Managerial decision options about BYOD with the consideration of shadow IT

Pál Fehér-Polgár

Óbuda University, Keleti Faculty of Business and Management, Budapest,

Hungary, feherpolgar.pal@kgk.uni-obuda.hu

***Abstract**: In recent years we have seen the rise and spread of BYOD (Bring Your Own Device) world wide. In this paper I will show definitions by security researchers for BYOD, and a proposed definitions for my research. When we are talking about using our own smart devices for work we cannot oversee the possibility to use them without approval of the management of the firm. Creating a secoundary non-official IT enviorinment in the firm. I will show the positive and negative side of this phonomonem and as a conclusion I will give managerial decision options for the firm for BYOD.*

***Keywords**: BYOD, Shadow IT, Enterprise Security*

Introduction

Definition of BYOD

BYOD is an acronym for Bring Your Own Device. [1][2][3][4] The term of device could mean in general a wide variety of employee owned tools and hardware, although the accepted meaning of device in this topic is IT devices, such as laptops, tablets, smart phones.

Application of BYOD

In my Information and communications technology ICT security research I narrow this definition to smartphones and tablets, as these types of devices are not always considered and used by the employees as fully flagged computers. On the other hand, these devices could be capable to have access to corporate data and can work (open, edit, insert, delete etc..) on that data also. Thus, in many aspects they have to be managed as one node in the IT infrastructure.[5][6][7]

For these devices, the most important use case is communication; e-mails and other messaging where corporate data need to be flowed between parties. Also, with these devices we can use the network infrastructure of the firm, reaching network drives, shared documents, shared databases, even the Management Information System of the firm, and much more. Just like with a computer. The question is, what kind of risks are there, and how to regulate?

In 2012 Cisco questioned IT decision makers in enterprises (>=1,000 employees) and midsize (500-999) companies in eight countries and three regions. [8]

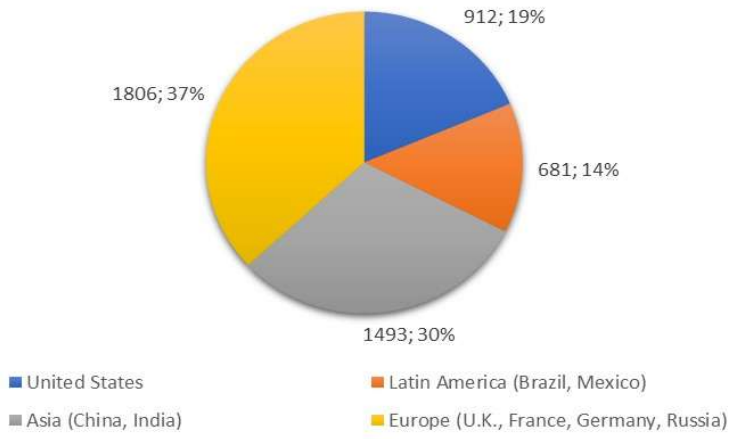

Figure 1. Regions and countries of the sample

Source: Cisco BYOD: A Global Perspective Harnessing Employee-Led Innovation

The sample contained 600 enterprises, 312 midsize from the U.S. and 2805 enterprises, 1175 midsize companies from the other three regions. The first interesting question was why an employee would want to use their own devices for work. As we can see on the second figure, the most important reasons are related to convenience and freedom of usage in the question of time, space and used hardware and software.

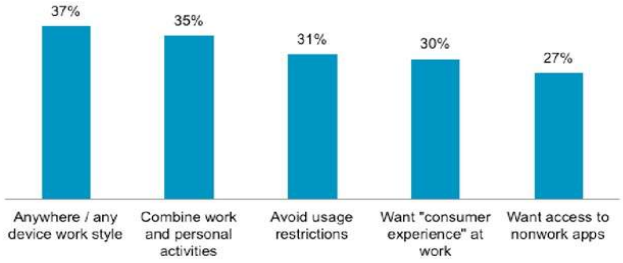

Figure 2. Top reasons Employees Use Their Own Devices for Work

Source: Cisco BYOD: A Global Perspective Harnessing Employee-Led Innovation

For these requests from the employees the IT department of the firm needs to give an answer. In the research Cisco has given four answers.

As an answer for this the research included a question about on which level is BYOD is accepted by the firms.

- All devices supported

- Selected devices supported
- Network access but no IT support
- Employee devices prohibited

As we can see the two most accepting regions were the U.S. and India (31%, 30%) where all devices were supported. It is also interesting that in average. more than seventy percent of the answerers said they support employee devices (selected, or all kind). This means that many companies need to deal with BYOD. On the other hand, in the European region the number of companies where BYOD is prohibited is higher than in the other regions. Also, in this region the highest percent of the companies which enabled only network access but no IT support. [8]

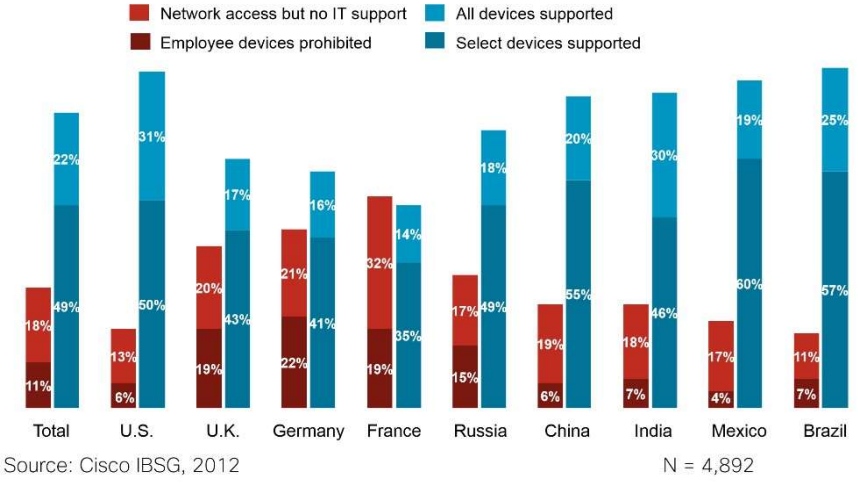

Figure 3. Levels of Company IT Support for Employee-Owned Devices
Source: Cisco BYOD: A Global Perspective Harnessing Employee-Led Innovation

In 2016 Ipsos made a Europe wide research about the digital trends in 20 countries in the sector of small- medium- and microenterprises. In Hungary, the 57% of small enterprises answered that they support BYOD, which had a growing trend since in 2014 they measured a 38% acceptancy. While the 67% microenterprises answered positively to this question, and the medium size answerers' acceptancy rate was 51%. [9]

Shadow IT

Definition of shadow IT

Shadow IT, also known as Stealth IT or Client IT, are Information technology (IT) systems built and used within organizations without explicit organizational approval. For example, systems specified and deployed by departments other than the IT department for testing and creating new services. [10][11][12][13]

Many IT specialists consider shadow IT as an important source of innovation. As such systems may become prototypes for future approved IT solutions. [14]

On the other hand, shadow IT solutions often not in line with organizational requirements for control, documentation, security, reliability, and in other aspects of ICT security.

Most important risks of BYOD consideration of shadow IT

From a theoretical point of view the most important risk sources of using self-owned mobile devices

1. Control over the corporate data, as how we can keep it, as the employee might transfer it to devices without of permission and carefulness.
2. The type of the device, as these devices by chance cannot be controlled by the firm.
3. When feeling security is „too inconvenient", as we could have seen convenience is a motivator for the employee and it can lead to usage of risky solutions in hardware and/or software.
4. Unregulated usage of self-owned devices. As valuable information can be lost via unprotected, uncontrolled devices.

Other important questions about risk sources of using self-owned mobile devices:

1. The quality and security of the network service when the device connects to the network of the firm.
2. Backups – how does the device makes backups for example for network failure? Does the device have a secure drive which cannot be reached other than our secured application?
3. The corporate data can be reached all day, from all networks, or could we make time and space regulations?
4. Can we lock out the user? For example, after three unsuccessful login attempts?
5. How do we authenticate the user? From user level (passwords, fingerprint) or from device level (device ID, secure chip, SIM card) or we are mixing these?
6. Can a user reach shared mailboxes and shared folders? For example, can a secretary reach his or her director's mailbox and their mails?
7. Can the employee connect a data storage device (Memory card, USB stick, etc.) and reach the data on it, from the secure application, and transfer data to the secure partition?

The strategic answers that managers can give to the risks

In the questionaire of Cisco we could see the levels of IT support for employee owned devices. On the managerial level of the firm this can be transformed as four level of managerial decision as the following:

- Tolerate
- Subject of vocal or written permission
- Encourage
- Completely ban

As a preparation for this managerial decision according to Lazanyi [15] the uncertainty can be reduced with the combination of the following procedures:

- Collect as much information about the viable options as it is possible, considering that the state of complete information cannot be achieved, and the consumable time and costs.
- Research for information about similar decisions from the past of the firm or from outside information sources and transform that knowledge for the current situation.
- Selection of a reference decision maker who can immersively reduce the uncertainty.

For selecting the appropriate decision option the Skill-Will matrix can be used as a managerial tool. It has two dimensions, one is for the willingness of the employee to applicate BYOD, while the other dimension is the skill of the employee. This skill dimension should include the usage skills of ITC devices with a strong consideration of the ICT security awareness of the employee.

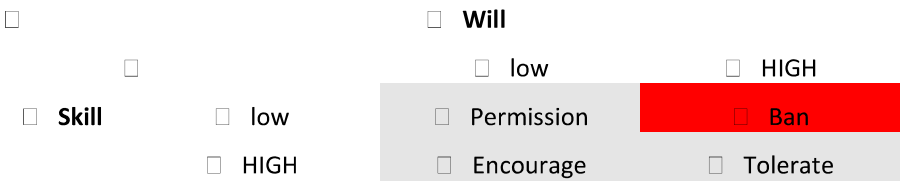

Figure 4. Skill-Will matrix with strategical decision options for managers on the application of BYOD
Source: Own edition of the Skill-Will matrix

Recommendations

Planning and managerial decision are needed on the following questions. What are the types of data, in what circumstances, and in what form (i.e. Only in the secure storage of the device) can be present on mobile devices? The selection of the usable devices has to be decided and also it is a have to to define the use cases and usage parameters when employees can use their own devices. To achieve this, we need proper IT and information security regulations and usage! Beside this we need to have appropriate level of security consciousness in information security.

References

[1] S. Blizzard (2015) Coming full circle: are there benefits to BYOD?, Computer Fraud & Security, Volume 2015, Issue 2, 2015, Pages 18-20, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(15)30010-5.

[2] A. Hovav, F. F. Putri (2016) This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive and Mobile Computing, Volume 32, 2016, Pages 35-49, ISSN 1574-1192, https://doi.org/10.1016/j.pmcj.2016.06.007.

[3] N. Zahadat, P. Blessner, T. Blackburn, B. A. Olson (2015) BYOD security engineering: A framework and its analysis, Computers & Security, Volume 55, 2015, Pages 81-99, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2015.06.011.

[4] U. Vignesh, S. Asha (2015) Modifying Security Policies Towards BYOD, Procedia Computer Science, Volume 50, 2015, Pages 511-516, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.04.023.

[5] G. Disterer, C. Kleiner (2013) BYOD Bring Your Own Device, Procedia Technology, Volume 9, 2013, Pages 43-53, ISSN 2212-0173, https://doi.org/10.1016/j.protcy.2013.12.005.

[6] B. Tokuyoshi (2013) The security implications of BYOD, Network Security, Volume 2013, Issue 4, 2013, Pages 12-13, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(13)70050-3.

[7] E. Kadena, T. Kovács (2017) The need for BYOD security strategy, HADMÉRNÖK 12 : 4 pp. 138-145. , 8 p.

[8] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf, L Buckalew (2012) BYOD: A Global Perspective Harnessing Employee-Led Innovation, Cisco IBSG Horizons https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf

[9] E. Kis (2016) Felhőben (lehetnének) jobbak a kkv-k, Computerworld 2016 június 8. https://computerworld.hu/uzlet/felhoben-lehetnenek-jobbak-a-kkv-k-211561.html

[10] RSA (2007) The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk

[11] J. Nelson (2015) Shadow IT is a reality for 90% of CIOs". Logicalis. http://cxounplugged.com/2015/11/shadow-it-is-a-reality-for-most-cios/

[12] A. Stuart (2016) The dangers of file sync and sharing services, Computer Fraud & Security, Volume 2016, Issue 11, 2016, Pages 10-12, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(16)30090-2.

[13] Browne, Sean, Lang, Michael, & Golden, William. (2016). Contextualising the insider threat: a mixed method study. Paper presented at the 11th Pre-ICIS Workshop on Information Security and Privacy (SIGSEC), Dublin, Ireland, 10 December.

[14] M.J. Handel, S. Poltrock (2011) Working around official applications: experiences from a large engineering project CSCW '11: Proceedings of the ACM 2011 conference on Computer supported cooperative work. pp. 309–312. doi:10.1145/1958824.1958870.

[15] Lazányi, K. (2016). A biztonsági kultúra szerepe a vezetői döntések támogatásában= The role of safety culture in supporting the leaders' decision making. Taylor, 8(1), 143-150.