The Influence of the Use of Mobile Devices and the Cloud Computing in Organizations

Fernando Moreira[1], Manuel Pérez Cota[2], and Ramiro Gonçalves[3,4]

[1] Universidade Portucalense, DEGI, Rua Dr. António Bernardino de Almeida, 541, Porto, Portugal
[2] Diretor grupo SI1-GEAC, Universidade de Vigo, Vigo, Espanha
[3] UTAD, Vila Real, Portugal
[4] INESC TEC, Porto, Portugal
fmoreira@upt.pt, mpcota@uvigo.es, ramiro@utad.pt

Abstract. In the last decade, companies tend to become virtualized. This virtualization is due in large part to developments in the use of mobile platforms and the impact on their infrastructure. The concept of BYOD (Bring Your Own Device) adoption and use of cloud computing are having profound implications for how the technologies are being used, as well as the interaction between individuals and these technologies. In this context, we conducted a study based on a questionnaire about the impact of the use of mobile devices and the cloud in organizations, taking into consideration their use in performing professional and personal tasks. With the questionnaire and its subsequent analysis it was found that organizations have a lack of understanding about almost all of the implications and consequences of the use of mobile devices and the cloud.

Keywords: BYOD, Mobile devices, Cloud, Organizations.

1 Introduction

The growth of mobile technology has changed the mode of operation of citizens in the day-to-day basis, either in your personal life or in your workplace [1]. As mobile platforms and infrastructures are evolving, the use of cloud computing has profound implications for the way the technologies are being used, as well as the interaction between individuals and these technologies. In this context it is relevant and necessary to identify the main changes expected in the next 5-10 years that may affect the work environment. For example, in 2015 the BYOD (bring your own device) concept and the use of mobile devices (*smatphones*, *pablets*, tablets and laptops) are generalized almost as well as cloud computing [2].

Mobile devices are appearing on the market at a rapid rhythm [3], [4], with increasing capabilities, and applications are increasingly sophisticated; however, the technological point of view will have a slower evolution, so the use of the cloud will be driven by facilities that offer either in storage or processing capability. In this context, it begins to assist the migration of services from mobile devices to the cloud. For example, Google uses the Google Drive and Quickoffice cloud-based, and Apple

Á. Rocha et al. (eds.), *New Contributions in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 353, DOI: 10.1007/978-3-319-16486-1_28

through iCloud expands to cloud the capacity of their devices for data synchronization, photographs, etc. Actually, mobile devices are becoming more data terminals, than in stand-alone [5] platforms.

A few years ago employees received a laptop computer and password to access the organization's network where they went to work. Today, the current generation arrives on the first day of work "loaded" with their mobile devices and expects to integrate them into day-to-day work, so that they can use them anytime and anywhere [6].

At this moment, organizations no longer give part of tools (devices) to fulfill the tasks, but the possibility of employees bringing their own devices is increasing, which is one of the latest trends, the BYOD. This situation has a positive side, which is the ability of employees to work with the equipment they like, and therefore may be more productive, but it raises security concerns because now the question to consider is no longer just the user, but the device or devices which it uses [7].

In this context, the department of information technology (IT) need to take into account the new facts brought by the BYOD. According to the study by Connected World [8], younger professionals and students have difficulty understanding the barrier between personal and professional life, where 33% of students do not mind to share their personal life online, because they would rather work from home or office, using social networks and cloud applications [6].

Emerging trends, including cloud computing and BYOD, complicate the task of organizations, increasing the "surface" of attack while decreasing effectiveness of traditional security methods [9]. For instance, according to the Verizon Data Breach Investigations report [10], the hacktivists organization was responsible for 100 million of 174 million stolen records through attacks on security breaches in data protection.

In a nutshell, on one hand, new ways of working models are emerging, where the BYOD is one of the most interesting and challenging and, on the other hand, the mobility, the "consumerization" [11] and the cloud is a key factor allowing a change in the way people is working. However, security issues related to mobile devices and data are a major barrier to the adoption of these new models of IT [12], [13].

In this context, we conducted a study on the influence of the utilization of mobile devices and the cloud in organizations. Taking into account the rapid proliferation of mobile devices in their own personal and professional execution of tasks as well with the use of cloud as a way to enhance or extend the capacity of performance in resolving the professional and personal tasks, without a "conscious" concern about the dangers of sharing data organizations, between devices and systems.

The paper is organized as follows: In the second section is a description of the thematic context, while the third section presents the research methodology. The fourth section is devoted to the presentation and discussion of the results, and the last section is devoted to presenting the conclusions.

2 Context

2.1 Cloud Computing

Cloud computing refers to the use of software, network infrastructure and capability to provide resources to users on-demand and the service measured through the business

model pay-per-use. It is a heterogeneous architecture, which benefits from a number of different technologies to provide remote services.

The National Institute of Standards and Technology (NIST) has identified five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (Software as a Service, Platform as a Service and Infrastructure as a Service) and four development models (Private cloud, Community cloud, public cloud and Hybrid cloud), shared by all systems of cloud [14], [15], [16].

The main security concern in cloud computing is data access by unauthorized individuals or systems. When data of an organization are moved placed in the cloud, the data owner is inside the organization, while the supplier, which is outside the organization is in fact from the time of placement of the data in the cloud actual "owner" of the data. The data need to be protected through the use of protection mechanisms (encryption, for example) in order to facilitate the migration to the cloud or between clouds. Beyond this concern is also necessary to note the data over the network, and how applications use data [17].

Many of the attacks on cloud computing are related to their distributed and shared [18] environments. Some studies have indicated that attacks on web services represent more than 60% of all attempts to explore online [19] vulnerabilities. These attacks can be considered as the more traditional threats, which are also of concern in cloud [20] environments. Moreover, some threats are specific for cloud environments because of the multi-tenant nature of the servers in the cloud and / or the use of virtual machines, which form the base of the cloud computing paradigm [21].

2.2 BYOD

BYOD is an acronym derived from the concept of "consumerization" [11] which describes the growing trend of new information technology to emerge first in the consumer market and then spread to the organizations (business and government). Currently, the "consumerization" involves mobile devices, but also services (DocBox, Dropbox, GoogleDrive, etc.) and social networks (Facebook, Twitter, Linkedin, etc.), as well as e-mail services. All these services, which are hosted in the cloud, are used by a new generation of devices, and are increasingly used in personal and professional [12] activities.

A survey conducted by Gartner Inc. shows that "*By 2017, half of Employers will require employees to supply their own device for work purposes*" [22]. However, this practice can result in potential security breaches and risks, because these devices will have access to data and networks of organizations, somehow outside the control of those responsible for the management of IT [23]. In another study presented by CISCO [24] the issue of mobility is widespread: 78% of employees have a mobile device for work and 44% are knowledge workers who work remotely at least one day per week, with a cost savings of about $ 2,500 / year / person. Based on the same study, companies are changing their IT infrastructures, 75% of them expect the use of mobile devices by employees in large numbers to safely connect to corporate networks.

With the purpose to perceive the benefits of BYOD is necessary to address two key elements: the distribution of applications and data to multiple mobile platforms and security issues. To address these concerns, it is important to understand what employees wish to have. Basically, they want to act on the working model "*any device, anywhere,*" perform personal activities during work and work activities during personal time.

Mobile devices present security issues when stolen, lost, exposed to viruses, etc. For example, in July 2012, 54% of major incidents of infringement reported by the US Department of Health and Human Services Office for Civil Rights, since September 2009, involved the loss or theft of unencrypted devices [25]. Another example that illustrates these problems is the case of the Massachusetts Eye and Ear Hospital has agreed to pay $ 1.5 million after a doctor had reported that his laptop computer was stolen and had not encrypted the data with more than 3000 records patients [26].

The organizations are losing control over who has access to the corporate network. The simple fact that more employees are using mobile devices in their work means a potential increase in data loss due to theft or loss of devices. Additionally, the increased use of shared files on cloud services by organizations and employees to increase efficiency and reduce costs, often without the permission of the organization, increase the potential of data being stolen or compromised [12].

Although there are encryption schemes for mobile devices, monitoring systems, antivirus software, authentication, etc., exists on the part of employees, a non widespread compliance with the security measures implemented in organizations with which they are associated. According to [27] a large part of the owners of mobile devices do not use a password or PIN to lock your device and let the device recorded the username and password of the installed applications to make data synchronization whenever necessary so that they do not always have to enter the user name and password.

Some organizations have adopted cloud storage, which provides mobile access to work data, and applications; however, so that an employee performs the download of a corporate file, the organization loses complete control over it. Furthermore, applications of mobile devices present security risks in any system of any organization, as can be seen in [28] *"... many apps on the market gather and send user information, such as name, password, location, demographic, or any other information, back to the software developers, which raises additional security concerns* ".

3 Research Methodology

The purpose of this section is to describe the procedures used to collect data that are the basis for this research. The main feature of the scientific method is an organized research, strict control of the use of observations and theoretical knowledge. The present study was based on quantitative research methodology.

Data collected for a quantitative research using questionnaires, requires special care because it is not enough to collect responses on the issues of interest, but also, how to make a proper statistical analysis to validate the results.

Aspects such as the sample size the way the questionnaire is prepared, the formulation of questions, data analysis, margins of error, the process of selection of individuals, who should compose the sample, among others, are important and must be taken into consideration for any investigation.

For the present study, we used the methodology of quantitative research, since it is more appropriate to determine the opinions and attitudes of the respondent based on structured questionnaires. In this approach, data is collected through structured questionnaires, and clear goals in order to ensure uniform compression of the respondents and a consequent standardization of results.

The method of the questionnaire, according to [29], is recommended when you want to know a population, to analyze social phenomena and, in cases where it is necessary to inquire a great number of people about a certain subject. The questionnaire before being made available online was subjected to the evaluation of five experts in the field. The objective of this study was to obtain answers that will measure the influence of the utilization of mobile devices and cloud in organizations. The quantitative study was based on an online[1] questionnaire with 33 questions. The questionnaire was online for 120 days, and 430 valid responses were received.

4 Data Analysis

The analysis of results will be performed in the following three sections. The first section presents a context of responses obtained. In the second section will be analyzed and discussed the issues related to mobile devices and the cloud. The last section will be devoted to analysis and discussion of results for mobile data access. Due to space limitations will be presented and discussed the results considered more relevant, since the questionnaire, as mentioned above, consists of 33 questions.

4.1 Context

After the process and analysis of data obtained from the valid responses to the questionnaires, the first observation that can be done relatively to the first part is the number of responses obtained, thus managing to include a great number of companies and sectors; the total number of 20 sectors of activity were obtained responses from 15 (Fig.1), where it can highlight the responses of sectors "Vendor / Integrator solutions e-business" and "Consulting services and businesses," with 17% and 13%, respectively. The geographical distribution and the size of the responding organizations can be considered very positive aspects. As regards the size of the organizations are achieved responses in all ranges, i.e. from organizations with fewer than 30 employees to companies with 1,000 to 5,000 employees.

The great majority of the answers (88%), illustrate that almost all responded that were involved or familiar with the strategies and / or practices of the organization concerning the use of mobile devices and the cloud, which illustrates the relevance of the study, for those organizations. Only 12% have no such concerns.

[1] https://docs.google.com/forms/d/1n6VxsSs8RUg4W3-waLzR_HwGfNMwKcRA_QhPJHzk_sA/viewform?c=0&w=1

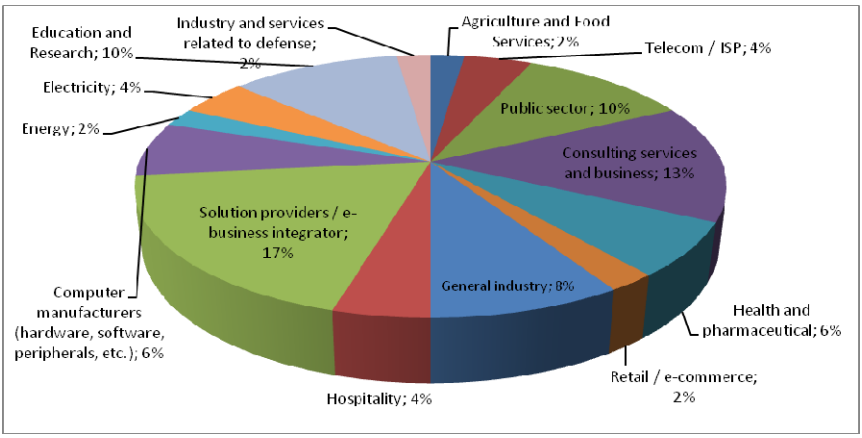

Fig. 1. What type of activity that best describes your organization?

As a first analysis it is possible to see that this issue is a matter of concern within organizations due to the benefits but also the risks that the use of these technologies can bring to organizations. However, it is not sufficient to be involved or familiar with these issues, is necessary to understand, whether it is being done proactively appropriate monitoring, and what action is being taken.

4.2 Mobile Devices and Cloud

In the introductory questions to the theme, we selected only three questions, but presenting only a chart to illustrate how respondents feel familiar with this topic.

The first question on familiarity with the topic, 74% of respondents are aware of the efforts that the organization, where it operates, is doing to data protection on mobile devices.

The second question of the analysis is related to the storage of data in the cloud and by observation of the values obtained; we conclude that there is a greater concern to 75% of the efforts of organizations to protect data in the cloud. The question is legitimate be asked is whether those efforts are being carried out properly and what effect are they having on the organizations.

As can be seen in Fig. 2, this question presents a set of eight statements where the respondents had to sort through a numeric scale of 1 to 5 (1 – Totally disagree 2 – Somewhat disagree, 3 – I have no opinion, 4 – Somewhat agree, 5 – Strongly agree). The eight statements are:

1 The productivity of employees sometimes conflicts with the effort of the organization to protect data on mobile devices.
2 The risk of data stored or accessed on unsecured mobile devices is growing.
3 The employees in my organization understand the importance of protecting data on mobile devices.
4 It is difficult to detect employees who use unsecured mobile devices to access data.

5 It is difficult to prevent employees using insecure mobile devices to access the data.
6 My organization understands the risks of data on mobile devices.
7 My organization is vigilant in protecting data on mobile devices.
8 My organization considers data protection on mobile devices as a high priority.

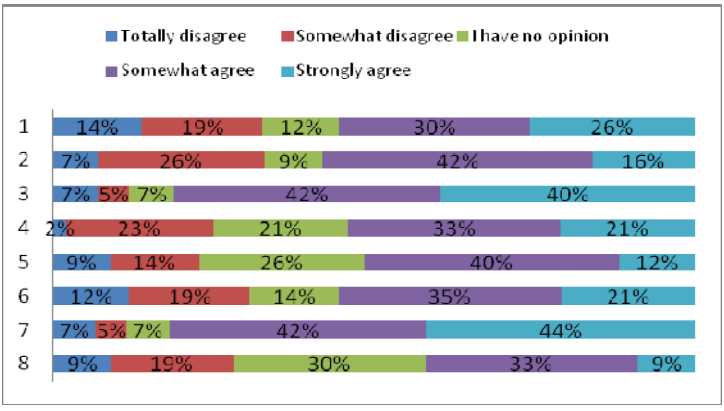

Fig. 2. Graphical results of 8 answers about data protection on mobile devices

In a first analysis of the results of Fig.2, we see that almost all statements obtained a score above 50% (when added scores 4 – I agree partially with 5 – Strongly agree) which clearly demonstrates the existing concern about data security on mobile devices. For example, it is possible to highlight the percentage of responses to the statement "*The employees in my organization understand the importance of protecting data on mobile devices*", where the total percentage of the last two points is over 80%.

4.3 Mobile Access to Data

Mobile access to data is another component of this study and after verifying that the organizations are familiar with these topics was necessary to understand how and the means for users to access the data. The obtained results allow concluding that more than half (55%) of organizations allow access to organizational data via employees' mobile devices. The results obtained on the question "*Does your organization have a policy which specifies the use of mobile devices of employees (BYOD) in the workplace?*" demonstrate some contradiction with the results discussed above, i.e. the respondents recognize the problems, but 61% of the organizations do not have a policy that specifies how employees' mobile devices should be used in the workplace.

To aggravate this trend the results to the question "*What percentage of mobile devices with access to all the organization's data with adequate security features?*" are very illustrative, since 51% of respondents indicate that they do not know or do not exist the appropriate security solutions on mobile devices that have access to all the organization's data.

The results presented in Fig. 3 and 4 are an example of the lack of understanding the implications and consequences the use of mobile devices and cloud in organizations. In Fig. 3, the graph, it is possible observe the problem dimension, since 86% of respondents answered do not know how many, and which, the organization's data that exist in the mobile devices used in the organization. While Fig. 4, 81% did not know the quantity of data residing in file-sharing applications in the cloud.

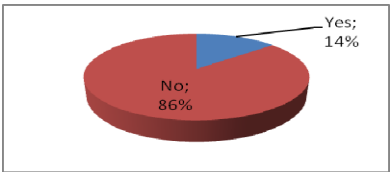

Fig. 3. Do you know how many, and what data the organization that exist in mobile devices used in your organization?

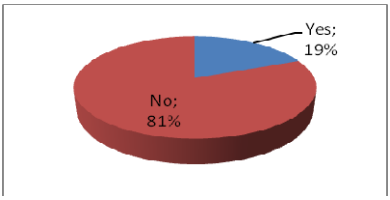

Fig. 4. Do you know the quantity of data residing in file-sharing applications in the cloud?

The analysis and discussion presented in this section, only shows part of the results of the survey, although it may be concluded that organizations know these issues (BYOD and Cloud), allowing its use in day-to-day recognize that there are risks and therefore consequences for their business, but a large part them, have no control over the employees, their devices and, more seriously, about information organizations (where is that information is and state that, as well as their status). Thus, it becomes important to adopt measures that help organizations overcome these limitations, such as how they can integrate mobile devices in their day-to-day.

5 Conclusion

In the last decade, companies have become highly virtualized due to outsourcing, the workforce has become more distributed (a mix of employees of the organization, with employees hired per project), workplaces increasingly distributed (in work organization offices and home-based), places of work outsourced (such as call centers), and increasingly digital nomad employees, with the philosophy of working anytime and anywhere.

This change in paradigm of organizations leads to the development of a new ecosystem where security is no longer just an IT issue or technology – is fundamentally a management problem that few organizations are addressing appropriately.

With the purpose of understand this new change, a study based on a questionnaire and its subsequent analysis was conducted to see the influence of the utilization of mobile devices and the cloud in organizations. One of the interesting results was the diversity of activity sectors that accede to study as well as the heterogeneity in the size of the number of employees (ranging from 30 organizations and 5,000 employees), it was noticed clearly, it is not yet possible, with these results make a generalization, the weaknesses that organizations have on these issues, despite knowing that these problems exist. What is interesting is to verify that organizations have a lack of understanding of the implications and consequences of using mobile devices and the cloud, separately or simultaneously. The above statement may be supplemented by the results obtained in relation to how and what data the organization that exists in the mobile devices used in the organization as well as the quantity of data residing in file-sharing applications in the cloud.

These results show interesting indicators for performing a set of recommendations and developing security frameworks that include not only the technological aspects of security across all levels of the hierarchy of an organization, and having a special focus on complete integration of employees (current and next generation) in this new ecosystem and especially in the training plans.

References

1. Mobile Marketing Statistics, http://www.smartinsights.com/mobile-marketing/mobile-mrketing-analytics/mobile-marketing-statistics/
2. Schubert, L., Jeffery, K., Neidecker-Lutz, B.: A Roadmap for Advanced Cloud Technologies under H(2020), http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-expert-group/roadmap-dec2012-vfinal.pdf
3. Communities Dominate Brands, http://communities-dominate.blogs.com/brands/2012/06/massive-milestones-in-mobile-will-these-numbers-change-your-mobile-strategy.html
4. Business Insider, http://www.businessinsider.com/2012-03-28/research/31248281_1_ios-android-hard-drive.html
5. Linthicum, D.: Mobile's next great leap will happen in the cloud (2014), http://www.infoworld.com/print/236891
6. Thomson, G.: BYOD: enabling the chaos. Network Security 2012(2), 5–8 (2012)
7. Mansfield-Devine, S.: Interview: BYOD and the enterprise network. Computer Fraud & Security 2012(4), 14–17 (2012)
8. Cisco ConnectedWorld Technology Report. Cisco, http://www.cisco.com/en/US/netsol/ns1120/index.html
9. Mike, P.: The state of information security. Network Security 2012(7), 1–9 (2012)
10. Verizon, Data Breach Investigation Report (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf
11. Consumerization, http://en.wikipedia.org/wiki/Consumerization
12. Scarfò, A.: New security perspectives around BYOD, Seventh International Conference on Broadband, Wireless Computing. In: Communication and Applications, pp. 446–451. IEEE Computer Society (2012), doi:10.1109/BWCCA.2012.79

13. Romer, H.: Best practices for BYOD security. Computer Fraud & Security 7, 13–15 (2014), http://dx.doi.org/10.1016/S1361-3723
14. Vaquero, L.M., Rodero-Merino, L., Caceres, J., Lindner, M.: A Break in the Clouds: Towards a Cloud Definition, SIGCOMM Comput. Commun. Rev. 39, 50–55 (2008)
15. Mell, P., Grance, T.: A NIST Definition of Cloud Computing. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
16. Cota, M.P., Gonçalves, R., Moreira, F.: Cloud Computing Decisions in Real Enterprises. Agile Estimation Techniques and Innovative Approaches to Software Process Improvement, pp. 313–330. Information Science Reference (IGI), Hershey (2014), doi:10.4018/978-1-4666-5182-1.ch018
17. Lokhande, T.S., Shelke, R.R.: A Review Paper on Cloud Computing Security. International Journal of Advanced Research in Computer Science 4(6), 70–73 (2013)
18. Farhad, A., Seyed, S., Athula, G.: Cloud Computing: Security and Reliability Issues, Communications of the IBIMA, Article ID 655710, 12 pages (2013), doi:10.5171/2013.655710
19. Murugaboopathi, G., Chandravathy, C., Vinoth Kumar, P.: Study on Cloud Computing and Security Approaches. International Journal of Soft Computing and Engineering (IJSCE) 3(-1), 212–215 (2013) ISSN: 2231-2307
20. Takabi, H., Joshi, J.B.D., Ahn, G.J.: Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, vol. 8, pp. 24–31. IEEE (2010)
21. Chen, Y., Paxson, V., Katz, R.H.: What's New about Cloud Computing Security? EECS Department, University of California, Berkeley (2010)
22. Gartner, https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf
23. Leavitt, N.: Today's Mobile Security Requires a New Approach, Computer, vol. 46(11), pp. 16–19. IEEE Computer Society, doi:10.1109/MC.2013.400
24. ISBG, http://newsroom.cisco.com/release/854754/Cisco-Study-IT-Saying-Yes-To-BYOD
25. Department, U.S.: US Department of Health and Human Services. Health information privacy: breaches affecting 500 or more individuals (data set), http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
26. Department, U.S.: US Department of Health and Human Services. Massachusetts provider settles HIPAA case for $1.5 million, http://www.hhs.gov/news/press/2012pres/09/20120917a.html
27. Jennifer, E.M.: Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage. Journal of Hospital Librarianship 13(3), 197–208 (2013), doi:10.1080/15323269.2013.798768
28. Luxton, D., Kayl, R., Mishkind, M.: mHealth data security: the need for HIPAA compliant standardization. J Telemed E-Health 18, 284–288 (2012)
29. Campenhoudt, L.-V., Quivy, R.: Manual de Investigação em Ciências Sociais. Gradiva Publicações (2008) ISBN:9789726622758