BYOD – A NEW TREND IN TELEWORK

Michał TRZISZKA

Poznan University of Technology, Faculty of Engineering Management, Chair of Management and Computing Systems; michal.trziszka@put.poznan.pl

Abstract: BYOD – Bring Your Own Device – refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smartphones) to their workplace, and to use those devices not only for private but also for business purposes. The study presents the analysis of the BYOD trend, the analysis of previous studies, and constitutes an attempt to determine advantages and disadvantages of adopting BYOD in a company. The paper ends with a short summary.

Keywords: byod, telework, byod trend, remote work.

1. Introduction

BYOD, which is the abbreviation for Bring Your Own Device, refers to permitting employees to bring personally owned devices and to connect them to the company network in order to perform professional duties. This phenomenon is developing dynamically and has its advantages and disadvantages as every new trend (Pentacomp, 2017).

The trend emerges in companies regardless of their size or type of business. The development of BYOD is promoted by an increasing prevalence of telework. In future, therefore, it will be favoured by teleworkers or employees who travel very frequently, e.g. salespeople. A stimulus to the growing importance of BYOD is also an increasing popularity and possibilities of using various mobile devices. These devices not only include computers, but also tablets or smartphones, which nowadays are almost equal to computers even though they were still the most common devices in companies several years ago. It may be argued that BYOD refers not only to a significant technological change, but also a change in the data management model in a company and another way of determining the boundaries of the IT environment of a company (Chmielarz, 2017). BYOD is making significant inroads into workplaces. However, device security is still a central issue. Independent studies confirm that one of the main trends and challenges for companies is consumerisation. By adopting BYOD,

companies are able to gain an advantage over competitors, but they cannot forget to implement appropriate security measures.

2. Description of BYOD use

It is worth analysing the benefits and threats associated with adopting the BYOD strategy in a company. The benefits include significant cost savings for a company. If employees use their personal devices, employers do not have to purchase them. Another benefit includes employee satisfaction and productivity. Employees use their own favourite devices – selected by themselves rather than assigned by the IT department. The BYOD trend also features mobility, which is of significant importance to Generation Y (also known as Millennials). It is Millennials that the BYOD phenomenon primarily concerns. Representatives of the digital generation are used to working in a coworking style, at favourite cafes, or at home – in other words, they are teleworkers. For them, being mobile is natural (Kołtonik, 2017).

Apart from savings on labour costs, competition on a global scale forces employers to be flexible. Demanding customers are seeking new products and services, primarily personalised – that is increasingly advanced and complex. The business cycles already known, which can be taken into account in business plans, saw the addition of a phenomenon of sudden and short-term changes in demand, which requires quick adjustment decisions to be made. These decisions may concern both the number of employed workers (numerical flexibility), including, therefore, all solutions aimed at minimising the protection of the employment relationship durability, and the adjustment of working time – its shortening and extension depending on the employer's demand (working time flexibility, work sharing) (Lach, 2006).

Progress in the field of new technologies, especially computer and telecommunications, ICT technology, and popularisation of the Internet means that sophisticated products and services are launched on the market more quickly, and they become obsolete and are replaced with newer ones more quickly as well. More and more capital-intensive technologies are simultaneously labour-saving. Not only does the demand for labour decrease, but also the nature of labour changes as more and more tasks involve creativity in the first place. Adapting to the market requirements, employers seek flexible and independent workers; however, an active and enterprising subcontractor organises their work on their own, thus not expecting managerial orders (Wiśniewski, 2010).

Work efficiency increases in the long run. It is influenced by a change in the staff management, higher productivity, and a lower staff fluctuation, while at the same time the flexibility of action of a company increases. Telework reduces bureaucracy, ensures a better circulation of information, while the use of new technologies and an enhanced work organisation policy result in a shorter response time of a company to market evolutions.

BYOD brings an advantage to companies by reinforcing innovation and creativity in the workplace while at the same time reducing the general costs of the entire organisation. An important link that should suppress the impetus of the new trend is the implementation of appropriate BYOD policies and procedures, which will ensure that all devices are protected. By cooperating with a partner responsible for security and competent to protect devices in a network, companies may derive benefits from the new trend and may not be overwhelmed by a large amount of information.

The analysis of the BYOD trend by technology companies and research agencies is still in progress. Over the last years, these organisations have carried out a number of studies concerning the functioning of this strategy in the work environment. The results presented by them demonstrate both advantages and disadvantages of the BYOD phenomenon.

The results of independent reports and observations focused on the use of mobile devices show that 83% of companies adopting the BYOD policy have relevant regulations concerning the installation of independent software in order to ensure protection against data leakage. 86% of IT managers from the USA, UK and Germany claim that the main issue concerning data security results from smartphones connected to the company network – 47% of companies allow their employees to connect their personally owned devices to the company network.

If a data leak is detected, many companies immediately change their security procedures to involve actions such as limiting access to data (45%) or installation of data-protecting software (43%). A small number of companies decide to stop adopting the BYOD policy after an incident has occurred (12%) (Gajewski, 28 November 2017).

The results of the "Modern IT in SMEs" study conducted for Microsoft by Ipsos MORI reveal that personally owned IT devices in the workplace are used in nearly half of Polish small and medium-sized enterprises. The most common personally owned devices used for business purposes include laptops (57%), followed by smartphones and tablets (48%) – they usually come with Android (73%), followed by Windows (13%) and iOS (10%). In case of tablets, which are used in the BYOD model by 20% of employees, Android is the most popular operating system, Windows came second (16%), whereas iOS came third (13%). More importantly, 54% of the respondents claim that they take a look at business documents after work with the use of company devices (51%) or their own (45%) (Gajewski, 2017).

Many people believe that BYOD is a natural stage of company development. In a world where increasingly more people use social media and tools available on the Internet, employees expect their company to allow them to use the devices that suit them best at work (Makowiec, 2016).

3. BYOD safety

In such sectors as defence or finance, where data security is of particular importance, companies tend not to allow their employees to use their own tablet or smartphone, but at the same time try to increase employees' productivity by using appropriate applications for selected devices. Multi-level protection and device management mechanisms should correspond to the needs of a company and user (Serafin, 2013).

A company should also consider legal issues related to the BYOD policy. Can the employer legally monitor devices owned by employees to control whether data integrity or terms of use have been violated, or whether time and resources have been misused? This model is based on the assumption that devices belong to employees. However, the rules should be adopted to the requirements of this new trend so that devices can be monitored to a limited extent at least (Serafin, 2013).

It is vital to consider costs and legal issues. Still, companies specialising in infrastructure, such as Alcatel-Lucent, develop solutions that facilitate the implementation of the BYOD model. It is already technologically possible to manage the BYOD environment and ensure users have secure access to data in an economically efficient way. In such network infrastructure, applications that make communication and cooperation easier may be safely used on devices selected by employees. In addition, it is possible to integrate platforms responsible for voice, data, and video transmission. Being already on the market, the Open Touch Conversation solution ensures easy communication between different devices such as iPads.

The task of a service provider is to adapt applications to strategies employed by IT managers. The application to be implemented should make it possible to communicate using different devices safely, and with economically effective infrastructure supporting such applications regardless of whether the company uses the BYOD model or not. Companies should not perceive the BYOD trend from the point of view of costs only, which are not always so important, but they should rather aim at increasing productivity and benefits reaped by individual employees. They may choose a pragmatic strategy based on due diligence investigation and 360-degree feedback, which makes it possible to determine the best speed of BYOD model implementation – adapted to the company requirements and users' roles. If they decide to introduce BYOD, they should make sure that employees are aware of their rights and limitations. To that end, comprehensive procedures and rules should be introduced (Anonim, 2017).

BYOD also entails some challenges associated with company data security. If devices are lost, stolen or hacked, there is a risk of a confidential information leak. IT support constitutes another issue. In an environment involving many devices with different operating systems, it becomes impossible to ensure the right technical support for all users of such devices.

Endless possibilities make it difficult to manage the entire IT structure effectively. The issues mentioned above are only one of the disadvantages of implementing the BYOD policy in a company.

Some of the risks related to this policy may be minimised by developing a security policy within a company. The policy should be known and followed by all employees. The security policy has to contain clearly defined rules in relation to rights, obligations and the scope of responsibility. For example: in order to avoid a confidential information leak, it is important for the security policy to specify, in particular, the requirements concerning password control, an ability to restrict access if security is endangered, or ability to delete sensitive information remotely in different situations. It is also important for the security policy to define the minimum requirements in terms of personally owned devices and software used on them. If these requirements are met, access to the company network and its resources will be made available. The issues mentioned above are only some that should be specified in the security policy. Once the policy is formulated, another step should involve the selection of appropriate tools with which the implementation of the BYOD strategy in a company will be possible. For example, Mobile Device Management (MDM) serves as a solution in this case. It involves software that makes it possible to remote control the entire group of mobile devices in a company (Kołtonik, 2017).

Companies that decide to introduce the BYOD model should keep the following three issues in mind:

- ensuring an appropriate system for the management of devices that connect to the company network,
- ensuring appropriate security solutions and policies in relation to access to company resources,
- in cooperation with employees, determining acceptable good practices and a range of activities that they may perform in relation to company resources with the use of their own devices; for example, these practices should include how to protect passwords, what applications are considered secure etc. (Microsoft, 2017).

4. BYOD in companies

Comprehensive preparation is required to enjoy BYOD benefits safely. The first step to be taken to protect company data is to conduct an internal audit and determine where important information is, who has access to it, how it is protected, and whether all scenarios concerning security threats have been considered. Another step involves determination of which applications may be installed on employees' personally owned devices. Then the appropriate security policy may be specified and IT solutions to introduce it may be developed. A good

solution makes it possible to manage and protect all end devices from a single control panel and supports all common operating systems used in mobile devices. It should also be convenient for the IT department by ensuring that the software installed on mobile devices is standardised. Both encryption and data leak protection are of particular importance. Mobile devices are particularly prone to theft or loss. Therefore, mobile solutions should enable IT departments and users to restrict and delete information on devices or in selected applications remotely (Chmielarz, 27 November 2017).

These days, there is a wide range of services provided by technology companies on the market. These services seek to support and facilitate the implementation of the BYOD policy in a company, for example Windows Inture available on the market may help to manage groups of both personally owned and private devices. The implementation carried out by Supremo in Grecos Holiday with a simultaneous launch of Office 365 serves as an example of introducing this service in Polish SMEs (Microsoft, 2017).

In 2017, the Nudge Rewards report was presented, which is entirely devoted to the approach to new technologies presented by employees and their employers (NudgeRewards, 27 November 2017). It shows that as many as 51% of employees are convinced that new technologies and mobile solutions can facilitate their work. At the same time, only 23% think that this is the case, and their employers use the potential of mobility in their business. The majority (58%) of employees use private devices while working for at least an hour a day. Only 43% of employers allow the use of private devices for business purposes. From the research, we can conclude that the BYOD trend is mainly in companies that have employees in the office than those working behind the company's unit. Only 1 in 10 employees, even though they have the employer's permission to use their own equipment, are encouraged to do so. The last problem is also cultural barriers, which is indicated by as much as 62% of employees. 42% of them are afraid that their supervisor does not accept the use of private equipment for business purposes and decides that they do not perform their duties properly.

5. Conclusions

The idea for BYOD is one of the innovative solutions that is meeting with approval of both employers and employees. It may bring about a considerable number of beneficial changes including higher employee's flexibility, employee's availability, and enjoyment derived from working using favoured tools as well. However, similarly to any change, it requires appropriate preparation on the part of an organisation, which will ensure that company data are protected. The methods for increasing employees' satisfaction and productivity include an office tailored to individual needs or possibility of using employees' own devices in the workplace. This positively translates to the quality of professional

performance. The employee is the most valuable asset in a company, so it is beneficial for the company in the long run to ensure that the employee has the right working conditions (Kołtonik, 2017). However, risks associated with BYOD should be kept in mind. In order to protect a company network and company data against threats posed by mobile devices, companies have to deal with security at the network level rather than at the end point level only. The only effective solution is to implement comprehensive actions, i.e. those that protect the core of the network and control the incoming and outgoing traffic generated by external devices. It is obvious that companies will have to put in a great deal of effort to support their employees in a new way.

Bibliography

- Lach, D.E. (2006). *Nowe formy zatrudnienia a zabezpieczenie społeczne w zakresie ochrony zdrowia w „Praca i Zabezpieczenie Społeczne”.* Warszawa: PWE.
- Makowiec, M., (2016). *Metodyka humanizowania telepracy.* Kraków: Wydawnictwo Uniwersytetu Ekonomicznego.
- Serafin, M., (2013). *Sieci VPN. Zdalna praca i bezpieczeństwo danych.* Gliwice: Helion.
- Wiśniewski, J., (2010). *Różnorodne formy zatrudnienia.* Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa Dom Organizatora.
- Chmielarz, W. (27.11.2017). *Prywatny sprzęt w pracy*. Retrieved from https://www.pb.pl/prywatny-sprzet-w-pracy-710341.
- Gajewski, M. (27.11.2017). *BYOD po polsku*. Retrieved from https://www.chip.pl/2015/01/byod-po-polsku.
- Kołtonik, A. (27.11.2017). *Z własnym laptopem do pracy*. Retrieved from https://www.e-biurowce.pl/pl/info/artykul/5289/z-wlasnym-laptopem-do-pracy.
- Microsoft (29.11.2017). *Badanie „Nowoczesne IT w MŚP 2014” przeprowadzone przez Ipsos MORI na zlecenie Microsoft*. Available online https://news.microsoft.com/pl-pl/2015/01/26/byod-po-polsku/.
- NudgeRewards (27.11.2017). *Your Guide to Getting Started with BYOD*. Retrieved from https://www.nudgerewards.com/getting-started-with-byod/.
- Pentacomp, Polskie Radio (27.11.2017). BYOD – *Nowy trend w firmach*. Retrieved from https://www.polskieradio.pl/111/1896/Artykul/606360,BYOD-nowy-trend-w-firmach.
- Polskie Radio (28.11.2017). *Czy warto inwestować w model BYOD?* Retrieved from https://www.polskieradio.pl/111ie/1896/Artykul/661968,Czy-warto-inwestowac-w-model-BYOD.