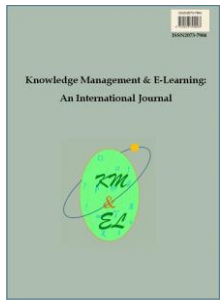
Knowledge Management & E-Learning, Vol.11, No.2. Jun 2019

"Bring your own device" policies: Perspectives of both employees and organizations

Kevser Gülnur Gökçe
Ozgur Dogerlioglu
Bogazici University, Turkey



Knowledge Management & E-Learning: An International Journal (KM&EL)
ISSN 2073-7904

Recommended citation:
Gökçe, K. G., & Dogerlioglu, O. (2019). "Bring your own device" policies: Perspectives of both employees and organizations. *Knowledge Management & E-Learning*, *11*(2), 233–246. https://doi.org/10.34105/j.kmel.2019.11.012

Knowledge Management & E-Learning, 11(2), 233–246

"Bring your own device" policies: Perspectives of both employees and organizations

Kevser Gülnur Gökçe

Department of Management Information Systems
Bogazici University, Turkey
E-mail: kevsergulnurar@gmail.com

Ozgur Dogerlioglu*

Department of Management Information Systems
Bogazici University, Turkey
E-mail: dogerlio@boun.edu.tr

*Corresponding author

Abstract: Bring Your Own Device (BYOD) policy, which allows employees to use their own mobile devices for work and connection to their corporate network, is getting popular in enterprises. While companies want to improve the efficiency and productivity of employees, employees prefer to use their own devices at work, which make them feel more comfortable and free. Although BYOD seems attractive, companies and employees have some security concerns in different and various ways. The aim of this study is to explore employee and organization perspectives about BYOD. Empirical part of the research has two parts: Qualitative and quantitative. Manager's opinions were determined through a series of interviews and then the findings were analyzed. In quantitative part, a questionnaire has been developed based on the literature review and qualitative findings. 12 interviews and 93 surveys were used in the analysis. It has been found that while organizations and employees percept BYOD as having benefits in many ways, their security and privacy concern is a strong barrier on the implementation of BYOD policy.

Keywords: Bring your own device; BYOD; Security; Privacy; IT policy

Biographical notes: Kevser Gülnur Gökçe has completed her MA degree in Management Information Systems program of Bogazici University. Her research interest is in knowledge management policies of organizations. She also works in finance industry as an information security analyst.

Dr. Ozgur Dogerlioglu is an Assistant Professor in Management Information Systems department of Bogazici University. Her research studies and published articles focus on the managerial and organizational impacts of Information Technology, learning organization, knowledge management, social networks and embeddedness, quality management and corporate culture. Strategic management, managerial communication and organizational impacts of Information Technology are the main subjects of the courses given by her. More details are available at http://www.mis.boun.edu.tr/en/team/ozgur-dogerlioglu-2

1. Introduction

Mobile devices play an essential role in people's lives for the need of easy and fast access to information (Botha, Furnell, & Clarke, 2009; Markelj & Bernik, 2015). As the life cannot be thought without them, the use of mobile devices for work is becoming very popular (Khan, Abbas, & Al-Muhtadi, 2015). Mobile devices offer a wide variety of functionalities including wireless technology, different types of applications, easy access and connection and therefore companies have started to give employees mobile devices in order to keep in contact with them after work hours (Shumate & Ketel, 2014). Nowadays employees want to use their own device for work and deciding whether or not permitting this request is a new problem for companies (Jaramillo et al., 2013).

Instead of using two devices for private and business applications, employees generally prefer using one device that may represent a proper solution. The result is "Bring Your Own Device" or BYOD, which means that employees make their own personal devices available for business purposes (Disterer & Kleiner, 2013). Employees can use their personally owned devices to access company resources such as email, file servers, and databases (Hayes & Kotwica, 2013). It is a very controversial subject in terms of managerial, technical and security concerns (Disterer & Kleiner, 2013; Tokuyoshi, 2013).

1.1. Advantages of BYOD for employees

Although allowing employees to bring and use their personal devices for work has some threats, it also brings some opportunities. The device used by employees for work should have ease of use not to lose motivation. People in the work place become much happier when they use their own phone which they like and know. Efficiency and production in the work environment rise with increased happiness (Cognini, Gagliardi, & Polzonetti, 2013). It also results in increased profits. Furthermore, employees can become more innovative because they can easily work together and share ideas any time and at any place (Waterfill & Dilworth, 2014).

Effectiveness and comfort: Employees can feel more comfortable when they access to enterprise network from anywhere, any time without any extra device or connection (Morrow, 2012; Thomson, 2012). They do not see it as extra workload when they work with their own device after work hours. Employees may not stay all day in the office and if they leave the office early, they may continue to work at any place which they feel themselves comfortable. This is also appreciated by managers for being able to keep employees performing for longer hours (Madzima, Moyo, & Abdullah, 2014).

Employees generally have complaints about company owned mobile devices since companies give them old technological devices because of budget constraints. It takes long time for companies to replace old fashion devices with new and higher technology ones. It is one of the reasons for employees to prefer BYOD as they do not want to have trouble with old corporate computing devices (Madzima et al., 2014). As employees can use their own devices more comfortably and connect the work environment whenever they want, they work more effectively (Zahadat et al., 2015).

1.2. Disadvantages of BYOD for employees

Although using their own devices leads perceptions of freedom and flexibility in terms of how, when, and where they can accomplish the work, it also leads to pressure on the

employees because of being always accessible and responsive to labor demands. BYOD creates stress and tension on users (Fujimoto et al., 2016).

Privacy concerns: BYOD can limit employees' activities on their own device with restrictive rules of the organization since BYOD device is used for both personal and business purpose. Users do not have right to choose which application can be downloaded and installed (Jaramillo, Ackerbauer, & Woodburn, 2014). They are also worried about their data privacy because company can access all the personal data for controlling the device remotely. Possibility of company access to their personal space make users feel irritated (Wang, Wei, & Vangury, 2014).

Information Technology (IT) department should cope with security and related managerial issues. Security solutions are especially important for protecting corporate data (Rhee et al., 2013; Porter, 2011). However, security solutions for organizational risks may create security risks for users.

Mobile Device Management (MDM) system is one of the options and it is a type of security software. MDM software permits administrators to control mobile devices as easily as desktop computers. It is preferred by organizations for monitoring smart devices' status and controlling them remotely in order to prevent any data leakage (Pogarcic, Gligora Markovic, & Davidovic, 2013). Enterprises are developing and adopting mobile device management systems in order to enhance the security of mobile devices. This type of software also handles the situation when the phone is lost or misused (Rhee, Jeon, & Won, 2012). Authentication rules, device settings are specified to limit the access to the corporate data. It also serves wiping feature if it is necessary (Chang, Ho, & Chang, 2014). MDM does not differentiate personal device and corporate area and it serves a common space for BYOD, it limits the user's freedom. As users cannot act as free as they want, it can be seen as a negative attribute by users (Wang et al., 2014). Application and desktop virtualization solutions are also used for helping to separate corporate network from unauthorized employee access (Dong et al., 2015). In this solution, users can access corporate network and data with remote access. Although user's area and corporate systems are separated from each other, some security policies should also be implemented to prevent any unauthorized data transfer (Ogie, 2016).

1.3. Advantages of BYOD for organizations

Organizations encourage BYOD because it has many advantages, such as reducing companies' cost and increasing users' productivity (Zahadat et al., 2015). Traditionally companies provide and manage devices for their employees while BYOD is less costly when compared to this traditional option. (Morrow, 2012; Scardilli, 2014). Organizations get rid of purchasing, maintenance and operational costs of company owned mobile devices. They become responsible for only configuring the connection between personal devices and company network (Shumate & Ketel, 2014; Ocano, Ramamurthy, & Wang, 2015). Increased flexibility, productivity, mobility and employee satisfaction are the main contributions of BYOD to organizations (Rivera et al., 2013).

1.4. Disadvantages of BYOD for organizations

Organizations may find the idea of allowing employees to use mobile devices attractive to keep employees satisfied in today's life conditions, but also, they face the risk of having corporate data unsecure (Morrow, 2012; Tokuyoshi, 2013). Another problem about BYOD is managing different types of devices. As the complaints differ for each

type of device, internal help desk or other departments can have troubles in solving specific problems (Cognini et al., 2013; Scardilli, 2014).

Security: Mobile devices that connect to enterprise networks significantly increase threats to sensitive data if the data is unencrypted (Morrow, 2012; Thomson, 2012). Especially mobile hot spots can be dangerous as data is sent via unsecured network (Shumate & Ketel, 2014). Nowadays, mobile devices become very attractive for hackers because it is not as safe as PCs because of unsecured Wi-Fi connection, less protective anti-virus system, jailbreak property and user ignorance. The operating system and application of devices may be affected by mobile threats involving exploits to take control of the whole system, or harmed part of the device (Madzima et al., 2014). Malware, viruses and malicious codes that open backdoor for attacks are also concerns for data leakage (Chang et al., 2014; Kim & Lee, 2014).

Due to the possibility of data loss caused by careless personnel, employees need to feel the responsibility of having corporate data in their mobile (Morrow, 2012; Lennon, 2012). They should know safe usage rules of mobile devices to avoid causing any security breach (Markelj & Bernik, 2015). They should also be aware of threat of phishing attacks that steal sensitive information from users with deceiving them (Arachchilage, Love, & Beznosov, 2016). Another subject taken into consideration is about employees who access confidential corporate data by their own device without any security precautions. It is challenging to prevent system and sensitive data from intentional damage of users. Security agreements including strict rules may be a solution to deter personnel from malicious act (Madzima et al., 2014).

Applications and information placed in mobile platforms must be protected from any threat that affects the integrity, availability and confidentiality of corporate data. In order to keep them safe, the policies about who may access and from where should be specified (Thomson, 2012). As organizations handle the drawbacks of BYOD, they need to take into consideration the security precautions to safeguard corporate data from both external and internal threats (Miller, Voas, & Hurlburt, 2012).

2. Research objectives

The purpose of this research is to study different perspectives of managers and employees on BYOD policy. Employee opinions affect company decisions because attitudes and thoughts of personnel are part of any implementation process in organizations. The research model shown in Fig. 1 assumes organizational perspective about BYOD policy to be a combination of managers' and employees' perspectives. Manager's perspective is clarified using qualitative method and quantitative approach is preferred for understanding employee perspective.

- Mobile devices have wide variety of functionalities for achieving work and non-work activities and let employees to continuously keep in touch with colleagues, families, and friends (Fujimoto et al., 2016). Using their own devices for work increases the motivation of employees and they begin to work more effectively (Shumate & Ketel, 2014). In hypothesis 1 the relationship between employees' BYOD perspectives and their effectiveness tendencies is tested:

H1: *When employees percept BYOD as having advantages more than disadvantages, they have a tendency for working more effectively with their own device when BYOD policy is implemented*

- New trending device models emerge each and every day with the rapid development of technology. Users want to get the blessings of technology for easier and quicker communication. Forcing the employees to use old-fashioned company owned devices mean restriction to their freedom (Madzima et al., 2014). Using the device they prefer and working with them make employees feel more comfortable and free (Shumate & Ketel, 2014). The hypothesis 2 is designed to check the relationship between employees' BYOD concept perceptions and their attitudes to connect comfort and BYOD:

H2: *When employees percept BYOD as having advantages more than disadvantages, they have a tendency to feel more comfort at work when BYOD policy is implemented*

- Whenever BYOD is discussed, the importance of organization's data security is considered more than the user's data privacy. However, the protection of user's data is also an important issue. As employees share the control of their own device and private information with BYOD, it seems risky for users (Madzima, et al., 2014). Companies should take the necessary actions to prevent the data leakage and mingle (Miller et al., 2012). Employees' risk perceptions and their opinions about BYOD concept is tested with hypothesis 3:

H3: *There is a relationship between the employees' privacy and security concerns about BYOD and employees' perceptions about BYOD as having advantages more than disadvantages*

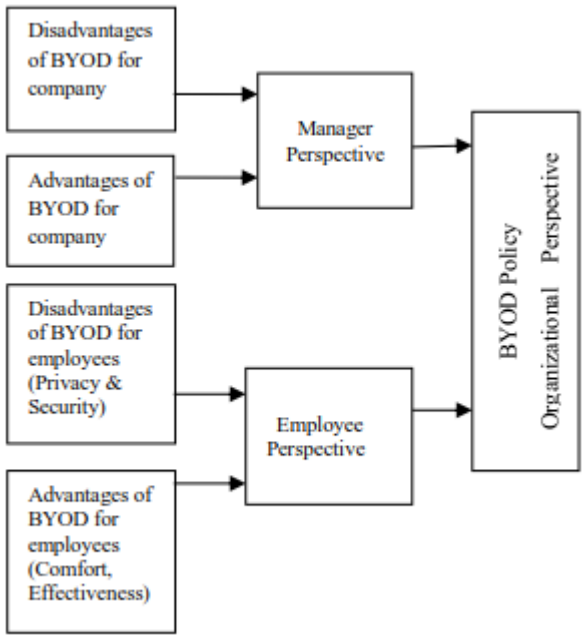


Fig. 1. Model for organizational perspective about BYOD policy

3. Methodology

3.1. Qualitative methodology

In order to learn their perspective about BYOD policy, managers who work in different sectors and departments were interviewed. The sectors have been chosen based on the relevance of mobility. The focus of the research was on the institutionalized and well-known companies because they follow technological developments closely. Small-sized enterprises are also included in the scope in order to compare them with larger firms and learn their attitude about the issue. The number of companies interviewed is 7 in 5 different sectors and 12 managers participated totally. Each interview lasted for 20-30 minutes and was done face to face or via phone with the managers. The questions were asked to understand company policies about BYOD, managers' own ideas and the general organizational needs and requirements about usage of personally owned devices. Managers were asked to evaluate necessity of BYOD in terms of the type and size of each sector, department and their own perspective. Answers and explanations of managers are categorized based on sectors.

3.2. Quantitative methodology

The target of the survey is to determine the perceptions of employees about BYOD policy and the main purpose is to observe the effect of independent variables related to advantages of BYOD such as effectiveness, comfort and privacy concerns.

Based on the literature survey and manager interviews a survey of 12 questions has been prepared. Survey includes 3 demographic questions, 5 multiple choice type and four 5-points Likert scale questions. The questionnaire is distributed to only working people in different sectors through online networks via e-mail, social networking sites and the offline network. Participants are informed about who is doing the research and what the research purpose is. SPSS version 21 is the software used for the analyses of quantitative data. Data has been collected from 93 respondents.

4. Results

The findings of qualitative part are based on manager opinions and according to the explanations of managers, the results are summarized with respect to sectors in Table 1.

For quantitative part, the results of reliability analyses are demonstrated in Table 2. The highest Cronbach's alpha belongs to effectiveness with 0.826 while the lowest Cronbach's alpha is 0.625 for comfort. These values indicate that variables used in the hypotheses tests are reliable.

Table 3 demonstrates answers of participants to the question starting with "if BYOD policy is implemented in my organization ……". When responses are analyzed based on "being able to access with personally owned device" or "being able to access with company owned device" 65% of respondents who "become happier", 49% of people who "feel freer" and 49% of people who "work more comfortably" already use their own devices at work. These findings are clear evidences of motivational strength and positive impact of BYOD.

Table 4 shows mean values of variables about effectiveness, comfort, privacy and security concerns. The mean values of variables in effectiveness dimension show that

respondents moderately support the idea of effectiveness increase when BYOD policy is implemented. On the other hand, it is obvious that employees are highly worried about all situations related to privacy and security issues. They have serious concerns especially about controlling their phone, company access to their photo and other private information.

Table 1
Summary of perspectives of different sectors about BYOD

	Finance (N=3) and Telecommunication (N=3) Sectors	Manufacturing and Service Sectors (N=3)	Small Enterprise (N=3)
Main Responsibility of the Sector	Finance and Telecommunication sectors collect and store large amounts of critical data about customers and stakeholders. They are responsible for being compliant to legal policy and standards about information security when using information technology.	Using information technology efficiently plays an important role for manufacturing companies in order to take fast decisions and responding customer quickly.	With only a limited number of applications, employees and customers, information technology is used for only running the business.
Security Concerns	Security is a vital issue because of processing and storage of critical customer data. Many concerns exist about implementing BYOD because of the risk of disclosure of corporate data.	Although they have critical corporate data their main concern is increasing customer satisfaction with rapid response. Managers believe that they can handle risks by taking related precautions like MDM, security software and anti-virus system.	Instead of developing their own information technology system; they have only one or two applications which are generally outsourced. So, it is easier to have secure systems when applying BYOD compared to other sectors.
Managers' General Attitudes	Managers generally support “company owned device” rather than” bring your own device”. They want to wait and see the day that advantages of BYOD are more than disadvantages of it.	BYOD is preferred by managers because of ease of use, easy adaptation and continuous availability of corporate data.	They are not interested in the advantages of BYOD. Availability of employees anytime and anywhere isn't so necessary for them because there isn’t too much work load.
Implementing BYOD	Before implementing BYOD, all security precautions are taken into account. IT and business departments should work together for BYOD implementation project in order to minimize related risks.	Almost all employees, but at least marketing and project departments should use BYOD with taking necessary security precautions. MDM should also be used for providing a more controlled system.	Managers say that it is better to implement BYOD when they become a larger company.

Table 2
Scale reliabilities

Scale	N	No. of items	Cronbach’s alpha
Effectiveness	93	2	0.826
Comfort	93	3	0.625
Privacy concern	93	4	0.741

Table 3
Responses to motivational strength statements (N=93)

Statements	# of Responses	%
I become happier	29	31
I produce innovative ideas	27	29
My productivity increases	32	34
I feel freer	51	55
It increases my communication with my co workers	22	24
My communication with my managers increases	20	22
I work more comfortably	53	57

Table 4
Mean values for the Effectiveness of employees when using BYOD, feeling comfortable with BYOD, privacy and security concerns about BYOD (N=93)

Variable	Mean*
Effectiveness	
My effectiveness in the work increases with accessing corporate data and applications from anywhere and anytime	3.37
I can finish the work in a shorter time if I have to work after work hours	3.41
Comfort	
I feel more comfortable if I use my phone	3.31
I have trouble with using company owned device	2.60
I dislike it when I have to carry both companies owned device and my own device	3.35
Privacy and security concerns	
My company has access to my private information and photos in my phone	4.27
All data and photos are wiped remotely if my phone is lost or stolen	3.88
My phone is controlled by my company	4.32
My manager sees my location and availability information	3.77

*Note. * 5 Point Likert Scale*

As it is seen in Table 5 the Pearson correlation value 0,429 (Sign.≤0.01) is significant for H1 and indicates the positive relationship between employees' positive perceptions about BYOD and their tendency to work more effectively with BYOD. In other words, if they think that BYOD is advantageous then they are more effective at work using their own devices which confirms H1.

H2 is supported with significant Pearson correlation value of 0.247 (Sign.≤0.05) and means that there is a positive relationship between the employees' tendency to work more comfortably if BYOD is used and the employees perceptions that BYOD has more advantages than disadvantages. When comparing the amount of participation of

effectiveness and comfort on employees' perspective about BYOD, it is observed that effectiveness is more influential based on higher Pearson correlation coefficient.

H3 is not confirmed since there is no significant correlation between variables. In other words, advantage or disadvantage related opinions of employees about BYOD do not have any statistically significant correlation to their privacy and security concerns.

Table 5
Pearson correlation result for Hypothesis 1, 2 and 3

Hypothesis	Pearson Correlation	Sig. (2-Tailed)
H1	0.429	0.00**
H2	0.247	0.02*
H3	0.015	0.886

*Note. **Correlation is significant at 0.01 level; *Correlation is significant at 0.05 level*

In order to explain the changes in employee perceptions about BYOD policy based on the independent variables such as comfort, privacy & security concerns and effectiveness a stepwise multiple regression analysis has been done. The basic statistical assumptions of linearity and homoscedasticity are checked with scatter plots whereas for normal distribution of residuals of regression Normal P-P plot is used. Durbin-Watson value of 1.436 indicates that there is only little or no auto-correlation in the data. A significant regression model is found with ANOVA values of ($F(3,89)=6.906$ $p\leq0.000$) and R^2 of the regression model is 0,189 with adjusted R^2 of 0,161. Although ANOVA analysis is significant, the coefficients for comfort and privacy concerns are not statistically significant. Tolerance value of 0.7 and VIF=1.429 for effectiveness show that there is no multicollinearity. The following is the estimated equation of fitted model and it only includes effectiveness:

*The employees' perspective about BYOD = 0.189 + 0.410 * effectiveness*

5. Conclusion and discussions

In parallel to growing internet addiction of people, most of the daily activities carried by traditional methods are transferred to digital environments. Selling and buying, financial transactions, keeping in contact with social groups, playing games, listening to music, watching movies, reading newspapers, magazines, books, finding new friends and many other activities exist in electronic form in today's digitalized world. The essence of activities is the same but the way they are done has been changed. Mobile devices such as smart phones, tablets and laptops are adding acceleration to this inevitable transformation in society.

Internet and mobile device usage behavior of people can also be explained with their values. Individual behaviors have their roots in people's mind, deep in their values. Each individual thinks, feels, decides and acts based on their value priorities in almost every action including communication, motivation and their life styles (Schwartz, 2014). Internet and mobile devices provide good support to Rokeach's some of universal terminal values (Rokeach, 1973) such as A comfortable life, A sense of accomplishment, Freedom, Happiness, Pleasure and Social recognition. Mobile devices are also very useful instruments for hedonism which represents individualism (Inglehart, 1997).

The increasing personal need and willingness to use their devices in the work place lead employees and managers to find new business process solutions in order to achieve better human relations together with higher productivity and effectiveness at the same time. Organizational support increases workers' tendency to share knowledge which also contributes to accomplishment of organizational goals (Castaneda & Durán, 2018). Allowing personnel to use their own devices in the work place for both work and their personal use is nice to hear for employees however not easy to implement for both managers and employees due to the existence of negative aspects to consider.

This study reviews advantages and disadvantages of using "personally owned device" in the workplace. The research looks at the field from two different perspectives: Employees and managers. Manager perspective is enlightened with the help of interviews. Interview data and literature review provided the basis for the survey instrument which served to learn employee perspective.

As institutions in financial sector are audited regularly and they are obliged to comply with international information security regulations and standards they do not look positively at the implementation of BYOD policy. They are extraordinarily sensitive for access, storage and protection of enterprise data. They claim that BYOD implementation would create extra workload for IT departments. In addition, the slightest information leakage or vulnerability will lead to financial losses and loss of reputation. Although it seems attractive for marketing departments which should respond quickly to customers, it is evaluated that the loss would be greater than the benefit with current conditions. When BYOD becomes widespread in time and if related regulations might be arranged, financial institutions also may take steps for implementation of BYOD policy.

The manufacturing organizations participated in the study are in automotive sector. They have indispensable need for high-level technology. Their most important goal is to produce solutions to customers as quickly as possible. This is feasible only with easy and fast access to information. According to managers in automotive sector the main reason of their support to BYOD policy is keeping contact with employees regardless of time and place.

The managers in small businesses were interviewed to learn their awareness about BYOD and plans for future. Because of low volume of workload and their weak IT infrastructure, small businesses do not show any interest at BYOD approach. The number of employees having high awareness of information security is found to be low and therefore usage of BYOD can create risks for small enterprises. The only attractive aspect is that continuous access to employees will improve the efficiency of the company as they have limited number of qualified personnel. An article written by Madzima et al. (2014) also supports the findings reached by this study's interviews. Since small-scale organizations may lack the technical knowledge in implementing proper security strategies, the adoption of BYOD presents security challenges and it may jeopardize their information systems security.

The research demonstrated that even if organizations support BYOD, the general attitude of the managers in different sectors lead them to serious concerns about the leakage of enterprise data. In order to design the most effective security strategy which supports BYOD, a close collaboration between top management, security staff and end-users is very essential (Marjanovic, 2013). IT department has an essential role in determining both policy and rules. It is also responsible for security issues of managing mobile devices such as deciding that malicious software is prohibited to download and setting the rules about security patches, updates and logging mechanisms. IT and Human Resources departments should establish a policy for wiping data in mobile devices

remotely in case of employee termination, data leakage or device loss (Marjanovic, 2013; Porter, 2011).

Organizations also need to educate their end users and increase their awareness about security (de las Cuevas et al., 2015). It is known that most of the data loss is caused by internal employees because of carelessness, not malicious users. Employees need to feel the responsibility of having corporate data in their mobile (Morrow, 2012; Lennon, 2012). They should know safe usage rules of mobile devices to avoid causing any security breach (Markelj & Bernik, 2015). They should also be aware of threat of phishing attacks that steal sensitive information from users with deceiving them (Arachchilage et al., 2016). Another subject taken into consideration is about employees who access confidential corporate data by their own device without any security precautions. It is vital to prevent system and sensitive data from intentional damage of users. Security agreements including strict rules may be a solution to deter personnel from malicious act (Madzima et al., 2014).

The research indicates no statistically significant difference among employees based on age, gender or education towards BYOD policy. On the other hand, about comfort and achievement values which are not only important for employees but for all human beings, statistically significant findings are reached. The research shows that when employees think that "BYOD advantages dominate" and use their own devices then they feel more comfortable. In other words, since BYOD supports "a comfortable life" value, employees are in favor of BYOD although there are some disadvantages. The subjects that are considered as disadvantages by employees are related to the possibility of leakage from their private lives. However growing inclusion of IT in individuals' daily life prepare them to accept close monitoring of their behaviors by various organizations such as government, financial institutions and commercial companies. Additionally, it is observed that many individuals themselves do not hesitate to share part of their private lives with public in social media. Running their business anywhere anytime with the help of their own devices raises their success at work. Although some of private life time is sacrificed to do business, they seem to be happy of being more effective. The highest benefits they get from using their own devices at work are "feeling freer" and "working more comfortably".

The results show that although employees and managers find BYOD advantageous in many different ways, they also have significant concerns about security and privacy. Companies should evaluate their context carefully before implementing BYOD, by taking all effects of BYOD into consideration. The next generations of "digital natives" will strongly tend to use their own devices at work and therefore organizations should start preparations for adoption of their system for BYOD (Miller et al., 2012).

This research contributes the literature by analyzing the organization and employee perspectives about BYOD policy. The qualitative data provided by the help of managers from different sectors, differentiates the study from others in the literature by taking the mission and vision of their enterprises into account.

However, the study has some limitations. BYOD was not common yet and it was an unfamiliar concept in most of the organizations in 2015 and 2016 during which the data was collected. Although BYOD concept was explained in detail to managers especially who are not working in the field of IT, interview results can be misleading. This is also the case for the survey conducted with employees. The answers of some respondents who do not have enough knowledge about BYOD may generate biased results. Another limitation of this study can be the low response rate of the survey and

time constraints for interviews. Participation of larger number of employees and managers from different industries may lead to more reliable results.

In future research, the scope of work can be extended internationally, and multicultural studies of the perspectives of employees and managers about BYOD from different countries may bring new approaches to BYOD policy.

ORCID

Kevser Gülnur Gökçe https://orcid.org/0000-0002-8982-4094

Ozgur Dogerlioglu https://orcid.org/0000-0001-5226-5578

References

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

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3/4), 130–137.

Castaneda, D. I., & Durán, W. F. (2018). Knowledge sharing in organizations: Roles of beliefs, training, and perceived organizational support. *Knowledge Management & E-Learning, 10*(2), 148–162.

Chang, J. M., Ho, P. C., & Chang, T. C. (2014). Securing BYOD. *IT Professional, 16*(5), 9–11.

Cognini, R., Gagliardi, R., & Polzonetti, A. (2013, December). Business management and mobile experience. In *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE. doi: 10.1109/IEEM.2013.6962363

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., García-Sánchez, P., & Fernández-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications, 68*, 83–95.

Disterer, G., & Kleiner, C. (2013). BYOD—Bring your own device. *HMD Praxis der Wirtschaftsinformatik, 50*(2), 92–100.

Dong, Y., Mao, J., Guan, H., Li, J., & Chen, Y. (2015). A virtualization solution for BYOD with dynamic platform context switching. *IEEE Micro, 35*(1), 34–43.

Fujimoto, Y., Ferdous, A. S., Sekiguchi, T., & Sugianto, L. F. (2016). The effect of mobile technology usage on work engagement and emotional exhaustion in Japan. *Journal of Business Research, 69*(9), 3315–3323.

Hayes, B., & Kotwica, K. (2013). *Bring your own device (BYOD) to work: Trend report*. Oxford, UK: Elsevier.

Inglehart, R. (1997). *Modernization and postmodernization: Cultural, economic, and political change in 43 societies*. Princeton, NJ: Princeton University Press.

Jaramillo, D., Ackerbauer, M., & Woodburn, S. (2014, March). A user study on mobile virtualization to measure personal freedom vs. enterprise security. In *Proceedings of the IEEE SOUTHEASTCON*. IEEE. doi: 10.1109/SECON.2014.6950672

Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R., & Cook, T. (2013). Cooperative solutions for bring your own device (BYOD). *IBM Journal of Research and Development, 57*(6): 5.

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science, 56*, 376–383.

Kim, S., & Lee, K. T. (2014, October). A security architecture for BYOD office. In

Proceedings of the International Conference on Advanced Technologies for Communications (ATC) (pp. 487–490). IEEE.

Lennon, R. G. (2012, October). Changing user attitudes to security in bring your own device (BYOD) & the cloud. In *Proceedings of the 5th Romania Tier 2 Federation Grid, Cloud & High Performance Computing Science (RQLCG)* (pp. 49–52). IEEE.

Madzima, K., Moyo, M., & Abdullah, H. (2014, August). Is bring your own device an institutional information security risk for small-scale business organizations? In *Proceedings of the Information Security for South Africa (ISSA)*. IEEE.

Marjanovic, Z. (2013). *Effectiveness of security controls in BYOD environments*. The University of Melbourne, Australia. Retrieved from http://hdl.handle.net/11343/33346

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications, 20*, 84–89.

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional, 14*(5), 53–55.

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

Ocano, S. G., Ramamurthy, B., & Wang, Y. (2015, February). Remote mobile screen (RMS): An approach for secure BYOD environments. In *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)* (pp. 52–56). IEEE.

Ogie, R. (2016). Bring your own device: An overview of risk assessment. *IEEE Consumer Electronics Magazine, 5*(1), 114–119.

Pogarcic, I., Gligora Markovic, M., & Davidovic, V. (2013, May). BYOD: A challenge for the future digital generation. In *Proceedings of the 36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO)* (pp. 748–752). IEEE.

Porter, K. M. (2011). Going mobile: Are your company's electronic communications policies ready to travel? *Business Law Today*. Retrieved from http://www.rc.com/documents/Going_Mobile_Porter_Jan_2012.pdf

Rhee, K., Eun, S. K., Joo, M. R., Jeong, J., & Won, D. (2013). High-level design for a secure mobile device management system. *Lecture Notes in Computer Science, 8030*, 348–356.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications, 6*(2), 353–358.

Rivera, D., George, G., Peter, P., Muralidharan, S., & Khanum, S. (2013). *Analysis of security controls for BYOD (bring your own device)*. The University of Melbourne, Australia. Retrieved from http://hdl.handle.net/11343/33338

Rokeach, M. (1973). *The nature of human values*. New York, NY: The Free Press.

Scardilli, B. (2014). BYOD or COPE: The best mobile strategy for the workplace. *Information Today, 31*(2). Retrieved from https://www.questia.com/magazine/1G1-363515159/byod-or-cope-the-best-mobile-strategy-for-the-workplace

Schwartz, S. H. (2014). Values: Cultural and individual. *Journal of Cross-Cultural Psychology, 45*(1), 5–13.

Shumate, T., & Ketel, M. (2014, March). Bring your own device: Benefits, risks and control techniques. In *Proceedings of the IEEE SOUTHEASTCON*. IEEE. doi: 10.1109/SECON.2014.6950718

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.

Wang, Y., Wei, J., & Vangury, K. (2014, January). Bring your own device security issues

and challenges. In *Proceedings of the 11th Consumer Communications and Networking Conference (CCNC)* (pp. 80–85). IEEE.

Waterfill, M. R., & Dilworth, C. A. (2014). BYOD: Where the employee and the enterprise intersect. *Employee Relations Law Journal*, *40*(2), 26–36.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81–99.