Bring your own device philosophy from the user's perspective: an empirical investigation

Chountalas, Panos and Karagiorgos, Athanasios

Hellenic Open University, School of Social Sciences

2015

BRING YOUR OWN DEVICE PHILOSOPHY FROM THE USER'S PERSPECTIVE: AN EMPIRICAL INVESTIGATION

Panos CHOUNTALAS
Hellenic Open University
School of Social Sciences
Parodos Aristotelous 18, 26 335, Patra
Contacting author e-mail: pchountalas@gmail.com

Athanasios KARAGIORGOS
Hellenic Open University
School of Social Sciences
Parodos Aristotelous 18, 26 335, Patra
e-mail: thanassisk@gmail.com

Abstract

Bring Your Own Device (BYOD) is a new trend topic, the IT management has to deal with. It enables the employees to use their own smart phones, tablets or other IT devices for business purposes (i.e. to access corporate applications or manage corporate data). Today, there is a considerable increase in organizations adopting the BYOD philosophy and consequently the debate about the costs, gains and risks is in full swing. The purpose of this study is to provide insights into the use of the BYOD philosophy, in terms of its perceived benefits and threats. To attain our goal, an empirical investigation was conducted of 156 BYOD's users. The results of this study indicate that BYOD is considered as a fairly innovative philosophy that brings some substantial benefits, such as an increase on both the mobility and flexibility at work. On the other hand, upon the use of BYOD, employees seem to be highly concerned about the privacy of their data. They are also afraid that they will be forced to work beyond their normal working hours. Since BYOD's use was typically perceived as non-complex, most employees stated that they were attracted by organizations that adopt the BYOD philosophy. This indicates that, as far as the employees are concerned, the BYOD's benefits outperform the threats.

Keywords: Bring Your Own Device (BYOD); IT management; mobile marketing; innovativeness; flexibility at work; privacy of data.

Please cite as: Chountalas P. & Karagiorgos A. (2015). Bring Your Own Device philosophy from the user's perspective: An empirical investigation. *Proceedings of the 2nd HOBA International Conference - Vol.1* (ISBN: 978-960-538-950-5). Patras, March 7-8, 1-12.

BRING YOUR OWN DEVICE PHILOSOPHY FROM THE USER'S PERSPECTIVE: AN EMPIRICAL INVESTIGATION

1. INTRODUCTION

Over the last years, the smart-phones and mobile computers (tablets or laptops) have changed the way that we live and work. The extensive use of mobile as a promotion tool highlights, not only its importance, but also the need for its more professional incorporation into marketing strategies. As a result, a new trend has emerged in business environments, widely known by the term "Bring Your Own Device" (referred hereafter as BYOD). BYOD is a philosophy which enables the employees to use their own IT devices for business purposes under the supervision of an IT department.

During the last few years, a considerably vast body of research has emerged, addressing various aspects of this topic, namely:

- Its perceived benefits (e.g. Morrow, 2012; Scarfo, 2012; Singh, 2012; Thomson, 2012; Yang et al., 2013; Thielens, 2013; Romer, 2014; Koh et al., 2014).

- Its perceived threats (e.g. Morrow, 2012; Scarfo, 2012; Miller et al., 2012; Astani et al., 2013; Ghosh et al., 2013; Tokuyoshi, 2013; Romer, 2014; Song & Lee, 2014; Crossler et al., 2014).

- Its practical implementation (e.g. Morrow, 2012; Scarfo, 2012; Miller et al., 2012; Oliver, 2012; Thomson, 2012; Astani et al., 2013; Ghosh et al., 2013; Tokuyoshi, 2013; Bell, 2013; Seigneur, 2013; Romer, 2014; Song & Lee, 2014; de Waard, 2014; French et al., 2014; Imazeki, 2014).

The purpose of this study is to provide further insights into the use of the BYOD philosophy and especially focuses on its perceived benefits and threats. The remainder of this paper is organized as follows. Section 2 provides the theoretical background of the BYOD philosophy. In this context, a definition is given and several other issues are presented under the light of the related literature (i.e. benefits for end users and business; implementation challenges; strategy and policy; and proposed steps to manage BYOD). Section 3 briefly introduces the research methodology. In Section 4 the research results are presented and analyzed. Finally, in Section 5 some final conclusions are given and further research recommendations are proposed.

2. BRING YOUR OWN DEVICE PHILOSOPHY

BYOD is a strategy that allows employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data and information exclusive to the company they work for (Gartner Inc., 2013). According to Gali et al. (2014), this evolutionary trend has the potential to redefine the relationship between employee and the IT department.

The definition of “Bring Your Own Device” is well documented in literature, however the term "Device" is often described in various ways. Specifically, in some cases "Device" is

narrowly linked only with smart-phones or tablets. But, in other cases its meaning can be extended, so as to include notebooks, printers or even hotspots.

In this section, BYOD's theoretical background is given, focusing on:

- The benefits for end users and business
- The implementation challenges
- The BYOD's strategy and policy
- The proposed steps to manage BYOD

2.1 Benefits for end users and business

It is widely believed that the major advantages derived from the implementation of BYOD philosophy is the higher productivity which stems from the improved employee satisfaction and worker mobility. Below, we present the major benefits from the implementation of BYOD philosophy both for end users and business:

- Increased productivity: Nowadays, many employees interact or respond to business tasks even if they are either away from their office or they find themselves outside of work hours. BYOD strategy provides the flexibility and the mobility to respond immediately to requests even if the employees are not working at that specific moment. This flexibility reduces the processing time and improves operational efficiency. It seems that many employees today do check their business email or perform any other kind of work after work hours, even on weekends or on vacation (Scarfo, 2012; Singh, 2012; Osterman Research Inc., 2013; Yang et al., 2013; Romer, 2014).

- Lower Corporate IT costs: With BYOD strategy, an organization can reach high cost savings, simply because employees carry the cost of purchasing, maintaining and upgrading their own devices that they use for work. Though BYOD strategy imposes a one-time, upfront investment to create an appropriate infrastructure to support the different devices, it can result in lower overall total cost of ownership in the long run (Scarfo, 2012; Cognizant, 2012).

- Employees are more efficient and satisfied: Efficiency is often reported as a direct outcome of BYOD implementation (Morrow, 2012; Singh, 2012; Thomson, 2012; Yang et al., 2013; Koh et al., 2014). According to Citrix Systems Inc. (2012), due to BYOD strategy, employees report higher satisfaction levels with such flexibility and mobility and even more the freedom to use private devices of their choice. It is found that 61% of companies that allow employees to use their private mobile device, experience higher employee satisfaction.

- Attracting, retaining and supporting new talent: It is believed that the majority of millennials that are going soon to become the key workforce of many companies are attracted from work places which allow them to use any tool or technology customized to their work and life preferences (Singh, 2012; Thomson, 2012; Cognizant, 2012; Thielens, 2013).

- Improved collaboration: Private owned devices equipped with improved mobile services allow employees to respond in real time and finish their tasks efficiently.

With virtualization, unlimited access to corporate data at anytime from anywhere and the development of innovative mobile applications, the opportunities for collaborative ways of working considerably grew (Thomson, 2012; Cognizant, 2012; Romer, 2014).

- Transforming the workplace: A modern IT infrastructure consists of cloud computing and application virtualization. Such an infrastructure, combined with managed personal devices, could provide access to the essential corporate resources for the employees, anytime, anywhere and in the most secure manner (Cognizant, 2012).

2.2 Implementation challenges

Without a doubt, the adoption of the BYOD strategy results in many challenges and difficulties as regards the IT department. Firstly, the vast choice of mobile devices, such as smart-phones and tablets, can create complexities regarding the management of these devices and as a consequence it can lead to challenges as security and data protection is concerned. Moreover, the support of all these different devices can cause significant rising costs. Below you will find the major challenges considering the implementation of BYOD strategy:

- Protecting data: The employees' private devices, as all the other corporate mobile resources, are very easy to get lost or theft because of their small size and high value. Most organizations provide policies in order to protect the corporate hardware. Thus, applications like Mobile Device Management (MDM) are adopted in order to track the lost personal devices, to wipe the sensitive corporate data that are stored on them and to lock unauthorized users (Cognizant, 2012; Ghosh et al., 2013; Astani et al., 2013; Song & Lee, 2014; Romer, 2014).

- Security: The fundamental danger of BYOD philosophy is that the private owned devices can access and store corporate data. Security policies should be implemented from the IT department even if the disparity of devices makes it particularly difficult. Moreover, the advanced features of the new intelligent devices, such as high definition cameras, recording functions and large storage capacity, can outguess many traditional IT security measures. Organizations that operate in regulated environments can ensure the security for private owned devices by adopting solutions that provide containerization of corporate environment (Miller et al., 2012; Morrow, 2012; Scarfo, 2012; Cognizant, 2012; Ghosh et al., 2013; Tokuyoshi, 2013; Romer, 2014).

- Support: Another challenge for the IT department is to provide support to the different mobile devices that are used by employees and at the same time to reduce the support costs. Thus, IT departments should allocate the appropriate resources, so as to implement the changes needed to effectively support BYOD (Morrow, 2012; Cognizant, 2012).

- BYOD costs: Companies may not save money if they do not adopt a certain policy and decide for example to repay their employees' mobile expenses. A strict expenditure policy with expense reporting should be adopted in order to invest in

solutions that provide mobile management and support for different devices (Cognizant, 2012).

- Compliance requirements: Companies should comply with a growing number of governance obligations. These obligations are focused on the archiving and safeguarding data, regardless of the device on which those data are stored. These governance requirements apply to any platform used by an organization, including those that are owned by the employees (Morrow, 2012; Cognizant, 2012; Crossler et al., 2014).

2.3 BYOD's strategy and policy

The most crucial issue, in order to adopt a BYOD strategy is to understand employee activities and how their tasks are related to the use of mobile devices. Firstly, organizations should group users into major categories considering the kind of work they perform on a daily basis and the related IT requirements they have. For this reason, a lot of companies enroll BYOD strategy initially only to qualified employees such as upper-level managers. The organization should take into consideration the nature of the business and industry in which it operates in order to identify how the strategy can stay compliant, especially on data security and usage commands. The organizations should also define the kind of device configurations, even more the suggested vendors that support the employees' business needs.

An important discussion should also be made by the organizations, regarding the balance between the adoption of BYOD strategy and the management control of the mobile devices. In this context, the organizations should decide whether they will manage the mobile devices in-house or hire an outsourcing vendor to take over this task.

Another key factor to employ BYOD strategy is its set-up cost. The organizations should calculate thoroughly the initial costs of setting up a new infrastructure for providing support to different devices and platforms. Organizations should also define the liability and scalability they are willing to receive and further calculate the ROI of such an investment. Finally, they should take into consideration tax and legal implications that may arise by the adoption of BYOD strategy, especially when they compensate employees for their expenses.

Support is another critical aspect of BYOD strategy because employees need anytime-anywhere access to a helpdesk. Regarding this kind of support, companies should integrate enterprise applications with certain mobile devices. The support should also include the customization, developing and updating applications in these private devices. It is crucial that a mix of sourcing, automation and technical customer support is needed in a solid BYOD support model. An agreement between IT departments and cooperative business units regarding the approach that they should follow for the BYOD program, will lead to a successful strategy.

According to Cognizant (2012), companies should consider a middle path between the two extremes, of the complete freedom that employee's desire and the full control that organizations seek over personal device work usage. A flexible and scalable strategy will

better facilitate the growing demand for BYOD, given the rapidly evolving device technology environment.

Implementing the BYOD strategy is only possible with a comprehensive policy. To develop an effective policy, organizations need to determine and understand some major factors regarding the devices and operating systems that they will support, the security requirements, the acceptable risk that are willing to take, etc. (for an in depth discussion regarding BYOD's strategy and policy, see Oliver, 2012; Cognizant, 2012; Astani et al., 2013; Bell, 2013).

2.4 Steps to manage BYOD

According to Osterman Research Inc. (2013), there are five steps any organization should follow in its attempt to manage BYOD:

- Understanding of benefits and risks: First, the extent of penetration of this trend into organizations needs to be fully understood. Even though most senior managers suppose that some of their employees are using personally owned smart-phones and tablets in work, they need to understand exactly what types of corporate data they are using (either for access or store), and the reasons to do so (see also Thomson, 2012; Morrow, 2012; Seigneur, 2013).

- Evaluating the options: Both IT and HR should examine their options for managing BYOD. The available options considering the adoption of BYOD can range from doing nothing (as the one extreme) to implementing draconian controls so as to eliminate the use of personally owned devices for purposes related to business tasks (as the other extreme). While some managers may decide to implement strict policies in order to protect corporate data or reduce the potential for malware penetration, they are highly advised to adopt a more open attitude (see also de Waard, 2014; Imazeki, 2014).

- Implementing protection policies: It is critically important for organizations that adopt BYOD strategy to implement detailed policies regarding the acceptable usage. As a best practice, most companies create a list of devices and operating systems that the employees are allowed to use. These policies should be detailed and thorough and should be part of a wider organizations' policy regarding the use of corporate resources. The major element of such a policy applied to mobile devices should be that: (a) any mobile device must be able to be wiped out by the IT department in the event of its loss, and (b) all devices that contain corporate content should be encrypted to prevent the leak of sensitive data. Corporate policies focused on employee-managed applications should also include requirements for the encryption of data stored in a third party’s cloud data center (see also Miller et al., 2012; Morrow, 2012; Scarfo, 2012; Ghosh et al., 2013; Tokuyoshi, 2013; Romer, 2014).

- Training users: It very important to train users on the best practices, as regards accessing and managing corporate data on private owned devices. Eventually, all employees should become aware of the dangers that can occur if corporate data are

not adequately protected or, even worse, are lost (see also Astani et al., 2013; French et al., 2014).

- Deploying the appropriate technologies: Finally, it is vitally important for the organizations to deploy technologies, such as Mobile Device Management (MDM), in order to manage the corporate risk efficiently (see also Ghosh et al., 2013; Astani et al., 2013; Song & Lee, 2014; Romer, 2014).

3. METHODOLOGY

As mentioned before, the purpose of this study was to provide insights into the use of the BYOD philosophy, mainly in terms of its benefits and threats, as perceived by employees who already use BYOD. Note that the present research was mostly inspired by the previous work of Loose et al. (2013).

The research was conducted using questionnaires distributed among employees working in financial, marketing or information technology departments in organizations operating in Greece. Seven critical variables were constructed, each consisted of a distinct batch of questions (namely: innovativeness; work performance; complexity; threats; employer attractiveness; future potential; IT experience). A 5-point Likert Scale was used to measure all variables' values. In order to create a common understanding for the term "BYOD", a definition was provided at the very beginning of the questionnaire. Some demographic questions were asked at the end of the questionnaire, as regards the respondents' gender, age and education level.

A pre-test (pilot) was performed based on a small sample. No serious flaws were identified via pre-test, though minor corrections had been made in order to improve the intelligibility of the questionnaire. After fine-tuning the questionnaire, all potential participants were informed about the study. They received the questionnaire's web-link via e-mail and after a three weeks time, 156 valid questionnaires were returned completed.

As regards the data analysis and results presentation, it was performed in three subsequent levels:

i. The first level involved the descriptive analysis of the critical variables used in the research and their constituent items. One sample t-test was used to examine whether the mean value of each variable was significantly different from the mid-point of 3.
ii. The second level involved the testing of three regression models, in order to examine possible effects among the critical variables.
iii. The third level involved the investigation of the participants' demographic characteristics role in influencing the critical variables. Six regression models were tested for this purpose.

Note that, in the coefficients analysis, no tolerance value was found below 0.60 and all VIF values were found to be lower than 1.70.

Several conclusions were drawn from all levels of analysis, as presented in the next section.

4. RESULTS

The demographic analysis of the sample shows that it consisted of 56% males and 44% females. The vast majority held a Bachelor's or Postgraduate degree, and circa 2/3 of them were under 35 years old. Regarding the main media for the implementation of the BYOD philosophy, it was noticed that nearly 80% of the respondents used a smart-phone, 70% used a laptop and 40% used a tablet. The above characteristics indicate that the sample was primarily consisted of young and well-educated employees who were very familiar with new technologies.

In Table 1 the variables used in the present study are introduced. For each variable a definition is provided, along with the number of its constituent items. Regarding internal consistency, as measured by Cronbach's Alpha, it is obvious that five variables were found clearly above the threshold of .80, while the other two (i.e. IT Experience and Future Potential) also maintained acceptable values.

Table 1: Variables used in the empirical survey

Variables	Definition	Items	Cronbach's Alpha
Innovativeness	Respondents' perception regarding BYOD's level of innovativeness.	3	.913
Work Performance	Respondents' perception regarding BYOD's contribution to work performance.	6	.913
Complexity	Respondents' perception regarding BYOD's level of intrinsic complexity.	4	.910
Threats	Respondents' perception regarding the level of possible threats associated with BYOD's use.	9	.888
Employer Attractiveness	Respondents' perception regarding the level of attractiveness of an employer that adopts the BYOD philosophy.	3	.829
Future Potential	Respondents' perception regarding BYOD's future potential in business.	6	.660
IT Experience	Respondents' experience on IT use (self-assessment).	5	.549

Examining the above mentioned variables, at a first descriptive level, we drew the following conclusions, as regards BYOD:

i. It is considered as a fairly innovative philosophy by most participants ($m=3.82$; $t=10.338$, $p<0.001$).
ii. It is perceived to increase both the mobility ($m=4.00$; $t=14.195$, $p<0.001$) and flexibility ($m=3.96$; $t=12.739$, $p<0.001$) at work.
iii. It does not seem to influence motivation at work ($m=3.14$; $t=1.740$, $p>0.05$).
iv. Its use is not considered as complex in general ($m=2.28$; $t=-9.590$, $p<0.001$), though some participants may request additional help sometimes ($m=3.23$; $t=2.357$, $p<0.05$).
v. It drives employees to be highly concerned about the privacy of their data ($m=3.50$; $t=5.254$, $p<0.001$).

vi. It makes employees more afraid that they will be forced to work beyond their normal working hours (m=4.06; t=11.275, p<0.001).
vii. It does not seem to raise worries about losing business (m=2.64; t=-4.258, p<0.001) or private (m=2.77; t=-2.244, p<0.05) data.
viii. It generally attracts employees to use it, if it is offered as an option by their employer (m=3.58; t=7.323, p<0.001).
ix. It is commonly expected to evolve as a mandatory practice in the future (m=3.92; t=11.526, p<0.001).

At a second level, we tested whether innovativeness, future potential, complexity and threats affect work performance (Model 1.1) and employer attractiveness (Model 1.2). The first three variables were also examined as possible predictors of threats (Model 1.3). The main results are presented in Table 2.

Table 2: Regression results

	Model 1.1	**Model 1.2**	**Model 1.3**
Variables	**Work Performance**	**Employer Attractiveness**	**Threats**
Innovativeness	0.318***	0.454***	0.138
Future Potential	0.531***	0.395***	-0.102
Complexity	-0.114	0.083	0.486***
Threats	0.104	-0.038	
R^2	*0.587*	*0.579*	*0.216*
F	*53.751****	*51.977****	*13.943****

*Standardized regression coefficients are shown; * p<0.05; ** p<0.01; *** p<0.001.*

From Table 2, it can be concluded that:

i. The employees, who perceive BYOD as a highly innovative philosophy and see its bright future potential in business, are more likely to anticipate BYOD to greatly enhance their own work performance. These employees also tend to be more attracted by organizations that adopt the BYOD philosophy (see Models 1.1 & 1.2).
ii. The employees, who find BYOD rather complex, tend to identify more possible threats associated with its use. Nevertheless, these employees do not seem to avoid organizations that adopt the BYOD philosophy, as it might have been expected (see Models 1.2 & 1.3).

At a third level, we examined whether the participants' demographic characteristics (i.e. gender, age, education level and IT experience) affected the variables at hand.

Table 3: Effects of demographic characteristics

	Model 2.1	**Model 2.2**	**Model 2.3**	**Model 2.4**	**Model 2.5**	**Model 2.6**
Variables	**Innovativeness**	**Work Performance**	**Complexity**	**Threats**	**Employer Attractiveness**	**Future Potential**
Gender	0.225**	0.259**	-0.045	-0.105	0.103	0.240**
Age	0.149	0.074	-0.109	-0.038	0.099	0.132
Education	-0.164*	-0.212**	-0.167*	0.243**	-0.309***	-0.243**
IT Experience	0.129	0.371***	0.014	-0.027	0.016	0.461***
R^2	*0.113*	*0.219*	*0.041*	*0.077*	*0.120*	*0.317*
F	*4.795***	*10.613****	*1.612*	*3.159**	*5.157***	*17.510****

*Standardized regression coefficients are shown; * p<0.05; ** p<0.01; *** p<0.001.*

The main conclusions drawn from Table 3, are presented below:

i. Women acknowledge BYOD's innovativeness in a higher degree, compared to men (see Model 2.1; $t=2.694$, $p<0.01$).
ii. Women anticipate BYOD to enhance their own work performance in a higher degree, compared to men (see Model 2.2; $t=3.321$, $p<0.01$).
iii. Men and women do not significantly differ in terms of acknowledging BYOD's perceived complexity (see Model 2.3; $t=-0.527$, $p>0.05$) and threats (see Model 2.4; $t=-1.251$, $p>0.05$).
iv. Age does not seem to play a significant role in all hypotheses tested (i.e. against Innovativeness, Work Performance, Complexity, Threats, Employer Attractiveness and Future Potential).
v. Less-educated employees acknowledge BYOD's innovativeness in a higher degree, compared to the well-educated (see Model 2.1; $t=-2.061$, $p<0.05$).
vi. Less-educated employees anticipate BYOD to enhance their own work performance in a higher degree, compared to the well-educated (see Model 2.2; $t=-2.855$, $p<0.01$).
vii. Less-educated employees find BYOD more complex, compared to the well-educated (see Model 2.3; $t=-2.049$, $p<0.05$).
viii. Well-educated employees identify more possible threats associated with BYOD's use, compared to the less-educated (see Model 2.4; $t=3.033$, $p<0.01$).
ix. Less-educated employees are more attracted by organizations that adopt the BYOD philosophy, compared to the well-educated (see Model 2.5; $t=-3.950$, $p<0.001$).
x. More IT-experienced employees are the ones that mostly anticipate BYOD to enhance their own work performance (see Model 2.2; $t=4.880$, $p<0.001$) and also see a brighter future potential for BYOD in business (see Model 2.6; $t=6.445$, $p<0.001$).
xi. IT experience does not seem to influence the perceived BYOD's level of innovativeness (see Model 2.1; $t=1.589$, $p>0.05$) or employer attractiveness (see Model 2.5; $t=0.196$, $p>0.05$).

5. CONCLUSIONS

The purpose of this study was to provide insights into the use of the BYOD philosophy, mainly in terms of its perceived benefits and threats. In this context, an empirical research was undertaken in order to examine the perceptions of employees who were already using BYOD. The data analysis was based on 156 valid questionnaires.

From the research results, several conclusions were drawn. First, it seems that BYOD is perceived to increase the mobility and flexibility at work. At the same time, some threats were identified, namely the data privacy infringement and the extension of working hours. In general, the employees who anticipate the potential contribution that BYOD might make in enhancing their own work performance, are more likely to be attracted by organizations that adopt the BYOD philosophy. However, the employees who find it difficult to use BYOD, tend to perceive more threats than benefits when their organization offers this option. Furthermore, it was examined whether any demographic characteristics influenced the critical variables of this research. It can be concluded that the gender and the education level do influence variables such as Innovativeness and Work Performance.

A limitation of the present study concerns employees, most being relatively young and well-educated. This was expected since the sample was exclusively constituted of BYOD users. Thus, the conclusions cannot be generalized to the whole population of employees. As a continuation of this study, it would be interesting to investigate the perceptions of non-users on all issues examined here. Subsequent comparisons between BYOD users and non-users could shed more light on the issue at hand.

REFERENCES

Astani, M., Ready, K. and Tessema, M. (2013). BYOD issues and strategies in organizations. *Issues in Information Systems* 14(2): 195-201.

Bell, M. (2013). Considerations When Implementing a BYOD Strategy. *IS Practices for SME Success Series*: 19-22.

Citrix Systems Inc. (2012). Best practices to make BYOD simple and secure. White Paper, viewed 20 February 2015, <http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf>

Cognizant (2012). Making BYOD Work for Your Organization. White Paper, viewed 20 February 2015, <http://www.cognizant.com/InsightsWhitepapers/Making-BYOD-Work-for-Your-Organization.pdf>

Crossler, R.E., Long, J.H., Loraas, T.M. and Trinkle, B.S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems* 28(1): 209-226.

de Waard, I.I. (2014). Using BYOD, mobile social media, apps, and sensors for meaningful mobile learning. *Increasing Access*: 113.

French, A.M., Guo, C. and Shim, J.P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems* 35(1): 10.

Gali, M.A., Barayuga, V.J. and Yu, W.E. (2014). BYOD: Connectivity Option for Alaminos City Hall. *International Conference on challenges in IT, Engineering and Technology (ICCIET'2014) July 17-18, 2014 Phuket (Thailand)*: 31-38.

Gartner Inc. (2013). Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013. Press Release, viewed 20 February 2015, <http://www.gartner.com/newsroom/id/2408515>

Ghosh, A., Gajar, P.K. and Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science* 4(4): 62-70.

Imazeki, J. (2014). Bring-Your-Own-Device: Turning Cell Phones into Forces for Good. *The Journal of Economic Education* 45(3): 240-250.

Koh, E.B., Oh, J. and Im, C. (2014). A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. *Proceedings of the International MultiConference of Engineers and Computer Scientists 2014*: 12-14.

Loose, M., Gewald, H. and Weeger, A. (2013). Determinants of Bring-Your-Own-Device (BYOD) Adoption from the Perspective of future Employees. HNU Working Paper Nr. 25, University of Applied Sciences, Neu-Ulm, Germany, viewed 20 February 2015, < http://publikationen2.hs-neu-ulm.de/HNU_WP25_Gewald_BYOD.pdf>

Miller, K.W., Voas, J. and Hurlburt, G.F. (2012). BYOD: Security and privacy considerations. *It Professional* 5: 53-55.

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security* 2012(12): 5-8.

Oliver, R. (2012). Why the BYOD boom is changing how we think about business it. *Engineering & Technology* 7(10): 28.

Osterman Research Inc. (2013). Putting IT Back in Control of BYOD. White Paper, viewed 20 February 2015, < http://www.slideshare.net/HyperOffice/byod-research-by-osterman>

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security* 2014(1): 13-15.

Scarfo, A. (2012). New security perspectives around BYOD. *Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, IEEE Computer Society*: 446-451.

Seigneur, J. M., Kölndorfer, P., Busch, M. and Hochleitner, C. (2013). A survey of trust and risk metrics for a BYOD mobile worker world. *SOTICS 2013, The Third International Conference on Social Eco-Informatics*: 82-91.

Singh, N. (2012). BYOD Genie Is Out Of the Bottle–"Devil Or Angel". *Journal Of Business Management & Social Sciences Research* 1(3): 1-12.

Song, M. and Lee, K. (2014). Proposal of MDM Management Framework for BYOD use of Large Companies. *International Journal of Smart Home* 8(1): 123-128.

Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security* 2013(8): 5-6.

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security* 2012(2): 5-8.

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security* 2013(4): 12-13.

Yang, T.A., Vlas, R., Yang, A. and Vlas, C. (2013). Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior. *International Conference on Social Computing (SocialCom)*: 411-416.