BRING YOUR OWN DEVICE (BYOD) VS. CHOOSE YOUR OWN DEVICE (CYOD)

Dr., Ştefan IOVAN, *Universitatea de Vest, Timişoara, ROMÂNIA*
Dr., Cristian IVĂNUŞ, *Academia de Studii Economice, Bucureşti, ROMÂNIA*

ABSTRACT: *Any company with growth ambitions must have a formal and well-defined mobile strategy, or it could lose, thanks to this, the promised economic recovery. BYOD (**B**ring **Y**our **O**wn **D**evice) refers to the fact that members of company ecosystems (management, employees, partners, etc.) will increasingly use their own personal mobile devices (smartphone, tablet etc.) in the future to work from anywhere and anytime. The phenomenon has been for several years now words that define concepts of deploying hyperbolised businesses around the world as essential concepts of the future. An all-new model in companies around the world is CYOD (**C**hoose **Y**our **O**wn **D**evice), where companies allow employees to choose the devices they want to use in the office, which is becoming more and more popular as an alternative to the BYOD phenomenon in the business environment. Following the accommodation of companies and employees with the BYOD program, the emergence of the new CYOD program proves the need and also the efficiency of the transformation and development of BYOD into a new form of use of devices in the workplace. The paper aims to present several security aspects of BYOD technology, with examples for Europe and Romania, and the ever-faster shift to CYOD technology*

KEY WORDS: *BYOD, CYOD, security, personal information, company information.*

1. INTRODUCTION

The smartphone generation means that business in most sectors needs to offer mobile services to customers. Adopting bring your own device (BYOD) also implies that mobile strategies must cover both internal and customer activities.

The BYOD phenomenon, through which companies allow employees to bring their own electronic office devices to access company data at any time, from anywhere, through any device, has spread rapidly in recent years, including in Romania.

An all-new model in CYOD companies, where companies allow employees to choose the devices they want to use in the office, is becoming more and more popular as an alternative to the BYOD business phenomenon.

Benefits of BYOD are obvious: Most employees have their own electronic devices - computers, tablets or smartphones, are familiar with them and can easily use them for professional purposes, and can handle tasks directly without losing time various problems arising from the lack of a specific application, software program or facilities on the service computer [1].

At the same time, there are some shortcomings of the BYOD concept, most of them on security. For example, company data and confidential information leave every day the headquarters and organization network, being exposed to a number of risks that also have some shortcomings in the BYOD concept, most of them on security. For example, company data and confidential information leave every day the headquarters and network of the organization, being exposed to a number of risks that make headaches for the IT department.

Approximately 15% of employees believe that their responsibility to protect company data stored on personal devices is minimal, if not nonexistent.

2. BYOD POLICY, A THREAT TO ITS SECURITY

Most of the companies consider the employees' tendency to bring their own device (BYOD) a growing threat to business. However, the percentage of companies taking steps to minimize this risk is relatively low, according to the study [2]. In this study, interviews with representatives of several companies from 24 countries were analyzed.

The most worried about this phenomenon are respondents in Japan, where 93% of companies have said that BYOD policy poses a threat to their business. Companies in North America (69%) and Western Europe (62%) also voiced concern about this policy.

Eastern European companies are less concerned about this issue, with only 54% saying that BYOD policy can be a threat to the IT security of the firm.

At the same time, most companies do not intend to introduce prohibitive measures regarding the use of personal devices at work. On the contrary, about 33% of respondents said they intended to encourage the use of Smartphone and personal tablets at work, while another 37% said they did not consider bans to prevent employees from using their own devices.

However, the percentage of companies that intend to limit the use of personal devices for service-related activities is rising: the number of respondents who said they intend to impose restrictions increased by 4%, from 15% in 2012 to 19% in 2013. The percentage of companies that intend to impose stricter rules against the use of personal devices at work has increased from 2% to 11%.

It is easy to understand why companies are increasingly worried about the threats posed by the use of mobile devices: the survey also shows that improper use of these devices is a frequent cause of IT security incidents, resulting in the loss of important data of the company.

Almost 17% (11 percentage points more than in 2012) among respondents said their businesses have been leaking confidential data because of the use of email, text messaging, and other channels available on smart phones and tablets.

However, a relatively small number of companies are now adopting specialized software to protect themselves against such threats. Approximately 39% of companies use antivirus solutions to integrate protect and manage mobile devices on the company's network, and only 28% of them use mobile-specific solutions.

As BYOD becomes a widespread policy and the number of incidents involving mobile devices increases, ensuring centralized management of these devices and maintaining safety become important and relevant needs. It is just as important that the solutions that perform these functions are easy to use, manage and integrate into the company's network.

A mobile agent is installed on the device to provide advanced protection against anti-malware threats, while Mobile Device Management (MDM) ensures secure mobile device configuration, making it easy to use.

Company data can be isolated and encrypted in a file on your personal device and, thanks to Remote Find, Lock and Wipe, these data can be deleted if the device is lost or stolen.

Using a single centralized administration console makes all company devices, including BYOD mobile devices, manageable from a single integrated security platform.

2.1. BYOD in Europe and concerns about IT security

Oracle has conducted a study involving 700 companies across Europe on the degree of acceptance of personal digital devices in business operations. The study [3] shows that there is still resistance to the adoption of BYOD practices in many regions, primarily driven by concerns about business information security on devices, user identity, and application security.

Instead, those organizations that have been opening to Bring Your Own Device practice benefit greatly from the benefits of this

policy, such as reduced IT costs and increased productivity, compared to companies in the denial phase.

Currently available solutions provide a high level of IT security control over personal or corporate devices, providing a simplified interface. Companies have the flexibility to share their personal data from employees' personal devices, using filters that isolate corporate data from personal data, making it easier for organizations to access and manage their applications.

To describe the attitudes of corporations across Europe to Bring Your Own Device, Oracle launched the study [3]. The report highlights some extremely interesting figures:

- Nearly half (44%) of European companies reject BYOD or would only allow this in exceptional circumstances;
- Another 29% permits these practices only to senior employees;
- Nearly a quarter of companies (22%) completely prohibit the storage of company information on a personal device, while 20% have no rules at all;
- More than half do not include smart phones in BYOD programs;
- Information security is the greatest concern; 45% of respondents are very worried about the security of devices; 53% of application security and 63% of data security.

The study [3] also shows that many of these concerns are related to the lack of data on the capabilities offered by modern security solutions:

- 37% have never heard of containerization (isolation of personal data from those of the company);
- Nearly 1/3 do not use any form of mobile device management (Mobile Device Management);
- 22% have never heard of Mobile Application Management.

Those who have adopted BYOD practices have a unified perspective, perceiving both tablets and smart phones as part of BYOD. They have successfully solved many of the safety issues and are prepared for a higher level of change in future BYOD versions. Respondents can be included in two categories: Those adopting BYOD ("Pioneers") practices and those who avoid those ("Skeptics").

- 83% of pioneers manage both smart phones and tablets as personal devices. On the other hand, 73% of skeptics do not include smart phones in BYOD practices. 2/3 of the skeptics are concerned about safety, as opposed to only 6% of pioneers.
- The pioneers are ready for change: almost two-thirds recognize the need to accept new personal devices and their complexity, while only 11% of skeptics share this vision.
- 86% of skeptics are deeply concerned about data and information security, compared with only 21% of pioneers.
- 65% of skeptics either do not manage data and information safety or only allow encryption on electronic devices, only 7% for pioneers.
- Pioneers understand the technology available: almost 80% of them have a form of mobile application coordination, compared with 12% of skeptics.

Variations in European countries and industries:

Countries:

- The Nordic countries and the Germany / Switzerland tandem (DCH) are leading countries in terms of general maturity in the BYOD approach;
- The Iberian Peninsula and Italy see most of BYOD's challenges. These countries also had the highest proportion of skeptics.

Industries:

- The communications industry was a general leader.
- At the other end of the top, the financial services industry.
- An interesting aspect is that the media industry has the largest proportion of pioneers and the lowest financial services industry; the public sector has the highest number of skeptics, and the communications industry has the least.

BYOD practices - developed in the right direction - can bring real business benefits; from increased employee productivity to reduced IT and hardware costs, and increased ability to attract young talent.

2.2. BYOD in the big and very big companies from România

CIO Council Romania, made the first edition of the study on the application of the BYOD concept in large and very large companies in Romania. It is a practical, user-friendly study that addresses the application or non-application of the IT concept for business efficiency, as well as the intention to apply it in the immediate future [4].

The study was based on the interpretation of the opinions, recommendations and forecasts of over 100 IT managers from large and very large companies operating in Romania. Also, the main reasons for applying / not applying the concept were studied.

The study [4] proves to be extremely important at a time when the extension of BYOD practices is slowed down by IT security concerns. This is the main reason why we wanted to find through this study [4] what is the de facto situation in Romania in large and very large enterprises, which generates the largest volumes of business in our country.

The results of the study [4] show that these concepts are still at the beginning of the road in Romania, at least in terms of large and very large enterprises. The adoption rate of concepts is not yet significant (as opposed to, for example, the concept of Cloud Computing) and the policies and procedures for this adoption are not clearly defined on a large scale.

Key values found in the study [4] and related to mobility:

- Only 50% of companies believe that the implementation of mobility is economically justified;
- 60% of companies are addressing ad hoc mobility without having a clear strategy or policy;
- In 20% of companies, the policies in force are not being respected, with tactile acceptance of personal devices.

Key values discovered by the study and related to BYOD:

- 38% of respondents say there is a policy in their company towards BYOD.
- Attitude towards BYOD varies significantly depending on the device used.
- BYOD's silent adoption is a significant phenomenon within companies, with rates ranging from 11% for smart phones to 21% for tablets.

The purpose of the study was not to advise companies on adopting these concepts in Romania. As such, it can only be a simple radiography that highlights the good and bad situations already existing [5]. Any future editions of this study will have the gift of highlighting the true market trend, at least from large and very large businesses.

3. CYOD, THE ALTERNATIVE OF BYOD PHENOMENY

Securing a BYOD device fleet becomes extremely difficult, especially in the context of a variety of devices on the market, and many employees store personal and professional personal data regardless of whether the device is personal or belong to the employer.

Thus, a new alternative BYOD concept now proposes to reduce the risks. CYOD - (Chooses Your Own Device) allows employees the freedom to choose to work on a particular device they know and control, with the company providing a pre-approved list of devices from which employees can choose.

The security benefits of the CYOD program are immense, as each security device can be preinstalled with a security solution and pre-defined firewall and network settings of a dedicated administrator. The administration of a small number of different specifications allows record keeping to be used and ensures that employees comply with data and information management requirements.

The disadvantage of those companies that offer employees the freedom of the BYOD program is the relative lack of luxury of choice. A company must, however, provide a wide range of devices as part of the CYOD program to be attractive to employees and to acquire their interest.

The CYOD phenomenon begins to gain ground in front of BYOD, for obvious reasons. The influx of personal devices operated by office workers has in recent years meant significant savings for hardware

acquisition, but has also led to the emergence of difficult to predict.

Following the accommodation of companies and employees with the BYOD program, the emergence of the new CYOD program proves the need and also the efficiency of the transformation and development of BYOD into a new form of use of devices in the workplace.

Regardless of the employee-embedded enterprise model, security of data and information is essential, and security companies offer a full range of business security solutions.

There are a number of simple steps that any company, regardless of business or size, has to follow to ensure infrastructure and data security.

Choosing the strategy and products that support employees' productivity. It is recommended that you thoroughly test your company's devices from an employee perspective and define the best work pattern for your organization, whether BYOD or CYOD. At the same time, each member of the IT department responsible for mobile devices must have a clear understanding of the issues they are facing**.**

Regardless of the model implemented in the company - BYOD or CYOD, a top-of-the-range product has to be implemented to prevent data loss. This product needs to be well integrated with existing mobile products and current strategy. Selected products must be performance-packed and designed to prevent confusion of company's IP, organization, data, and confidential information. By default, company data will not be copied to the currently available small devices or any other portable and smart gadgets that employees might have in the future.

Every company has to compose the ideal team for a particular project.

Mobility projects involve IT, legal, human resources, security, and business operations. All of these groups have an interest in the productivity and security of the workspace and mobile devices used in the company. Each will have a specific specification and will have to resort to concessions to keep the project in the market dynamics of mobile devices. Partnerships with specialized security companies that have a vast array of resources can result in team alignment and problem-solving for mobile devices and data security, no matter who owns these devices in the business environment.

4. CONCLUSIONS

It is good to see that some organizations in Europe adopt BYOD to take advantage of these benefits, but the report revealed a real cause for concern in the skepticism of many other companies in accepting that BYOD is developing around them in their immediate vicinity and in adopt this change for its own benefit.

The security issue seems to have pushed many organizations in Europe into denial and resistance against BYOD. However, technologies such as containerization, end-to-end encryption, and application and device management, supplemented by uniform company data storage [6], can secure BYOD practices.

It is vital for parties involved in the BYOD ecosystem to clarify this situation within their own organizations. This should lead to a major increase in the number of European organizations benefiting from the benefits of BYOD practices.

Mobility brings more benefits to companies with formalized mobile strategies, revealing a huge gap in mobile business results. It was found last year that mobility generated revenue for 75% of companies with the most comprehensive strategies, compared with 30% of companies with less developed strategies.

Mobility success includes business strategy, business applications, and official measurement of results, in addition to infrastructure engineering. A fully planned approach and coherence can make mobility a real business factor, while an incoherent program creates the risk of a tactical value rather than a strategic solution for the organization [7].

Approximately 60% of organizations have a mobile strategy, but there are different levels of maturity. Most mobile mature companies, known as mobile companies, account for 21%

of the total. Another 40% of companies are committed to this, with strategies and policies, but without pro-active government.
8% of companies are "mobile-minded," with packages of mobile initiatives and policies, but without a global strategy or government.
11% of organizations do not have any mobile strategy set up, nor do politicians or governments in this regard.

5. REFERENCES

[1] Ștefan Iovan, Cristian Ivănuș: *The Mobility – A Trend in Multinational Companies*, Târgu Jiu: "Academica Brâncuşi" Publisher, *Annals of the "Constantin Brâncuşi" University, Engineering Series,* Issue **3**/2017, (***CONFERENG 2017***), pag. 175 – 180, (2017);
[2] **** * ****: *Global Corporate IT Security Risks 2013,* *http://www.kaspersky.ro/out?key=C4ErGhweJK9Hw*
[3] **** * *** : *Oracle BYOD Index Report, imap://rmaier@mail.agora.ro:143/fetch>UID>.INBOX>281261*
[4] **** * *** : *http://www.agora.ro/sites/default/files/revised_brosura_BYOD_v2_mai.pdf*
[5] Ștefan Iovan, Cristian Ivănuș: *European Economic Growth through the Mobilization of Innovation and Entrepreneurship*, Proc. of 16th European Conference (***E_COMM_LINE 2015***), București, România, (2015);
[6] Cristian Ivănuș, Ștefan Iovan: *Providing Products and Services in Cloud Computing Technology*, Proc. of 14th European Conference (***E_COMM_LINE 2013***), București, România, (2013);
[7] Ștefan Iovan, Cristian Ivănuș: *Software applications for mobile and mobile protection*, Târgu Jiu: "Academica Brâncuşi" Publisher, *Annals of the "Constantin Brâncuşi" University, Fiability & Durability Series*, Issue: **1(21)**, (***SYMECH 2018***), pag. 263 - 268, (2018);