Strategies for minimizing the influence of the use of BYOD and Cloud in organizations: 4CM Model

Fernando Moreira
UPT, IJP, DEGI, Porto, Portugal
IEETA, UA, Aveiro, Portugal
fmoreira@upt.pt

Manuel Pérez Cota
Director grupo SI1-GEAC
Universidade de Vigo
Vigo, Espanha
mpcota@uvigo.es

Ramiro Gonçalves
UTAD, Vila Real, Portugal
INESC TEC, Porto, Portugal
ramiro@utad.pt

***Abstract*— In the last decade, companies have become tend virtualized thanks to the use of outsourcing, the workforce has become more distributed, workplaces are increasingly distributed and outsourced and increasingly digital employees, with the philosophy of work anytime and anywhere. This development has, and has had a very big impact on mobile platforms and infrastructure, on the one hand, the adoption of the BYOD concept and the use of mobile devices and on the other hand, through the use of cloud computing will have profound implications in the way the technologies are and will be used as well as on the interaction between individuals and these technologies. By applying for a questionnaire and subsequent analysis showed that organizations have a lack of understanding, almost complete, the implications and consequences of using mobile devices and the cloud in organizations. A result of the Focus Group performed we propose the 4CM model.**

Keywords—BYOD; Mobile devices; Cloud; Organizations; security.

I. INTRODUCTION

With the evolution of mobile platforms and infrastructure, the use of cloud computing has profound implications for how the technologies are and will be used as well as on the interaction between individuals and these technologies. In this context, it is relevant and necessary to identify the major changes expected in the next 5-10 years that can affect the work environment. For example, in 2015 the concept BYOD (bring your own device) and the use of mobile devices (smartphones, tablets and laptops) were practically widespread, as well as cloud computing [1].

Mobile devices are emerging in the market at a rapid pace [2, 3], more and more capabilities and applications are increasingly sophisticated.

These devices are reaching a level of sophistication from a technological point of view that will have a slower evolution, so the use of the cloud will be driven by facilities that offer either in storage capacity or processing capability. In this context, it begins to watch a migration of mobile services to the cloud. For example, Google uses Google Drive and Quickoffice cloud-based (for example, for editing documents), Apple through iCloud expands to cloud the ability of the devices to sync data, photos, etc. In fact, mobile devices are becoming more than stand-alone platforms data terminals [4].

Mobile devices are allowing create a lot of information about each individual, which is raising questions about the privacy of the individual to a new level. For example, the GPS lets you know exactly where the mobile device is (outside) at a given moment, and consequently the individual himself. However, this idea has been around for over 15 years [5].

At this time, organizations are no longer provide the tools (devices) to perform the tasks, but the possibility of employees bringing their own devices is increasing, which is one of the latest trends, the BYOD. This has a positive side which is the possibility of employees working with the equipment they like, and therefore may be more productive, but it raises security issues because the question now to take into account is no longer just the user but the device or devices that the user use [6].

In this context, the information technology (IT) departments need to be aware of the chaos caused by BYOD. According to the study of Connected World [7], the young professionals and students have difficulty understanding the barrier between personal and professional life, to the point of 33% of students do not mind to share their online personal life because to work from home or office, using social networks and cloud applications [8].

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

In this context, we carried out a study on the influence of the use of mobile devices and cloud in organizations, considering the rapid proliferation of own mobile devices in the execution of personal and business tasks, as well as the use of the cloud in order to maximize or extend the performance capability in solving personal and professional tasks, without a "conscious" concern of the dangers of sharing data between devices of organizations and systems. As a result of the study is proposed the 4CM model as a guide for minimizing the problems found in the survey results.

The rest of the paper is organized as follows. In the next section, a background of the addressed subjects is presented. In section III it is presented the research methodology, while in section IV it is presented data analysis. In section V it is presented the 4CM model proposal. Finally, in the last section, conclusions are discussed.

II. BACKGROUND

A. Cloud Computing

Cloud computing refers to the use of software, network infrastructure and capacity to provide resources to users in an environment on-demand and the service measured by pay-per-use business model. It is a heterogeneous architecture, which has a range of technologies to provide various remote services. The National Institute of Standards and Technology (NIST) has identified five essential characteristics (on-demand self-service, broad network access, resource pooling, elasticity rapid and measured service), three service models (Software as a Service – SaaS, Platform as a Service – PaaS, and Infrastructure as a Service – IaaS) and four development models (Private cloud, Community cloud, Public cloud and Hybrid cloud), common to all cloud systems [11, 12, 13, 14, 15].

The security problems always have a vital role in any area that is growing, especially when introducing new technologies, because it's inevitable that these new technologies bring benefits, but also new difficulties and risks [16]. It is the security that has the highest priority if the system has involved direct, or indirect, on the economy and privacy of organizations and / or individuals.

Data security, according to [17, 18] can be divided into the following features: (1) Information security (related to the protection of information and information systems from unauthorized access [19]); (2) Durability (time servers are active [20]); (3) Availability (availability of data in the cloud); (4) Consistency (consistency in data base management system); (5) Sensitive data (what types of data can be stored in the cloud); (6) Virtual Machine (different virtual machines are vulnerable to attack [21]); (7) Integrity (no supplier can give the assurance that everything is recorded with the desired privacy); and (8) The cloud over control (control is performed only by the service provider, so it is a risk factor to take into consideration how the security and privacy of data).

Many of the attacks on cloud computing are related to their distributed and shared environments [22]. Some studies have indicated that attacks on web services constitute more than 60% of all attempts to exploit online vulnerabilities [23]. These attacks can be considered as the more traditional threats, which are also of concern in cloud environments [24]. The code injection attacks, authentication breaks and session management, Cross-Site Scripting (XSS) and incorrect security setting, are among the most common of these services [25]. Moreover, some threats are specific to cloud environments because of the multi-tenant nature of the servers in the cloud and / or the use of virtual machines that form the basis of cloud computing paradigm [26].

B. BYOD

BYOD is an acronym from the concept of "Consumerization" [27] which describes the growing trend of new information technologies emerge, first in the consumer market and then spread to organizations (business and government). Currently, the "Consumerization" involves mobile devices, but also services (DocBox, Dropbox, Google Drive, etc.) and social networks (Facebook, Twitter, Linkedin, etc.), as well as email services. All these services are used by a new generation of devices that are based in the cloud, and are increasingly used in personal and professional activities.

Mobile devices present, however security issues when stolen, lost, exposed to viruses, etc. For example, in July 2012, 54% of major incidents reported violation since September 2009, the US Department of Health and Human Services Office for Civil Rights involved the loss or theft of unencrypted devices [28]. Since 2009, a total of 464 information violations in the United States affected 20.8 million people [29]. Another example that illustrates these problems is the case of the Massachusetts Eye and Ear Hospital has agreed to pay 1.5 million dollars after a doctor has reported that his laptop was stolen and did not have the data encrypted with more than 3,000 patient records [30].

The cost of just one security breach in data access can cost the organization, according to the Ponemon Institute, between $ 1 million to $ 58 million [8]. Additionally, organizations are losing control over who has access to the corporate network. And the fact that more employees are using mobile devices in their work means that this represents a potential increase of data loss due to theft or loss of devices. In addition to this, the increased use of shared files from cloud services by organizations and employees to increase efficiency and reduce costs, often without the permission of the organization, they do increase the potential of data being stolen or compromised [31].

A study referenced in [32], shows that one of the characteristics that have been found with regard to security is that 90% of the common vulnerabilities in personal computers are also present in mobile devices, regardless of operating system. According to the same study, the same percentage applies to mobile applications, i.e. any of the tested applications had one or two security holes. Additionally mobile devices still have a characteristic that leads to the occurrence of much more frequently attacks because they often use applications without any quality control, as well as access to public networks. Thus, in a BYOD environment it is possible to make very aggressive attacks because employees use their mobile devices in completely insecure public networks, as using the corporate network. Additionally, mobile device applications present security risks in any system of any organization, as can be seen in [33, 34] *"… many apps on the market gather and send user information, such as name, passwords, location, demographic, or any other information, back to the software developers, which raises additional security concerns*".

III. RESEARCH METHODOLOGY

The purpose of this section is to describe the procedures carried out for the collection of data that form the basis of this research, as well as the methodology for the proposal validation. The main feature of the scientific method is organized research, strictly control the use of observations and theoretical knowledge. This study was based on quantitative research methodology and the creation of a focus group.

Data collected for quantitative research through the use of [35] questionnaires requires special care because it is not enough to collect responses about the matters of interest, but how to do statistical analysis for proper results validation. Aspects such as the sample size, the way the questionnaire is prepared, the questions formulation, data analysis, error margins, the selection of individuals process of who should compose the sample, among other things, are important and they should be taken into account for any investigation.

For the present study, we used the methods of quantitative research; since it is the most appropriate to determine opinions and attitudes of who answers to structured questionnaires. In this approach, the data is collected through structured questionnaires, clear and objective so as to ensure uniformity in the understanding of the respondents and a consequent standardization of results.

It was created a focus group composed of academic, industry experts and researchers. During these meetings was intended to discuss and evaluate the improvement proposals made to address the actual situation found. Throughout these meetings were collected, mostly qualitative data, which will be complemented by the bibliography research performed.

The goal of this study was to obtain answers that will measure the influence of the use of mobile devices and cloud in organizations and propose improvement measures. For data collection was used a structured questionnaire and to validate the model 4CM was created a focus group. The quantitative study was based on an online questionnaire with 33 questions. The questionnaire has been online for 120 days and 430 valid responses were received. In order to understand the reasons for the results of the questionnaire and find solutions to them, we decided to initiate a process of focus groups involving seven experts from industry and academia.

IV. DATA ANALYSIS

Due to space limitations will be presented and discussed the results considered more relevant, since the questionnaire, as mentioned above, consists of 33 questions, and [36] can be used to complete this analysis.

Mobile access to data is one of the components of this study, and after verifying [36] organizations are familiar with these issues is necessary to understand the form and the means for users to access the data. The results shown in Figure 1 allowed concluding that more than half of organizations allow access to organizational data via mobile devices of its employees. These results together with the results in Figure 2 demonstrate some contradiction with the results discussed in [36], i.e., the problems are recognized, but 61% of the organizations do not have a specific policy in the use of mobile employees in the workplace.

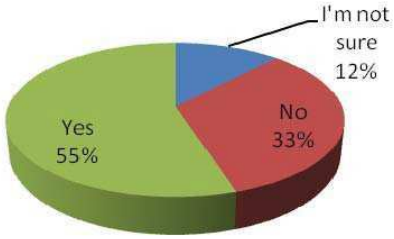

Fig. 1. Does your organization allows employees to use their private mobile devices (BYOD) to access and use the organization's data?

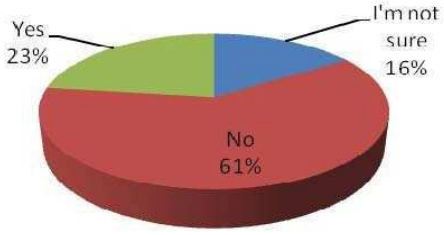

Fig. 2. Does your organization have a policy that specifies the use of mobile devices of employees (BYOD) in the workplace?

To aggravate this trend the results of Figure 3 are well illustrative, since 51% of the responses shows that do not know (26%) or do not exist (25%), all the security means suitable to mobile devices that have access to all organizational data.

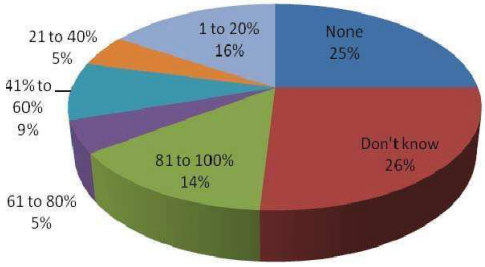

Fig. 3. What percentage of mobile devices with access to all the organization's data with adequate security features?

The results presented in Fig. 4 and 5 are an example of the lack of understanding the implications and consequences the use of mobile devices and cloud in organizations. In Fig. 4, 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. 5, 81% did not know the quantity of data residing in file-sharing applications in the cloud.

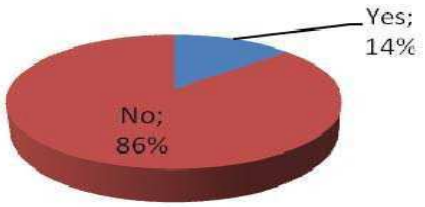

Fig. 4. Do you know how many, and what data the organization that exist in mobile devices used in your organization?

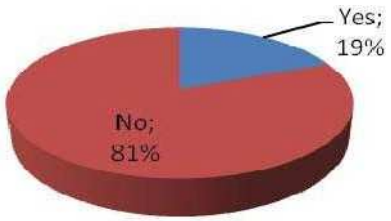

Fig. 5. Do you know the quantity of data residing in file-sharing applications in the cloud?

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.

The focus group held has subsequently been chosen to be a qualitative research method [37] popular for being able to provide details about complex situations [38]. The achievement of the focus group, served thus to complement the quantitative method performed, which is a practice advocated as being beneficial by many researchers [39], [40]. The group of researchers was carefully chosen in order to generate knowledge and to explore opinions. The individuals were selected based on their knowledge in the field, having performed three meetings of approximately 2 hours each. The sessions were recorded (audio – with the express agreement of the participants) and transcribed, and the material used to deepen our research on the use of BYOD and Cloud in organizations. This material was treated by content analysis based on categories. As a result we present below the proposed 4CM model.

V. 4CM MODEL PROPOSAL

Any credible bibliographic source regard to security shows that perfect security is impossible. However, the traditional model is to protect all equally, which is becoming unsustainable in many organizations because of the heterogeneity of the assets to protect, and even more complicated to completely differently in the access to them.

The digital era has come faster than organizations and security professionals can adapt. It is understandable that the security model of organizations in relation to its assets - data / information – has not evolved as quickly as the new technological approaches. In this context, this new ecosystem requires a shift in focus, because there is a conflict between usability and security, end users and IT managers, personal interests and corporate interests, that is, it is no longer possible only protect the data / information the same way it was performed when it was confined to the data center, but use a holistic way.

This new ecosystem, discussed above, in using its three main components (BYOD, mobile and cloud) can be summarized as follows: (i) new models of work organization are coming, BYOD is one of the most interesting and challenging; (Ii) mobility, "consumerization" and cloud are key factors to allow implementation of professional tasks anywhere and at any time and (iii) security issues relating to the device and data are one of the main barriers to adoption of these new IT models, which leads to the definition / appearance of new security models which take into account factors other than just the traditional ones.

With all the constraints presented throughout the article and after the literature review ([6], [14], [31], [33], [41]), it is concluded that a model to successfully treat issues related to the BYOD, mobile devices and use of SaaS cloud applications, has to cover many functions within the organization, including human resources, juridical, IT, financial and operational. Consequently, these challenges must be addressed by many perspectives including organizational and technical. In this context and after the achievement of Focus Group, it proposes a model that includes four components, and the result of their intersection results in an improvement proposal to the issues discussed above (Fig. 6).

Fig. 6. 4CM model.

The 4CM model shown in Figure 6 consists of the following components:

1) To restrict information security focus to nuclear and critical assets;

2) To protect the key assets with security systems in multiple layers;

3) To involve employees who use information to protect the assets they work with;

4) To build teams with business partners to boost protection systems and make security a business problem and not just an IT problem.

Each of the four components presented, will be developed in the following subsections.

A. *Restrict security focus of information on nuclear and critical assets*

To determine which are the most critical assets of the organization is essential, but is sometimes controversial. Some organizations believe that the data is the most valuable assets that are required to protect. However, if the risk attributes are assigned to a set of assets – data, software, networks and personal – it becomes clear that there is much more that must be taken into account as to how to minimize penetration in organizations, and attacks its assets.

To resolve this issue it is must define a classification regarding the criticality of each asset of the organization and labeling, for example, each of BYOD devices with a risk assessment, that is, according to a listing compiled by the organization regarding the criticality each asset, equipment and applications should be labeled. This question will worsen to the extent that organizations should take into consideration that the future employees have with you, not just a Smartphone, a tablet, but also several wearable networked devices. The question that can be asked is: How to support some types of wearable devices on corporate networks? So, if there was the problem of smartphones and tablets these new devices further increased security problems.

One of the most complex activities due to the amount of information that is required to treat it is to have solutions that allow for gathering and evaluating the total amount of data that is transferred to and from each application of the organization that will be accessed.

As solutions to the questions discussed above is possible to establish some policies: (1) To protect the network traffic to prevent the remote devices that connect to the corporate network could put the data at risk. (2) To protect the contents of the traffic from the vulnerability and exploits; the managed devices should have the active protections to defend against this type of content. (3) Definition of use policies from the applications through the appropriate control over some applications, who can access and how; (4) Policies control devices via Mobile Device Management tools (MDM) to ensure that a minimum number of features are provided in the operating systems of mobile devices and (5) To protect the data on the devices through Mobile Content Management tools (MCM), asking the following question: Should a BYOD device having corporate data? What measures are used to make data secure, or destroy them in case of loss or theft of the device? One solution is to use containers to limit the scope of location data. Another possibility is to first consider which applications (and data) the device is allowed to access, for example, by using virtualization for remote access to an application without needing to install the application or save the data on the devices.

In this sense, the security management architecture should allow the organization to provide a centralized way to establish policies and access to all these factors. For example, control access to applications for specific users, monitor traffic and unknown files by nature and unidentified can be dangerous. For example, many organizations do not know who is using a particular IP address and the identity is not used as security policy element. Should start with the assumption that unknown elements are not reliable, may involve greater precision measurements of who can access a particular resource, which solves part of the BYOD integration problems. Another question is to know the type of device and location, because it is necessary to know if the device has or not the necessary security features, but the organization must provide and require the use as well as its location, because often devices are connected outside the potentially dangerous Wi-Fi networks. To address this issue, in a radical way, you can lock the devices through the Network Access Control (NAC). However, using a less conservative control policy is possible, and desirable, to establish who are the users that want to use applications and data, examine the contents and analyze the risks and incorporating devices and location in security policies.

B. *To protect the key assets with defense systems in multiple layers.*

The layered approach to access to key assets makes sense, using read-only policies or different containers (sandbox, etc.) [31]. Defense systems in several layers for software rely heavily on a combination of assessments carried out directly by the IT department and software checks designed to identify vulnerabilities [25].

In this context organizations must establish a number of strategic security layers to provide the necessary access to corporate information while minimizing risk and maintaining compliance. Thus, organizations should stop distinguishing between devices that are connected to the corporate network (internal) and devices outside, but to be concerned primarily with the protection of information. Access to sensitive information should be organized in order to apply best audit process in real time and logs systems and implement appropriate security solutions to support the BYOD integration strategies, such as those that can manage data replication.

In this context the following practices are planned:

1) Choose a solution that protects all sensitive data on all devices, ie, the solution must support the operating systems used in mobile devices (Android, BlackBerry, iOS, Windows Phone);

2) Policy-oriented network based on the use NAC technology to control how and which mobile devices that access the network. For example, two solutions, Cisco Networks BYOD, and Meru Networks BYOD. This approach will allow support a wide variety of devices and provides a more secure connection to the network. In addition, a centralized security system is also incorporated to help detect devices and users and apply different policies and rules to each user. It is used one MDM solution to control the accounts of employees and logs of employees who access the network, resources used, etc. While the second solution is intended to be easier to use by employees and less intrusive, that is, the system can assign the employees rights and privileges according to their function and where they are;

3) To centralize access control monitoring it will allow the IT department able to monitor the distribution of files and detect anomalous behaviors before the data breach. This proposal is related to the fact that many companies and public organizations have invested heavily in ECM systems. Organizations should select a MCM solution that provides access to content stored on these systems. Thereby, file sharing becomes secure and naturally integrates the workflow and remote employees in locations outside the organization have access to critical files whenever necessary;

4) To increase the confidence and control through the use of private clouds: Whenever possible, organizations should implement their MCM solutions in private clouds, giving full control of the location and availability of data to your IT department;

5) To choose certified MCM solutions, for example, Federal Information Processing Standards (FIPS) with 140-2 certificate;

6) To identify which devices can be used on the corporate network, which applications are allowed and prohibited, data should not be stored locally after being used for a mobile application. Block risk services and installation of applications that can be harmful to the security of the organization, such as the integrity and confidentiality of data. Organizations must implement security policies (passwords, ...) for all devices and have strategies for lost or stolen devices, and *at the time that* an employee *cease to belong* of the organization's staff;

7) Remotely control the devices via MDM tools and complementary with MCM solutions for data control;

8) Use separation techniques based on virtualization for remote access to resources (applications and data are on the corporate network and not on the devices), dual boot (the device can boot different operating systems) and mobile virtual platform, to separate applications space from the enterprise and personal. In the case of virtualization, can be another effective method to manage corporate data on BYOD environments. This approach allows developers to access through secure passwords to your desktop and applications using their mobile devices; in case of loss or theft of the device, the remote connection is broken and therefore no longer exists access to applications and data.

9) To reward those who are proactive in their security practices. The practices presented can be complemented with the use of monitoring technologies and standards of analysis, such as DLP (Data Loss Prevention), monitoring of security events and forensic information tools.

10) Finally *the approach* phone-center focuses on security on the device itself, with a MDM system installed by the manufacturer of the devices. In this approach controls are placed on the device to work based on how devices access network and data resources. Dual Sim and containerization are used to separate the workplace (ie applications) of personal space on the device.

In the nutshell, integrate MDM tools to network infrastructure to automate the on-boarding security has to grow. Approaches type phone-centric, particularly using containerization technology to restrict users to access, copy, move (paste) or editing data from containers applications, are used in conjunction with virtualization approaches to provide remote access to the containers. Specific policies are implemented by organizations to work hand-in-hand with MDM and network approaches to reduce the risk of potential data loss. For example, organizations such as the defense industry generally choose more conservative methods to deny access to all personal devices on corporate networks; however, most organizations should adopt BYOD controls that offer some flexibility to employees while forcing corporate policies and adopt best practices.

C. To involve employees who use information to protect the assets they work with

Employees are the greatest source of threats and prevention, because are these that are often the entry point for vulnerabilities.

Some of the most sophisticated threats arise through social engineering, especially using social networks and email contacts, targeted to executives and key operational staff within the organization. One of the references and suggestions made in [42] it is to try to "wear the skin" who will prepare the attacks, as well as their own IT staff and business partners. Thus, according to the authors, because employees are often the channel for the intrusion, so it is essential to include them in prevention.

Another example of integration of employees in developing security models process in this new ecosystem, it is indicated in [33] that for several years started a safety awareness initiative that coincides with a shift from PCs to tablets, mobile applications and cloud services. Indicating, for example, that hospitals are adopting new mobile device management policies. The Health Information Management Systems Society (HIMSS) revealed that among the 180 IT executives from hospitals, the number of those who have implemented a formal policy on the use of mobile devices increased from 38% to 68%, between 2011-2012 [43], with very positive results.

This risk-based approach is not easy and requires a major change of mindset in organizations, because today the introduction of BYOD and cloud creates a new ecosystem and

raises new problems and one way to minimize is the involvement of employees in the processes of control. In this context, organizations also need to form its employees, as safety is a concern for all. Many data losses are due to little care of the employees and not to malicious users. Ensure that employees understand the security policies and take the proper safety precautions is essential to be able to maintain this new insurance ecosystem.

D. Build teams with business partners to boost protection systems and to transform security a business problem and not just an IT issue

The well-defined notion of the boundary between the inside and outside of an organization no longer appropriate due to changed functioning paradigm of organizations. As a result of the security risks are now transversal to all the decision pyramid layers and, therefore, you must follow the principle that there is no way to build a "wall" 100% safe around this modern digital ecosystem.

Thus, on the one hand it is needed, and must work together, namely, working with all stakeholders in order to implement integrated security solutions for systems that must interact with each other so as to have only a single framework of security, that each of the organizations have their. This solution is only possible if there is a sharing of best practices of each of the organizations participating in the entire distribution chain, on the other hand it is always possible to adopt some technological measures to minimize the risks.

Based on the results obtained in the surveys and subsequent analysis it is shown that it is, or should be, face an evolutionary model of security as holistic security, using various techniques of technology and management, with wide acceptance and accountability, layered and tailored to minimize the risk when the security problem is hierarchically seen from top to bottom.

To better understand how it can transform the security in a business problem, is necessary to analyze, for example, if a particular department uses cloud storage and whether this decision was approved by the department director. Verify whether suppliers often they access critical data use compatible security processes. These issues can be addressed in the same way as suggested in [6] and / or [41].

In a nutshell, organizations have to accept that losses and violations will occur and thereby cause a change of absolute prevention mentality to a specific prevention, combined with resilience and a sense of acceptable loss.

VI. CONCLUSIONS

In the last decade, companies become highly virtualized due to the outsourcing (service providers, cloud services, etc.), the workforce became tends to spread (a mixture of organization's employees with employees hired for projects) workplaces increasingly distributed (work in organizing and home-based offices), outsourced workplaces (such as call centers), and digital employees increasingly nomadic, with the philosophy of work at any time and in any place.

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

In order to understand this new change, a study was performed, based on the application of a questionnaire followed by carrying out of a focus group in order to understand the influence of the mobile devices and cloud use in organizations, and the proposal of 4CM model as a guide for minimizing the problems found in the results of the questionnaire.

These results show interesting indicators for developing security frameworks that include not only the technological aspects of security to go through all of an organization hierarchy levels and with a special focus on full integration of employees (current and new generation) this new ecosystem and especially in training plans. Some of these aspects have already been discussed in the previous section, but need practical implementations, and respective evaluation.

References

[1] L. Schubert, K. Jeffery, and B. Neidecker-Lutz, “A Roadmap for Advanced Cloud Technologies under H2020”, Retrived from http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-expert-group/roadmap-dec2012-vfinal.pdf

[2] Communities Dominate Brands, Retrived from http://communities-dominate.blogs.com/brands/2012/06/massive-milestones-in-mobile-will-these-numbers-change-your-mobile-strategy.html

[3] Business Insider, Retrived from http://www.businessinsider.com/2012-03-28/research/31248281_1_ios-android-hard-drive.html.

[4] D. Linthicum, “Mobile's next great leap will happen in the cloud”, InfoWorld, 2014, Retrived from http://www.infoworld.com/print/236891.

[5] E. Knorr, “The mobile spy in your pocket”, InfoWorld, 2014, Retrived from http://www.infoworld.com/print/236880.

[6] S. Mansfield-Devine, “Interview: BYOD and the enterprise network”, Computer Fraud & Security, Volume 2012, Issue 4, April 2012, pp. 14–17

[7] Cisco, “Cisco ConnectedWorld Technology Report”. Cisco, 2011. Retrived from www.cisco.com/en/US/netsol/ns1120/index.html

[8] G. Thomson, “BYOD: enabling the chaos”, Network Security, Volume 2012, Issue 2, 2012, pp. 5–8

[9] M. Potts, “The state of information security”, Network Security, Volume 2012, Issue 7, 2012, pp. 9–11

[10] Verizon, “2012 Data Breach Investigation Report”, www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf

[11] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," *SIGCOMM Comput. Commun.* Rev., 39, 2008, pp. 50-55.

[12] P. Mell, and T. Grance, “A NIST Definition of Cloud Computing”, National Institute of Standards and Technology. 2009, Retrived from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[13] M. Hogan, F. Liu, A. Sokol, and J. Tong, “NIST Cloud Computing Standards Roadmap”. 2011.

[14] T. Lokhande, and R. Shelke, “A Review Paper on Cloud Computing Security”, International Journal of Advanced Research in Computer Science, Volume 4, No. 6, 2013, pp. 70-73

[15] M. Cota, R. Gonçalves, and F. Moreira, “Cloud Computing Decisions in Real Enterprises”, Agile Estimation Techniques and Innovative Approaches to Software Process Improvement, 2014, pp. 313-330.

[16] H. Romer, “Best practices for BYOD security”. Computer Fraud & Security, Volume 2014, Issue 1, pp. 13-15.

[17] G. Murugaboopathi, C.Chandravathy, and P. Vinoth Kumar, “ Study on Cloud Computing and Security Approaches”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013, pp 212-215

[18] Cloud Security Alliance. “Security Guidance for Critical Areas of Focus In Cloud Computing V 3.0.”, 2011, Retrived from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[19] P. Bryden, D. Kirkpatrick, and F. Moghadami, “Security Authorization - An Approach for Community Cloud Computing Environments”, Retrived from http://www.boozallen.com/media/file/Security-Authorization-An-Approach-for-CCEs.pdf

[20] K. Finley, ” The Dark Side of the Cloud: IBM Partner Gives Folks Two Weeks to Move Data”, Retrived from http://www.wired.com/wiredenterprise/2013/09/nirvanix/

[21] R. Chow, P. Golle, R. Masuoka, J. Molina, and E. Shi, “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control”,Retrived from http://www2.parc.com/csl/members/eshi/docs/ccsw.pdf.

[22] F. Ahamed, S. Shahrestani, and A. Ginige, “Cloud Computing: Security and Reliability Issues,” Communications of the IBIMA, vol. 2013, Article ID 655710.

[23] Sans Institute, “The Top Cyber Security Risks,” SysAdmin, Audit, Network, Security Institute. 2009, Retrived from http://www.sans.org/top-cyber-securityrisks.

[24] H. Takabi, J. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE, 8, 2010, pp. 24-31.

[25] Open Web Application Security Project. OWASP Top 10 Risks, 2013. http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

[26] Y. Chen, V., Paxson, and R. Katz, “What's New about Cloud Computing Security?”, 2010. *EECS Department, University of California, Berkeley.*

[27] http://en.wikipedia.org/wiki/Consumerization

[28] US Department of Health and Human Services. Health information privacy: breaches affecting 500 or more individuals (data set). 2012. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html .

[29] M. McGee. Health breaches: 20.8 million affected. Health Info Security. 2012. http://www.healthcareinfosecurity.com/health-breaches-208-million-affected-a-4977

[30] US Department of Health and Human Services. Massachusetts provider settles HIPAA case for $1.5 million. 2012. http://www.hhs.gov/news/press/2012pres/09/20120917a.html .

[31] A. Scarfò “New security perspectives around BYOD”, Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, IEEE Computer Society, DOI 10.1109/BWCCA.2012.79, 2012. pp 446-451

[32] N. Leavitt, Today's Mobile Security Requires a New Approach, Computer, Volume:46 , Issue: 11, IEEE Comp. Society, pp. 16 – 19

[33] J. Moyer. “Managing Mobile Devices in Hospitals: A Literature Review of BYOD Policies and Usage”, Journal of Hospital Librarianship, 13:3, 2013, pp. 197-208

[34] D. Luxton, R. Kayl, and M. Mishkind.” mHealth data security: the need for HIPAA compliant standardization”. J Telemed E-Health.18. 2012, pp. 284–288.

[35] L. Campenhoudt, and R. Quivy, “Manual de Investigação em Ciências Sociais”, Gradiva Publicações, 2008, ISBN:9789726622758

[36] F. Moreira, M. Cota, and R. Gonçalves, “The Influence of the Use of Mobile Devices and the Cloud Computing in Organizations”. New Contributions in Information Systems and Technologies, ed. Álvaro Rocha; Ana Maria Correia; Sandor Costanzo and Luís Paulo Reis. Volume 353, 2015, pp. 275-284.

[37] P. Ghauri, and K. Gronhaug. “Research methods in business studies – a practical guide”. 3rd ed. 2005, London: Prentice Hall.

[38] H. Bernard, “Research methods in anthropology – qualitative and quantitative approaches”. 4th ed. 2006, Oxford: AltaMira Press.

[39] R. Gonçalves, J. Martins, J. Pereira, M. Oliveira, and J. Ferreira. "Accessibility levels of Portuguese enterprise websites: equal opportunities for all?", Behaviour & Information Technology 31, 7, 2011, pp. 659 - 677.

[40] J. Pereira, J. Martins, R. Gonçalves, and V. Santos, "CRUDi Framework Proposal: Financial Industry Application", Behaviour & Information Technology, 1: 2014, pp. 1 - 24.

[41] Bernard Mathaisel, Terry Retter, and Galen Gruman, “How to rethink security for the new world of IT”, 2014 http://computerworld.com.edgesuite.net/insider/InfoWorld-new-security.pdf

[42] F. Palmieri, U. Fiore and A. Castiglione. “Automatic security assessment for next generation wireless mobile networks". In: Mobile Information Systems 7(3), IOS Press, 2011, pp. 217-239

[43] Healthcare Information Management Systems Society. “2nd annual mobile technology survey”. 2012, http://www.himss.org/content/files/FINALwithCOVER.pdf