analyzed students' intentions to join a BYOD program at work and examined how they perceived the benefits and risks associated with it. The results showed that the intention to enroll in a BYOD program was mainly driven by perceived benefits while the risks were widely neglected. The perceived risks included financial, security, privacy, safety, and performance risks. According to the study, it is evident that the upcoming generation of employees will be supportive towards BYOD implementation at workplaces regardless of potential risk factors. This implies the necessity of developing new BYOD strategies or policies suitable for so-called digital natives (Hershatter and Epstein, 2010) as these future employees do not fall into the categories of classical perceived risk theory (Weeger et al., 2018).

Gender difference should be also considered for BYOD policies as it can produce different outcomes for male and female users. A previous study on young Korean males and females reported that the patterns of their computer use were different (Lim & Meier, 2011). According to the study, both males and females used computers for four general purposes: social networking, personal knowledge, formal learning, and entertainment. Different preferences in their computer use was observed as males spent more time on entertainment, such as multi-user online games, and females focused more on social networking websites. In addition, another study on gender difference was conducted in a primary school of Canada involving 51 boys and 44 girls (Johnson, 2011). The study reported that there was a difference in home-based internet use but no difference in school-based use.

Through the literature review, different aspects of BYOD have been discussed. In particular, there were several benefits and concerns with BYOD implementation. Possible benefits include reducing cost pressure, increasing student engagement, up-to-date devices, professional development for education providers, and increasing work efficiency at workplaces. On the other hand, possible drawbacks carry security risks and distractions from learning due to social networking services. Studies on BYOD user perceptions have also provided valuable information for creating appropriate BYOD policies which should encompass possible gender differences.

As evident in previous studies, successful implementation of BYOD in class or at workplace requires continuous research on students' perception or attitude towards BYOD. As they will become a new generation of employees equipped with ICT skills, the research output will also contribute to a smooth transition of the current workplace towards a more ICT oriented environment. To this end, our study was conducted involving 110 university students in South Korea with a view to investigating their perceptions on BYOD related issues and future implementation in class or at workplace.

Method

Sample

This study sample incorporates 110 undergraduate and master students in total, studying in an international business school of a private university in South Korea. Although the researchers were working at the same university but in different departments, the researchers delimited the study sample to that faculty's students in order to increase the honesty of sample and to decrease the sense of pressure to join the study. As Fraenkel and

Wallen (2000) point out, this type of convenience sampling will help the researchers address a large sample size targeting an increase in the possibility of population representation.

The prepared study instrument was uploaded onto a webpage and its URL was shared on the closed faculty Facebook group (as an informal way of communication) and sent also as an email to students' school email addresses (as a formal medium of communication). The URL stayed active for two weeks and then collected data was downloaded to an SPSS file.

According to the dataset, the age of participants (n=110) ranges from 20 to 29 with a mean score of 25.53 and 2.87 standard deviation. As Table 1 demonstrates, majority of the participants are enrolled in a master's degree program, and there is a circa equal distribution of male and female participants for this study.

Table 1. Gender versus currently attending education level of participants

	Master	**Bachelor**	**Total**
Female	42	11	53
Male	45	12	57
Total	87	23	110

Study Instrumentation

This research intends to reveal higher education students' ideas and perceptions on BYOD trend for their current school activities and prospective professional life. Therefore, the researchers needed to develop their own study instrument based on the existing literature and on their personal experiences with that trend, which has also been recommended by Johnson and Christensen (2004) for such cases. In subsequent to initial study instrument design, the researchers sent the file to their three colleagues to get their opinions on the instrument so that the content validity of the instrument would be increased. Later on, the last draft version of the instrument was directed to an English language expert for proofreading. The finalized version of the instrument was uploaded onto an online statistics webpage and URL was shared with the sample.

The finalized study instrument was comprised of three sections; (i) basic demographics (age, gender and current degree program), (ii) BYOD at school questions (the frequency of bringing their own devices to school, a degree of comfort for BYOD at school, 12 survey items on a Likert scale for perception, two questions on online and physical security issues for BYOD at school), and, after being presented with a hypothetical workplace scenario asking them to bring their personal devices to work, (iii) BYOD in workplace questions (a degree of comfort for BYOD at work, two separate questions on feelings towards online security at work, 12 survey items on a Likert scale for perception and two questions on online and physical security issues for BYOD at work).

It is important to note here that these 12-survey items for school and workplace were produced in a way that researchers could compare them statistically with ease. For instance, the item referring to online security at school has been changed to online security at workplace. Prior to all analyses, related reliability analyses were conducted for questions on BYOD at school and BYOD at work and Cronbach alphas were calculated as 0.71 and 0.74 respectively. According to Fraenkel and Wallen (2000), these values, which are higher than 0.60 indicated satisfactory levels of reliability.

Data Analysis

As the study instrument included three sections, the researchers initially analyzed them in sections as well. First section was listed in frequencies and percentages. Second and third sections were reported as frequencies (and percentages) and mean scores / standard deviation for 12 survey items.

After the general depiction of study results, the researchers conducted comparative analyses. 12 items for BYOD at school and second set of 12 items for BYOD at work were checked whether gender / education level variables make significant differences by using separate independent sample t-tests. Lastly, the 12 items for BYOD at school and BYOD at work were compared by using paired sample t-tests.

Results

After basic demographics, the participants were asked to mark how often they brought the listed technological devices to their school (Table 2). Nearly half of the participants reported that they often bring their laptops.

Table 2. How often the participants bring the following technological devices to school

	I don't have	Never	Occasionally	Sometimes	Often	Always
Laptop	1 / 0.9%	-	-	38 / 34.5%	53 / 48.2%	18 / 16.4%
Tablet	1 / 0.9%	8 / 7.3%	30 / 27.3%	41 / 37.3%	24 / 21.8%	6 / 5.5%
Smartphone	7 / 6.4%	18 / 16.4%	23 / 20.9%	21 / 19.1%	25 / 22.7%	16 / 14.5%

The participants were additionally asked if bringing their own devices made their learning more comfortable for them. The majority of participants (n=81, 74%) agreed with the statement whereas 29 participants disagreed (26%).

Afterwards, the researchers offered 12 survey items on a 5-Likert scale (from "strongly agree" to "strongly disagree") on BYOD at school (Table 3). At a first glance, the participants disagreed with the fact that they worry about their professors being able to access their personal devices in school (*M*=1.95). On the other hand, the participants showed relatively less disagreement on the survey item that their information could be accessed by their classmates (*M*=2.29).

Furthermore, the results demonstrate that there is a moderate level of alertness toward bringing their devices to school, when students are asked to consider online security issues. It seems that they do not completely trust the school to protect their devices. Moreover, the participants were not exactly sure about the physical security of their devices while they were in school. The mean scores on students' awareness of security arrangements in the school were higher for physical security than online security.

Table 3. BYOD at school questions

Survey Items	**M**	**SD**
1. I am worried that my data can be stolen while using school internet.	3.87	0.67
2. I am worried that another student can access my personal devices in school.	2.29	0.91
3. I am worried that my professors can access my personal devices in school.	1.95	1.26
4. My school protects my data from cyber-attacks.	2.97	0.95
5. A school should have a back-up system in case of damage or loss due to cyber-attacks.	3.35	1.07
6. My school controls the contents that I can access while using school internet.	3.03	1.13
7. I believe that my personal data is secure while using school internet.	3.15	1.04

Survey Items	M	SD
8. I believe that my personal devices are secure in my school that nobody will steal them physically.	3.13	1.13
9. I believe that there is a team in my school working on online security.	3.30	1.16
10. I believe that there is a team in my school working on physical security.	3.45	1.13
11. I believe that social media can be banned while using school internet.	3.19	1.14
12. Exchanging school related contents with my classmates while using my personal device is safe.	3.22	1.13

The participants were asked who should be blamed in case of damaged or loss of personal data in a school due to a cyber-attack. They mostly preferred to blame the other students (n=36, 33%) and the school (n=35, 32%). Afterwards, the participants put the blame on the IT department (n=21, 19%) and lastly themselves (n=18, 16%).

The same question was asked to participants but this time the blaming was about physical theft. The dominant options stayed the same; the school (n=36, 33%) and the other students (n=34, 31%), although the order changed slightly. However, the participants blamed themselves (n=21, 19%) more than the IT department (n=19, 17%).

From this point onward, the participants were given a scenario explaining that, when they start working, their company will give provide them with free internet connection only and hence they must bring their own devices (laptops, smart phones, etc…) to their workplace.

Based on the scenario, the first question was whether or not they would feel comfortable by bringing their own devices to workplace. While 58 of the participants (53%) marked no, 52 of the participants (47%) reported in favor. Next question was asking if they would feel that their personal data would be secure when bringing their devices to the workplace. 52% of the participants (n=57) pointed that their data would be secure, while 48% of the participants (n=53) disagreed. As a third question, they were asked to state whether or not they would feel that their personal data would be secure when connecting to the company internet with their own devices. The disagreement increased to 61% in that question (n=67) that they do not feel secure to use company internet with their own devices (39% (n=43) accepted that approach).

Subsequently, the participants were offered 12-survey items on a 5-Likert scale (from "strongly agree" to "strongly disagree") for BYOD in the workplace (Table 4). Initially, similar hesitance as in BYOD at school seems to exist between co-workers and the managers regarding access to personal information. The results unfolded that participants trust their colleagues (M=2.35) less than their boss (M=1.85) on that issue.

Additional similarities with BYOD at school are detected in the workplace scenario. Unlike BYOD at school, the participants expected that there will be an online security team for them at their workplace more often than a physical security team.

Table 4. BYOD at workplace questions

Survey Items	M	SD
1. I am worried that my data can be stolen while using company internet.	3.88	0.65
2. I am worried that another colleague can access my personal technological devices at work.	2.35	0.92
3. I am worried that my boss can access my personal technological devices at work.	1.85	0.99
4. My work will protect my data from cyber-attacks.	3.00	0.98
5. A company should have a back-up system in case of damage or loss due to cyber-attacks.	3.33	1.09
6. My work can control the contents that I can access while using company internet.	3.15	1.02
7. I believe that my personal data will be secure while using company internet.	3.06	1.14

Survey Items	M	SD
8. I believe that my personal technological devices will be secure at work that nobody will steal them physically.	3.17	1.13
9. I believe that there will be a team at my work for online security.	3.45	1.14
10. I believe that there will be a team at my work for physical security.	3.17	1.16
11. I believe that social media can be banned while using company internet.	2.36	0.92
12. Exchanging work related contents with my colleagues while using my personal device is safe.	3.33	1.15

In an additional question, the participants were asked who should be blamed in case of damage or loss of personal data in a company due to a cyber-attack. The answers were ordered as follows; 41% the company (n=45), 28% the other employees (n=31), 23% themselves (n=25) and 8% the IT department (n=9).
The same question was asked once more by changing the cyber-attack to a real physical theft. In that case, although the order of accusation stayed the same, the percentage of the other employees increased dramatically. Hence, the order appeared as follows; 40% the company (n=44), 39% the other employees (n=43), 12% themselves (n=13) and 9% IT department (n=10).

The Comparisons

In order to get deeper knowledge about BYOD at school/workplace, the researchers conducted comparison-based statistical tests on the data. It is important to note that 12 Likert-scale questions both in school part and workplace part are formed in a way that they address the same issue from either school or workplace perspectives. To illustrate, 'my school' has been replaced with 'my work' in the second group of questions.

When "gender" was the comparison variable, neither BYOD at school items nor BYOD for workplaces items showed significant differences in the results of separate independent samples t-tests. More independent samples t-tests were conducted for participants' degree program (bachelor versus master). One question for BYOD at school and one other question for BYOD for workplace exhibited significant differences according to the education level variable (Table 5). Masters students believe more than undergraduate students that their data is protected from cyber-attacks in their school. Conversely, undergraduate students believe more than master students that they would have control over their data when using a company internet connection. When the sample sizes for master and bachelor students (87 versus 23) are considered, the results should be interpreted sensitively due to the sample size difference.

Table 5. Independent sample t-tests for educational level

Survey Item	Educational Level	n	M	SD	*t*	*p*
BYOD at school (Question 4)	Master	87	3.07	0.99		
My school protects my data from cyber-attacks.	Bachelor	23	2.60	0.73	2.092	0.039
BYOD at workplace (Question 6)	Master	87	3.02	1.05		
My work can control the contents that I can access while using company internet.	Bachelor	23	3.61	0.79	-2.505	0.014

The last comparison was whether the items in two sets of BYOD approaches significantly differ to each other. Paired samples t-test results yielded only one significantly differing item (item 11 – 'I believe that social media can be banned while using school internet' versus 'I believe that social media can be banned while using company internet') ($p<0.000$, $t=6.475$). It

shows that the participants believe in the necessity of social media banning for universities (M=3.19, SD=1.13) more than workplaces (M=2.36, SD=0.92), while using the internet services provided by either the school or the workplace.

Discussion and Conclusion

Based on the results obtained in this study, it is evident that a majority of students support BYOD at school. However, more than half of the students were against BYOD at workplace. This could be due to students' dependence on laptops or other personal devices to study and complete their coursework. In most universities in South Korea, it is almost impossible to provide a work device to each individual student for financial reasons. According to the Korean Statistical Information Service (KOSIS), South Korean universities where e-learning was not yet implemented, cited financial difficulty as the primary reason for that (65.1%) (KOSIS, 2017). The shortage of available ICT devices on campus makes students rely on their personal devices and, indeed, more than 90% of our survey participants brought laptops to school. On the other hand, employees are less dependent on their personal devices as computers or laptops are generally provided at workplace. Such different levels of dependency on personal devices might have produced different responses belonging to students to BYOD at school and workplace.

In this study, it was also observed that students would blame different targets for cyber-attacks occurring at school and workplace. Students did not perceive their school as the primary party to blame whereas an employer was perceived as more responsible. This could mean that students might be more generous towards their school in terms of online security or have fewer expectations. In fact, the survey results indicated that students' expectations of physical security were higher than online security at school, while there was an opposite expectation in the workplace. Overall, students believe that their future workplace should protect personal devices from cyber-attacks. A similar result was obtained in a study conducted by Harris, Patten and Regan (2013). As mentioned in the literature review, most participants from that study believed BYOD security is the employer's responsibility and they were also overconfident with protecting their own devices from cyber-attacks (Harris, Patten & Regan, 2013). This indicates students' general lack of security awareness and also correlates with the result obtained in our study where students did not consider themselves responsible for online and physical security but rather placed this expectation on the school or workplace.

Students' awareness on both online and physical security should be considered carefully for one of the major concerns with BYOD is security (Dhingra, 2016) and the security awareness is a critical factor to determine the outcomes of BYOD implementation. As mentioned by Katsikas (2000), awareness is the first step of learning followed by training and education. A lack of security awareness will fail students or future employees to complete subsequent training and education which will impose a critical security threat on educational institutions and workplaces. Thus, future BYOD policies should be considered not only to improve online or physical securities but also to escalate user security awareness in order to maximize the benefits of BYOD.

There was no significant difference observed between male and female participants in terms of their perceptions of BYOD. From the previous study conducted by Lim and Meier (2011), gender difference was observed on computer usage preference. Whether this reported gender difference can produce different attitudes towards BYOD still needs further clarification. That

no gender difference was observed in our study could be on account of the fact that the presence of class rules set by professors underlining internet access would be limited and that focus would be more on formal learning. This conjecture aligns with Johnson (2011) who reported a difference in home-based internet use but no difference in school-based use.

Another finding that is worth mentioning as part of results was that there were different levels of trust in online security between graduate and undergraduate students. Masters students apparently have more trust in cyber-security issues both at school and workplace. Whether this is due to the education level or other factors, such as the amount of time spent on the school premises or life experience, calls for further investigation. Based on this observation, it is recommended that schools or workplaces adjust BYOD security policies accordingly for education level and work experience.

Along with that our survey participants believed that accessing social media is more inappropriate at school than at work. This could be due to possible distractions caused by social media, as was mentioned amongst one of the concerns with BYOD in a previous study by Cheng (2016). As such, utilizing social media for BYOD at school might increase potential risk factors for learning whereas it can be considered more flexibly at workplace.

This study highlights various aspects of students' perception of BYOD at school and at workplace, but further study is required to extend our current understanding. Conducting the same survey in other South Korean universities will inflate the sample size and further clarify the findings of this study. At the same time, current employees' perception of BYOD could also be inquired into as a source for comparison to the results obtained from students. After all, successful implementation of BYOD will depend on continuous effort to investigate user perceptions and reflect them accordingly on BYOD policies and procedures. As suggested in this study, there are various factors to take into account for BYOD implementation which includes dependency on personal devices, security awareness, gender difference, education level, and access to social media. It is believed that the outcomes of this study can be utilized to produce BYOD regulations suitable for each educational institution or workplace in near future.

References

Armando, A., Costa, G., & Merlo, A. (2013, March). *Bring your own device, securely*. Proceedings of the 28th annual ACM Symposium on Applied Computing, Coimbra, Portugal.

Beckett, P. (2014). BYOD-popular and problematic. *Network Security, 2014*(9), 7-9.

Blaschke, L.M. (2018). Self-determined learning (Heutagogy) and digital media creating integrated educational environments for developing lifelong learning skills, in Kergel D., Heidkamp B., Telléus P., Rachwal T., Nowakowski S. (Eds.). *The Digital Turn in Higher Education*, Springer, Wiesbaden, VS, pp. 129-140.

Bring your own Device (BYOD) for Learning (2017). *PDST (Promoting and supporting the integration of ICT in education) Technology in Education*. Retrieved from https://www.pdsttechnologyineducation.ie/en/Technology/Advice-Sheets/Bring-your-own-Device-BYOD-for-Learning.pdf

BSI Group (2015). *Bring Your Own Device (BYOD) - An information security and eDiscovery analysis: A Whitepaper*. Retrieved from https://www.bsigroup.com/globalassets/localfiles/en-us/whitepapers/byod-info-sec-and-edisco-analysis.pdf

Cardoza, Y., & Tunks, J. (2014). The bring your own technology initiative: An examination of teachers' adoption. *Computers in the Schools, 31*, 293–315.

Cheng, G., Guan, Y., & Chau, J. (2016). An empirical study towards understanding user acceptance of bring your own device (BYOD) in higher education. *Australasian Journal of Educational Technology, 32*(4), 1-17.

Clifford, M. (2012). Bring your own device (BYOD): 10 reasons why it's a good idea. Retrieved from http://www.opencolleges.edu.au/informed/trends/bring-your-own-device-byod-10-reasons-why-its-agood-idea/

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science, 78*, 179-184.

Downer, K. & Bhattacharya, M. (2015). *BYOD Security: A New Business Challenge*. Proceedings of the 5th International Symposium on Cloud and Service Computing (SC2 2015), IEEE CS Press. doi: 10.1109/SmartCity.2015.221

Falloon, G. (2015). What's the difference? Learning collaboratively using iPads in conventional classrooms. *Computers & Education, 84*, 62-77.

Fraenkel, J. R., & Wallen, N. E. (2000) *How to Design and Evaluate Research in Education*. (4th ed.). McGraw-Hill, New York.

Garba, A. B., Armarego, J. & Murray, D. (2015). Bring your own device organisational information security and privacy. *Journal of Engineering and Applied Sciences, 10*(3), 1279-1287.

Harris, M. A., Patten, K., & Regan, E. (2013). *The Need for BYOD Mobile Device Security Awareness and Training*. Paper presented at Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, United States, August 15-17, 2013. Retrieved from https://pdfs.semanticscholar.org/3c49/f54f096685f285357edd76dc6316f04a275e.pdf

Hershatter, A., & Epstein, M. (2010). Millennials and the world of work: An organization and management perspective. *Journal of Business and Psychology, 25*(2), 211–223.

Hopkins, N., Sylvester, A., & Tate, M. (2013). Motivations for BYOD: An investigation of the contents of a 21st century school bag. Paper presented at the 21st European Conference on Information Systems, Utrecht, Netherlands. Retrieved from http://aisel.aisnet.org/ecis2013_cr/183

Johnson, B. & Christensen, L. (2004). *Educational Research: Quantitative, Qualitative and Mixed Approaches*. (2nd ed.). Pearson Publication: Boston.

Johnson, G. M. (2011). Internet activities and developmental predictors: Gender differences among digital natives. *Journal of Interactive Online Learning, 10*(2), 64-76.

Katsikas, S. K. (2000) Health care management and information systems security: Awareness, training or education? *International Journal of Medical Informatics, 60*, 129–135.

Kong, S. C., & Song, Y. (2015). An experience of personalized learning hub initiative embedding BYOD for reflective engagement in higher education. *Computers & Education*, *88*, 227-240.

KOSIS [국가통계포털]. *Korean Statistical Information Service*. Retrieved from http://kosis.kr/statHtml/statHtml.do?orgId=115&tblId=TX_115_2009_H4479&vw_cd=MT_ZTITLE&list_id=115_11528_002_006&seqNo=&lang_mode=ko&language=kor&obj_var_id=&itm_id=&conn_path=MT_ZTITLE

Lim, K. & Meier, E. B. (2011). Different but similar: Computer use patterns between young Korean males and females. *Educational Technology Research and Development, 59*(4), 575-592.

McLean, K. J. (2016). The Implementation of Bring Your Own Device (BYOD) in Primary [Elementary] Schools. *Frontiers in psychology*, *7*, 1739. doi:10.3389/fpsyg.2016.01739

Putri, F. F. & Hovav, A. (2014). *Employees´ compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory*. Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel, June 9-11, 2014. Retrieved from http://aisel.aisnet.org/ecis2014/proceedings/track16/2

Rackley, R., & Viruru, R. (2014). Preparing teachers for the BYOD classroom. In M. Searson & M. Ochoa (Eds.), Proceedings of Society for Information Technology & Teacher Education International Conference 2014 (pp. 2608-2613). Chesapeake, VA: Association for the Advancement of Computing in Education.

Song, Y. (2014). "Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school. *Computers & Education, 74*, 50–60.

Taneja, A., Fiore, V., & Fischer, B. (2015). Cyber-slacking in the classroom: Potential for digital distraction in the new age. *Computers & Education, 82*, 141-151.

Ubene, O.-I. E., Agim, U. R., & Umo-Odiong, A. (2018). The impact of Bring Your Own Device (BYOD) on information technology (IT) security and infrastructure in the Nigerian insurance sector. *American Journal of Engineering Research (AJER), 7*(5), 237-246.

Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., Grant, G., & Pittayachawan, S. (2018). Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives. *Information Systems Frontiers*, 1-17.