Employee’s awareness on security aspects of use bring your own device paradigm in Republic of Croatia

Dragan Peraković[*], Siniša Husnjak[*]
*University of Zagreb, Faculty of transport and Traffic Sciences,
Department of Information and Communication Traffic,
Zagreb, Republic of Croatia, EU
dragan.perakovic@fpz.hr, sinisa.husnjak@fpz.hr

Vlatka Mišić**
**Graduate student at University of Zagreb, Faculty of Transport and Traffic Sciences,
Zagreb, Republic of Croatia, EU
vlatka.misic@gmail.com

Tibor Mijo Kuljanić***
***PhD student at University of Zagreb, Faculty of Transport and Traffic Sciences,
Zagreb, Republic of Croatia, EU
tibor.kuljanic@gmail.com

Abstract—**Within this paper, a conducted survey analyses the knowledge on the term of the use of personal device in the corporate environment and employee awareness of security issues that arise with introducing BYOD trend in business. BYOD represents a risk to business, usually present as the risk of data theft, unauthorized access to applications and systems of corporation, loss of reputation and such. BYOD, like any other system, must be systematically planned, implemented, monitored and improved. Employees are not sufficiently educated and aware of the security risks that BYOD brings.**

Keywords- BYOD, terminal devices, security, corporative data, security issues

I. INTRODUCTION

With the rapid advancement of technology, smart mobile terminal devices (smartphones), are becoming an integral part of every organization. The usage of personal devices in the corporate environment is introduced as Bring Your Own Device (BYOD) concept, which means the linkage of employee’s devices to the corporation’s network. Employees mostly bring their own terminal devices, such as smart mobile terminal devices, tablets and laptops for use in the working place.

Today, smart mobile devices are the most widely used terminal devices. They are widely used and are no longer used only for classical communication, i.e. for calls and text messages, like it was the case ten years ago. The amount of data stored on mobile devices is large, and users are often not aware of it. Compromised data can greatly damage the owner, there is a risk of identity theft, financial damage, reputational damage or other forms of manipulation of data by malicious users. Particularly high risk of manipulation of data occurs in a corporate environment, where information stored on the terminal devices can be particularly vulnerable.

With the advent of BYOD model and its integration into the organizational structure there are seem to appear multiple problems while trying to protect such devices. The main goal of any organization is to protect business data and private information infrastructure, but at the same time they are legal and regulatory obliged to respect the privacy of the owner of the device, that is employees. The introduction of mobile terminal devices in business brings many advantages such as access to corporate data on the field, optimization and reduction of operating costs, satisfaction of employees and customers, performing everyday tasks away from the office and so on.

Although BYOD model brings many benefits to employees and employers, there are some security issues regarding sensitive information. The device that is not owned by the organization is used in storing, processing and sending sensitive information, while an unauthorized access to such information could have a huge negative impact on the organization.

This study questions the understanding and frequency of use personal terminal devices in the corporate environment in the Republic of Croatia and the awareness of employees about security issues brought by using personal device at workplace.

II. TRENDS IN THE USE OF SMART MOBILE TERMINAL DEVICES

Smartphones, thanks to the rapid development of technology and the sale price, have become available for a large number of users. Characteristics of mobile terminal devices become almost the same as those of laptops and personal computers, and therefore they are not used only for personal but also for business purposes [1].

The term of smartphone is introduced to the market as a term that included a new class of mobile phone that offers integrated services, from voice communications, instant messaging, personal information management through to various applications and features of wireless communication [2]. Although there is no exact definition of smart mobile terminal device, it can be said that this is any device that extends the capabilities of the classic mobile device. Additional features that are expected for smart mobile terminal device are not exactly defined and do change over time [3]. Key features of smart mobile terminal devices [4]:

a. operating system (OS)

b. applications

c. full (“software”) QWERTY keyboard

d. constant Internet access

e. the ability to exchange messages

Functionalities of mobile terminal devices do not depend only on the hardware, but also on operating system that is being used [4]. Since June 2013 Android is leading operating system for smartphones, as the number of devices sold crossed until then leading iOS [5]. Since that event the dominance of Android OS on the market is evident, which was confirmed by results of research in security aspects of using personal devices in the corporate environment conducted for this study (Figure 1).

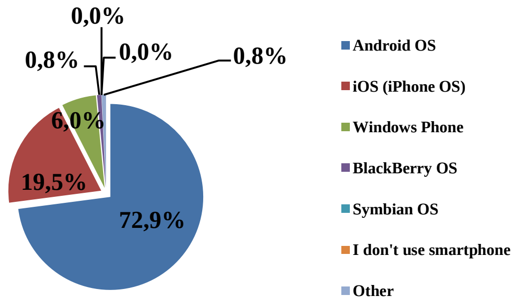

Figure 1. Frequency in the use of individual operating systems of mobile terminal devices

Mobile data traffic will reach the following milestones within the next 5 years [6]:

- monthly global mobile data traffic will be 30.6 exabytes by 2020,
- number of mobile-connected devices per capita will reach 1.5 by 2020,
- average global mobile connection speed will surpass 3 Mbps by 2017,
- total number of smartphones (including phablets) will be nearly 50 percent of global devices and connections by 2020,
- because of increased usage on smartphones, smartphones will cross four-fifths of mobile data traffic by 2020,
- monthly mobile tablet traffic will surpass 2.0 exabytes per month by 2020,
- 4G connections will have the highest share (40.5 percent) of total mobile connections by 2020,
- 4G traffic will be more than half of the total mobile traffic by 2016,
- more traffic was offloaded from cellular networks (on to Wi-Fi) than remained on cellular networks in 2015,
- three-fourths (75 percent) of the world’s mobile data traffic will be video by 2020.

III. BRING YOUR OWN DEVICE TRENDS

In the last few years there has been a new trend in the IT environment – BYOD, that many corporations and organizations implemented in their business [7]. BYOD allows employees to bring their own terminal devices to their workplace, such as laptops, smart mobile devices and/or tablets, to work on them and connect them to the corporate network instead of using devices in the corporate property [8].

The introduction of mobile terminal devices in business brings many advantages such as access to corporate data on the field, optimization and reduction of operating costs, satisfaction of employees and customers, performing everyday tasks away from the office and so on [9]. The company can save a lot of money that would be spent on the purchase of expensive equipment if the BYOD is not being used. Thanks to the employees who pay for their own devices, companies can save up to $ 80 per month per employee [10].

A recent survey by Intel performed on many organizations about benefits of BYOD for IT and as follows [11]:

- 28% improved efficiency and productivity
- 22% improved worker mobility
- 17% saving on inventing in new machines
- 9% job satisfaction and retention
- 6% reduce IT management/troubleshooting

However, due to the mobility of devices, their small size and the ability to connect through several available technologies, mobile devices are vulnerable to security threats from other devices such as PCs and laptops. Some of the security threats to mobile devices are [1]:

- theft or loss of a mobile terminal device,
- attacks on devices intended for recycling,
- attacks through malware (malicious) content (viruses, worms, spyware, adware, ransomware and Trojan horses)
- monitoring data through specific sensors (GPS, accelerometer, microphone, camera)
- phishing attacks
- exploitation of vulnerabilities in web browsers,
- automatic download of applications,
- attacks through falsified information about the network,
- exploitation of network gaps,
- social engineering.

The impact of these threats can affect private information, intellectual property of corporation, confidential information, financial assets, the availability and functionality of the devices and services and the personal and political reputation [4].

In order to preserve the security of information it is essential to maintain the integrity, confidentiality and availability of information system resources [12]. The integrity, confidentiality and availability are the three basic principles of information security. Resulting problem can be solved by separating private and business data in the device and thus reduce the risk of compromising user privacy and unauthorized access to sensitive information of the organization. Such solutions are often implemented within a comprehensive enterprise mobility management system (EMM) [1].

It is forecasted that 200 million out of 350 million mobile device users will be utilizing them in conjunction with the BYOD approach by the year 2016 [13]. In [14] autor have forecasted that, by 2016, worldwide shipments of smart phones will reach 480 million, with 65% being used in bring-your-own device environments. Gartner predicts by 2017, 50% of employers will require employees to have their own device for work purposes. According to Forrester, 50% of 18- to 31-year-old and 40% of 32- to 45-year- old workers believe technologies used in their private life are “better” than those in their professional life[15].

IV. Descriptive analysis of employees’ awareness on security aspects of use bring your own device paradigm

This paper includes research on the term of the use of terminal devices in the corporate environment (BYOD). The conducted survey examined the frequency of the use of personal terminal devices in the corporate environment in the Republic of Croatia and the awareness of employees about security issues that come as a result of using personal device at workplace. The target users for this research were exclusively employed persons. The research included 133 respondents, of whom 67 women and 66 men. Respondents are mostly younger, between 18 and 35 years.

According to research conducted for this paper it can be concluded that employees in Croatia often use their own terminal devices in the workplace but BYOD trends are not developed as they are developed in the United States or other countries of the European Union. 12.8% of respondents never use their personal terminal devices in the workplace, 9.8% of respondents rarely use their personal terminal devices, 22.6% use them occasionally, 17.3% often, and even 37.6% of respondents use their personal terminal device at workplace very often. These results are shown in Figure 2.

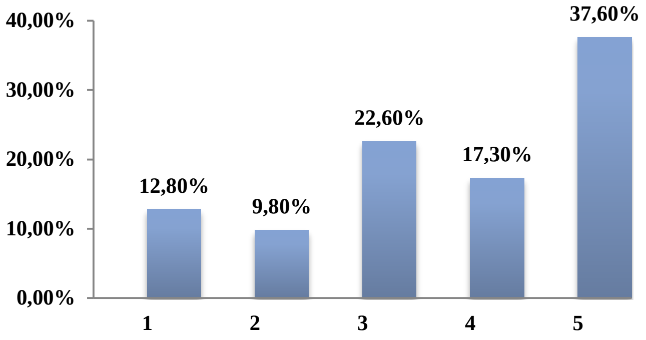

Figure 2. The use of personal terminal device at workplace

Smart mobile terminal devices (66.17%) are most often used personal devices at workplace, followed by laptops or notebooks (17.29%). Types of personal terminal devices used at work are shown in Figure 3.

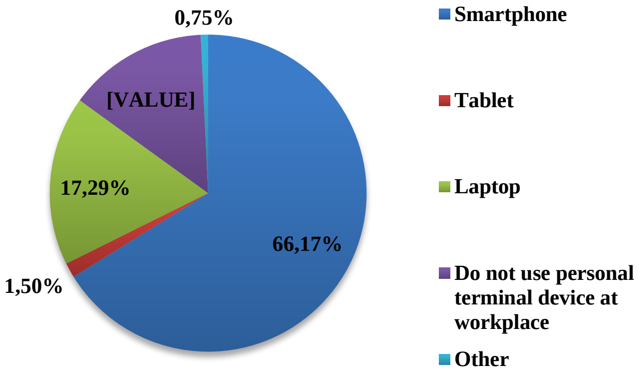

Figure 3. Types of personal terminal devices used at workplace

Conducted research shows that most users (38.35%) connect their personal device to the corporate network very often or never (32,33%) as is shown in Figure 4.

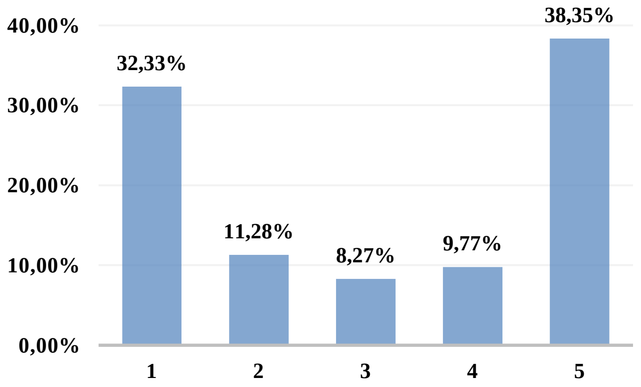

Figure 4. The frequency of access to the network with personal device in corporate environment

Results of the research on the user awareness of security issues of connecting personal terminal device to the corporate network are disturbing (Figure 5). 30,00% of respondents do not even consider (with greater conviction) that the security of company data is compromised, while 38,46% do not consider (with less conviction) that the security of data is compromised. 68,46% of respondents are not aware of security issues of using their personal terminal devices in the corporate environment. 16,92% of respondents don’t know is the security of data compromised, 0,77% state it does not matter whether the security of data is compromised, 3,08% think that the security of data is compromised but don’t consider it important, while only 10,77% of respondents believe that the security of company data is greatly compromised.

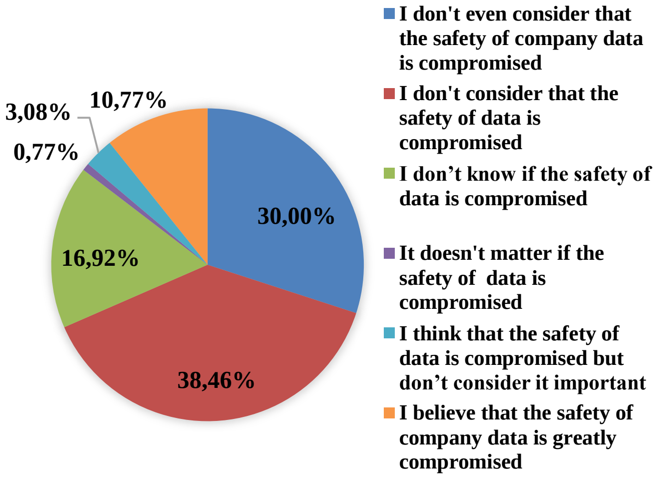

Figure 5. Awareness of compromising security of company data by accessing the network with personal device

More than a half of respondents are not familiar with the term of BYOD (Figure 6). 36.64% of them had never heard of the term BYOD, and 13.74% have heard of the term but are not familiar with it. 16,03% of respondents were poorly informed about the BYOD term. 10.69% of respondents are well aware of the BYOD term, while 22.90% of them stated that they are fully aware of the term.

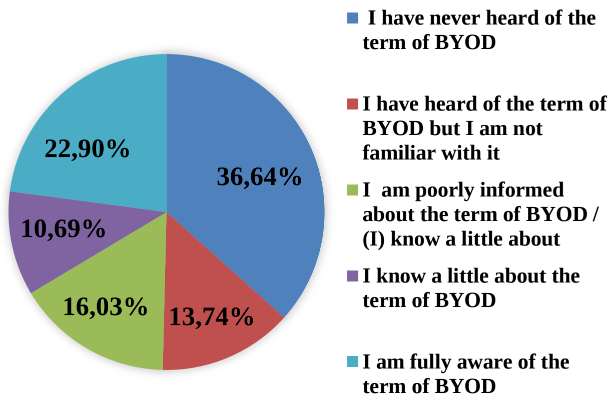

Figure 6. Percentage of the respondents familiar with the term of BYOD

According to conducted research shown in Figure 7 it can be concluded that employees are not educated enough, or they are not aware of security policy of the company and the ways to ensure the security of company data. Even 44.27% of respondents don’t know if the company in which they work has a BYOD security policy. 27.48% of respondents claims that the company in which they work is not conducting BYOD security policy, and 12.98% say they do not know what is BYOD security policy. 6.87% of respondents claims that the company has a BYOD security policy, but the employee doesn’t know much about it, while only 8.40% say that the company conducts BYOD security policy and the employee is well familiar with it.

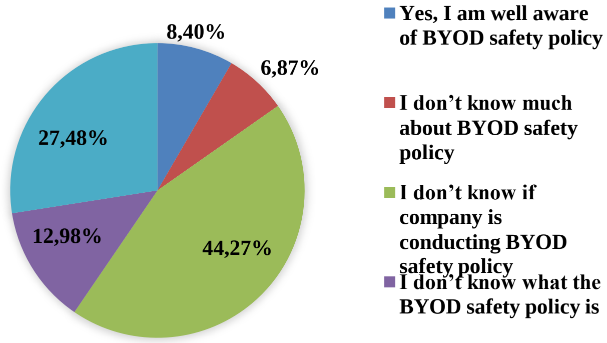

Figure 7. Percentage of the companies conducting BYOD security policy

V. Conclusion

BYOD is one of the newer causes of data vulnerability where employees within corporation access to sensitive corporate data using their personal devices, i.e. laptops, smart mobile terminal devices, tablets and similar. According to the results of the research it can be concluded that employees in the Republic of Croatia do not use their personal terminal devices in the workplace as much as employees in the United States and other countries of the European Union. In cases where personal terminal devices are being used, the term of BYOD has not been adopted.

The employees are not educated enough about security risks to corporate data. Employees believe that corporate data is not owned by them and that their compromise is not going to affect them. The consequences of security flaws can be very high, not only for business but also for its employees, which shows the importance of continuous education of employees.

Companies that allow their employees to use their personal terminal devices should have priority to protect the basic principles of information security (integrity, confidentiality and availability). Nowadays, the information is more valuable to companies than physical assets, and to ensure competitiveness in the market it is crucial that the information is well protected.

REFERENCES

[1] D. Peraković, S. Husnjak and I.Cvitić, “Comparative analysis of enterprise mobility management systems in BYOD environment,” The 2nd Reseach Conference In Technical Disciplines, RCITD 2014, pp. 82-85, November 17 - 21, Žilina, 2014

[2] M. Sarwar, T.R. Soomro, “Impact of Smartphones on Society”, European Journal of Scientific Research, Vol. 98, No. 2, 2013., pp. 216-226

[3] D. Peraković, S. Šarić and S. Husnjak, “Analysis of the Evolution of Terminal Devices in the Use of SMS Service,” in Proceedings of 15th International Conference on Transport Science, ICTS 2012, pp. 1-9, May 28th, Portorož, 2012

[4] D. Peraković, S. Husnjak and V. Remenar, “Research of Security Threats in the Use of Modern Terminal Devices”, Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium, Vol. 23., pp. 545-548, October 24 – 27, Zadar, 2012

[5] W3C Mobile Devices Statistics. Available at: http://www.w3schools.com/browsers/browsers_mobile.asp

[6] Fundarc Communication (2016). WiFi is much required to offload many cellular services those can lead to expansion of customer base. Available at: http://fundarc.co.uk/

[7] B. Hayes and K. Kotwica, Bring Your Own Device (BYOD) to Work, The Security Excutive Council, Elsevier Inc., 2013

[8] J.P. Shim, D. Mittleman, R. Welke, A.M. French, J.C. Guo, “Bring Your Own Device (BYOD): Current Status, Issues, and Future Directions, Georgia State University,” The 19th Americas Conference on Informaton Systems, AMCIS 2013

[9] Andrej Radinger (April 2008) Mobilna rješenja u poslovnom okruženju. Available at: http://www.infotrend.hr/clanak/2008/4/mobilna-rjesenja-u-poslovnom-okruzenju,159,446.html

[10] J. Keyes, Bring Your Own Devices (BYOD) Survival Guide, New York, CRC Press, 2013

[11] http://www.intel.com/content/www/us/en/mobile-computing/consumerization-enterprise-byod-peer-research- paper.html

[12] M. Bilandžić, V. Cvrtila, R. Kralj, B. Javorović, N. Lebeda, Business intelligence i zaštita tajnih i osobnih podataka i informacija, Zagreb, Defimi, 2005

[13] M. M. Singh et al, “Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model”, International Journal of Mobile, Network, Communication and Telematics (IJMNCT), Vol. 4, No. 5, 2014, pp. 1-17

[14] M.Dhingra, “Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)”, International Conference on Information Security & Privacy (ICISP2015), Vol. 78, pp. 179-184, December 11-12, Nagpur, 2016

[15] B.Gray, Building A Bring-Your-Own-Device (BYOD) Program. Forrester Research (Hrsg.), 2012