JIEE Časopis priemyselnej elektrotechniky
Journal of Industrial Electrical Engineering
ISSN 2454-0900
www.jiee.eu

BYOD phenomenon and corporate computer network security.

[1]*Michal NEMETZ*, [2]*Anna HODULÍKOVÁ*

[1] GX Solutions, a. s, Slovak Republic
[2] Department of Theoretical a and Industrial Electrical Engineering, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Slovak Republic

[1]michal.nemetz@gmaill.com, [2]anna.hodulikova@tuke.sk

***Abstract* —Currently playing corporate network security a main role in business processes, which seeks to adopt new technology trends to improve the business in terms of performance and efficiency, in order to keep pace in the fierce market competition. However, the introduction of cloud computing and opportunities for employees to work on their own mobile devices brings additional risk to the company processes. The question to be answered is how can the above risks are reduced to acceptable levels, to promote the safe adoption of IT consumerization. In order to find answer to it, this diploma thesis proposes safety measures for the company.**

***Keywords* — assets, BYOD, cloud computing, corporate network security, mobile device, risk**

I. INTRODUCTION

IT consumerization opens up new possibilities for innovation in the corporate mobility. A new trend that applies to corporate mobility is BYOD, which means employees can bring their devices to work instead of having to find an organization provide the necessary hardware/software. Thanks to the adoption of this policy, employees can use their own laptops or smartphones when working. Because they are aware of how to use these devices, can work productively. In addition to higher job satisfaction BYOD policy shifts costs to the user, thus increasing the efficiency of the organization, because these devices have a high tendency to increase performance, consequently, an organization can benefit from the latest features and capabilities of mobile devices that are on offer.

Another new technology is "cloud computing", which can be easily understood as governance, storage and use of data via the internet, where users already having unlimited computing power on demand, without large capital investment, which is paramount in terms of company and have access to their data anytime and anywhere where is internet access.

The security is a very broad term, encompassing a rich array of diverse elements affecting its quality, depending on the type of system to be secured. In the IT field are five quality attributes, through which is compiled the system security:

- Confidentiality
- Integrity
- Availability
- Access control
- Non-repudiation

This thesis deals with security architecture, the firm shall include in its overall architecture of network security for mobile devices. In chapter VII. we analyze, design requirements in policies BYOD, where we divides the assets of the authority and the risk involved. In chapter XI. The overall secure corporate architectures that are part maintained above mentioned quality attributes.

II. MOBILE DEVICES

Mobile device, or even a portable device is small, portable, electronic, wireless device, witch operating system, communication ports and various applications. With mobile devices in the corporate environment should be counted, as they provide enough power for normal work, such as connecting to the internet, report writing (email, chat, skype), calendar, different activities (measuring, counting) which can be achieved through additional programs, or applications, which makes them a capable competitor for personal computers. From Intel's forecast suggests that by 2015 the number of mobile devices in the world will reach 1.5 billion [1].
The most common mobile devices using the IT field can include:

- Notebook
- Smartphone
- Tablet
- E-book reader

III. ASSETS AND COMPANY'S NETWORK SECURITY

Assets are the total property that the organization owns and that has some value to it.

ASSETS ALLOCATION

a) Publishable

Publishable assets are less sensitive information. This information is not protected from public disclosure and if disclosed will not compromise the privacy or safety of the employees of the organization, clients and partners. This is information of a commercial nature, which mainly serve to promote the organization sales of goods and services in order to make a profit. For example brochures, flyers.

b) Limited

This group might include sensitive information that must be protected from disclosure, either because of the danger of abuse of information, or morally. When disclosure may jeopardize the privacy or safety of employees of the organization, customers, partners (documents on risk management, internal audit reports). The organization must follow its policies and procedures for disclosure before providing information to external parties [2].

c) Personal – protected by law no. 122/2013 Z. z. About Privacy Policy

This information must be provided separately physically (hardware access), as well as virtual corporate network via internet, internal network or intranet.

d) Confidential

Include internal organization information, intended for limited use because their disclosure or obtain third party organization may jeopardize the privacy or safety of employees of the organization, clients, partners. The information in this category may access and use the internal parties only if they show a special permit. External parties requesting such information to authorized activities must be under a contractual obligation of confidentiality to the organization – confidentiality agreement.

e) Critical – The highest level of classified information

Information that is considered to be very sensitive (know-how, new projects and various specific data that has been so designated organization) and are intended for use only predetermined individuals with the fact that their every access is recorded separately and logging. This information must be as secure encryption and stored outside normal information. This section is exempt from disclosure because it could cause serious damage or injury of the organization, employees, client, partners, or cause great financial harm to the organization.

IV. MODEL SELECTION PROVISION AND CLOUD DEPLOYMENT FOR OUR ORGANIZATION

The organization realizes that the cloud can be used for faster access to corporate information, such as strengthening their own infrastructure. Compared with conventional storage solution on their own servers (in-house), private SaaS cloud model offers some unique features. SaaS applications can be deployed more quickly and with minimal effort, which is a key factor for the organization. In addition, SaaS service offers scalability, faster and ensuring flexibility, enabling organizations to adapt their activities in accordance with changes in the needs and the needs of consumers [3]. SaaS solution also provides better protection against network attacks by detecting in real time and further use of security controls [4].

Unlike local services (on- premise), access to SaaS is provided on a subscription basis, and the organization pays fees for the use of applications (monthly, semi-annually, annually). The result is that the solution using SaaS eliminates or significantly reduce input costs for launching infrastructure of the organization. In addition, SaaS reduces the cost of disaster recovery networks [5][6].

Technically the SaaS applications centrally located in the cloud provider's network. It allows SaaS providers to deploy updates for applications transparently. By the end user SaaS applications are accessed through the internet and web browsers equipment in the company as well as mobile devices.

With the increasingly growing number of business applications delivered through a SaaS organizations can choose from the options supplier, where and how applications are delivered. Thus the organization can concentrate on their core business mission.

V. OUTLOOK FOR THE ADOPTION OF BYOD POLICY

The concept of IT consumerization refers to the introduction of new information technologies, which are primarily made by individuals and then spread to business and government organizations. Nowadays consumerization revolves around the use of new hardware, such as smartphones and the use of advanced services such as social media and cloud services. Consequently the concept of BYOD which follows the general trend applies to mobile workers, bringing their own portable device to your workspace, used for work as well as personal purposes. BYOD is becoming more demanding for IT managers because it helps in assists emerging trends in the workplace, such as teleworking, cloud computing and workshops. BYOD is also convenient for organization, both in terms of reducing operational costs, as mobile employees to use their personal devices instead of their organization necessary hardware provided. BYOD phenomenon increases productivity, whereas mobile workers are offered more opportunities for cooperation in the use of their favorite devices [7][8].

VI. OVERVIEW OF INTERESTED PARTIES

Large number of corporate and external stakeholders have conflicting views and interests with adoption of BYOD policies in organizations. The difference between the various groups of actors can be defined on the basis of their roles allow or prevent the implementation of BYOD policies.

Table 1
Mais stakeholders

Stakeholders	**Role**	**Impact**
Organization	Allows	High
Employees	Allows / Prevents	Medium
Customers	-	Low
External cloud partners	Allows / Prevents	Medium
ISP	Allows	Low
Device vendors	Allows / Prevents	Low
Government	Prevents	High

VII. DESIGN REQUIREMENTS AND RISKS OF BYOD

Information security is established using ISO 27001 standard, which describes the concept of information security and its importance to the organization. The next section deals with the standard medium of information, because the information can exist in many forms (eg printed on paper, stored electronically, etc.) Further information is given importance in terms of ensuring:

- confidentiality – ensuring access to information only to authorized persons
- integrity – ensuring accuracy and completeness of data and methods of treatment throughout their life cycle
- availability – ensuring access to data according to the needs and access to appropriate values for authorized users
- access control – prevention of the unauthorized use of funds carried out by means of authentication and authorization.
- non-repudiation – during a transaction not receiving or the sending party deny that they have taken or send a file.

The above requirements are necessary for the organization in the implementation of BYOD and cloud computing technology, based on a number of clear corporate tenants (one software application serves multiple customers – the lessee) and the occupational hazards of mobile devices. More specifically given that the only cloud hosts all types of data classifications that are derived from several customers, it is essential that the confidentiality and integrity of corporate data are protected from dangerous persons during transmission, processing and sharing the cloud. Consequently, the need for managing access mechanism to ensure that the data is read or adjustments are performed only by authorized persons and of their employment authorization. Corporate data should be available at any time if the beneficiary remote or local employee requests access, while the presents undeniable proof of identity of the person performing any type of activity [9].

Employees combined use mobile devices for business and personal purposes, which further explains the need for the above safety requirements, because the confidentiality and integrity of corporate data should be protected from personal applications that may contain malware and prevent access to corporate data by third parties device that can be used (egg, family members of employees, friends, etc.).

VIII. LEGAL REQUIREMENTS

In addition to the above safety requirements an organization that has a policy of BYOD and SaaS applications should fulfill a series of legal requirements, particularly concerning the applicable laws for remote monitoring of personnel and data processing on mobile devices. In addition, cloud computing is a further legal problems affecting BYOD policy that should be addressed the security architecture design.

The main obstacle for organization that has adopted a policy BYOD are privacy concerns, corporate and employee data on mobile devices. Given the mobility policy stems from the fact that employees can use their own mobile devices for work-related tasks, the organization must establish a set of rules in order to protect the company in case of destruction or leakage of confidential company data and implementation of the monitoring of personal devices to ensure that all activities and employees to access company data using devices in accordance with business rules. It carries the risk that the organization is violating the rights of its employees to the requirements of the protection of their personal data, which may lead to reduced job satisfaction and even defense organization [10].

IX. FULFILLMENT OF LEGAL REQUIREMENTS

Tab. 2 , provides an overview of requirements that our proposed security architecture be fulfilled.

Security architecture alone is not enough to define the appropriate security controls and their precise location on the enterprise to the cloud, which would ensure the adoption of BYOD poliies, because the loss of security properties depend on a variety of risks. Therefore, in the next chapter to be monitored in order to monitor any gaps in the existing security architecture and spaced accordingly right controls in the right places.

Table 2
Securirity architecture

Legal requirements	
a.	Create employee consent for personal monitoring classification
b.	Provide detailed records of all personal data breaches in tracking mobile devicesí
c.	Define a set of allowed functions and services for mobile staff
d.	Making sure that employee devices support a minimum level of safety features is authorized for business purposes
e.	Define the level of Access the cloud provider to corporate data stored on corporate SaaS cloud
Information Security	
a.	Protect the confidentiality, integrity and availability of corporate data and during operation even at rest
b.	Protect the confidentiality, integrity and availability od corporate data stored on employees mobile devices
c.	Protect corporate servers availability
d.	Protect the availability of mobile devices platform
e.	Secure Access control and internal corporate cloud databases and applications
f.	Ensure non-repudiation for all corporate data and Access to applications

X. RISK ASSESSMENT

Risk assessment is the cornerstone of any information security program, it allows organizations to identify weaknesses and shortcomings before IT managers will continue to implement appropriate security controls. Used to assess the risk framework. These frameworks are intended to assist organizations in identifying risks, establishing priorities and defining instruments of camping defense mechanism of company. For our work we chose a framework from Microsoft, which is freely available on the internet [11].

Fig. 1 Assessment of degree of risk

As illustrated in Fig.1 assess the degree of risk can be divided into three phases. The first phase is the planning phase, which builds the basis for successful risk assessment, appropriate matching, determining the scope and gaining adoption assessment of the degree of risk. The next stage is

collecting data, during which the risk-related information obtained from stakeholders across the organization. More specifically the data elements that are collected during this phase relate to organizational assets, threats and vulnerabilities of our system as well as existing and proposed security check. The final phase is the phase of prioritization of risk, where risks are identified and quantified fixed and repeatable process [12]

Organizational asset are classified as:

• LBI – classification of low business impact: there are classified assets which if disclosed without authorization may involve limited or no loss of property organization, or with related parties (business partners)

• MBI – classification of medium business impact: influences are incorporated assets, which if disclosed without authorization, could seriously harm the physical organization, or related parties. Should it be limited access to MBI activated only for IT administrators.

• HBI – classification with high business impact: here they are all assets when published without permission, could result in serious, even catastrophic material losses organizations or relying party.

Tab. 3 provides an overview of selected assets together with their classification based on the commercial influence of the loss of every application security requirements. It should be noted that the impact of each asset class is defined using the fictitious user lists provided by the Microsoft Security Management Guide. Given that our security architecture is designed to protect key assets, the poposed table od assets should be designed based on customer business environment of each company before making the risk assessment phase, to optimize security.

Table 3
Classification of assets

Assets	**Rating category**
Corporate database	HBI
Corporate database on cloud	HBI
Data centers / servers	HBI
Corporate workstation	LBI
Corporate data on cloud	MBI
Employee mobile devices	LBI
Corporate data on employee devices	MBI
Personal data of employees	LBI
Power / phone lines	MBI

XI. PROPOSAL OF SECURITY ARCHITECTURE

After we built priority list of risks to the organization's most valuable asset, we can get further and set appropriate risk mitigation measures.

a) Deployment of selected technical checks (Fig. 2)

b) Deployment of operational control

Preventive operational control of our security architecture design include electronic locks, fences and security gates that protect corporate devices from intruders. Additional locks on laptops for staff workstations and alarm systems are also deployed additional security for computing devices. In addition automatic fire protection systems and temperature / humidity control should be installed to protect the organization's key assets from natural disasters. Power supplies for sensitive electrical equipment should be available so applications and operating systems are switched off in a safe manner offsite in order to facilitate recovery od lost or damaged data in the event of a catastrophic event. In order to keep corporate data should be followed by formal procedures to ensure that mobile external storage device with a replacement corporate hardware are demagnetized, od secured by orher methods prior to disposal [13].

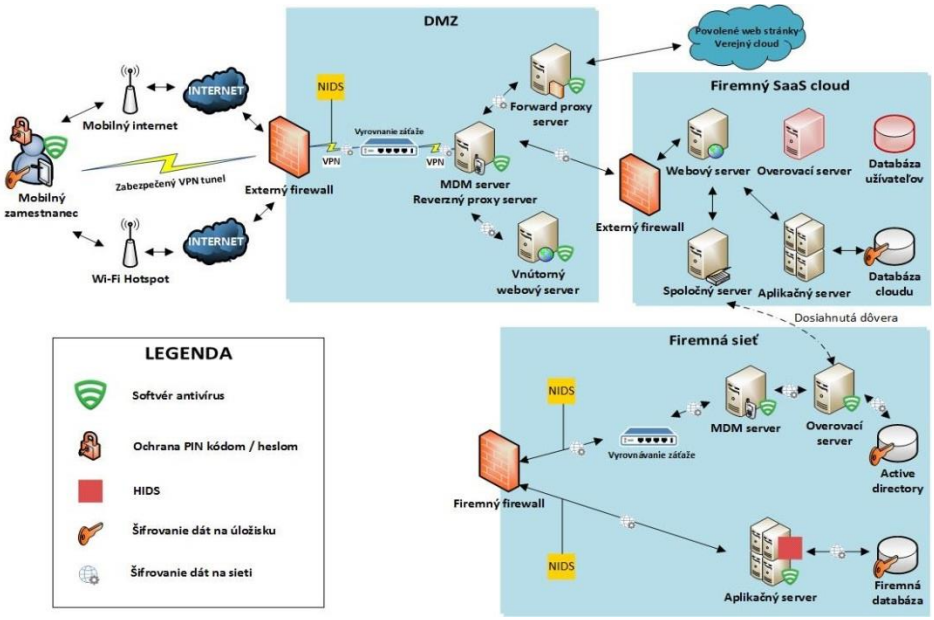

Fig. 2 Information security architecture

c) Deployment of organizational control

Preventive controls are primarily board documented security plans that explain how different safety features and installed as safety processes are carried out.

Our proposed security requires that there be a policy for employee use of equipment in organizations. In this sense, business teams and IT management should jointly develop guidelines and documents for the allowed protocols and services that can be installed on employees mobile devices. This technology should be periodically reassessed and updated to reflect the new mobile devices and environmental changes.

Another preventive control which are part of our security architecture is the implementation of a system consisting in the provision of access to company information for new employees and shut down the accounts of former employees who have left the organization. Security procedures should also include rules for employees that are transferred within the company positions and with varying levels of access. In this sense, security system should define a clear division of responsibilities and privileges for employees to use only the resources that are related to their job function.

Finally training on safety precautions are checks that are mandatory for all new employees. The training should cover all aspects of security, including security policy, network security, application security, physical security and procedures for the protection of personal mobile devices. Lay down clear rules on what employees should do if they become witnesses of the things that threaten the safety of some of the earlier steps.

In addition they conducted periodic tests to ensure staff absorb new material while updating and training courses are conducted regularly to ensure that all staff are aware of current practices and risks.

XII. CONCLUSION

By now, no one disputes the importance of corporate network security and protection of corporate assets since the last 20 years a significant proportion of human activities in the company related to computer and information technology, and it is certain that this trend will not change. Since companies are trying to save and consumerization of IT companies are pushing forward this thesis was to familiarize with the needs and possibilities of secure corporate network access via mobile devices, which we applied to a notional corporate network.

The main contribution of this thesis is to design the overall security architecture, we received identifying vulnerabilities within the existing corporate network security and

- Valuation of assets of the company and subsequent identification of risks,

- Identification of threats and vulnerabilities,
- Determine the protective measures according to the technical, organizational and operational areas of analysis.

Finally it should be noted that the greatest threat, while the most important limiting factor for corporate security and the entire security system are humans and it depends just on us, users, to realize our large share of responsibility in corporate network security.

ACKNOWLEDGMENT

The support by the project VEGA grant No. 2/0069/15 of the Scientific Grant Agency of the Ministry for Education of the Slovak Republic is acknowledged.

REFERENCES

[1] BUSINESSIT.CZ: Mobilní zařízení pro lepší byznys [online] 2011, http://www.businessit.cz/cz/eknihy-o-it-zdarma-ke-stazeni.php
[2] Metodický pokyn pre kategorizáciu citlivosti údajov z dôvodu bezpečnosti (verzia 1.0) [online] December 2012, http://www.informatizacia.sk/zverejnovanie-informacii/15141s
[3] EFQM: Študijné materialy k štandardom základných znalostí IB [online] 2012, informatizacia.sk/ext_dok-stud_2014_02_laici/16984c
[4] WALTERS, Richar: The cloud challenge: realising the benefits without increasing risk [online] Computer Fraud & Security, August 2012 [cit. 2014-04-12]. http://www.saasid.com/wp-content/uploads/2012/09/ComputerFraud_and_Security_2012-08_SaaSID.pdf
[5] ARMBRUST, Michael: Above the Clouds: A Berkeley View of Cloud Computing [online], Electrical Engineering and Computer Sciences University of California at Berkeley, Február 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
[6] IBM Cloud Computing [online], [cit. 2014-04-12], http://www-05.ibm.com/sk/cloud/#b2
[7] SCARFO, Antonio: New Security Perspectives around BYOD [online], November 2012, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6363095&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6362368%2F6363025%2F06363095.pdf%3Farnumber%3D6363095
[8] KUCHÁR, Martin: Nový IT trend BYOD: Úspory pre firmy, komfort zamestnancov [online], Október 2012, http://www.zive.sk/clanok/60938/novy-it-trend-byod-uspory-pre-firmy-komfort-zamestnancov
[9] COGNIZANT, Making BYOD Work for Your Organization [online], Jún 2012, http://www.cognizant.com/RecentHighlights/Making-BYOD-Work-for-Your-Organization.pdf
[10] ISO/IEC 27001, Informačná bezpečnosť – Cenné aktívum [online], http://www.vincotte.sk/component/content/article/32.html
[11] BRENNER, Joel: RISK MANAGEMENT: ISO 27001: Risk Management and Compliance [online], [cit. 2014-04-21],?AID=3255
[12] Microsoft Services: Security and governance strategies for the consumerization of IT [online], 2012 [cit 2014-04-22], http://az370354.vo.msecnd.net/whitepapers/Security-and-governance-strategies-for-the-consumerization-of-IT.pdf?WT.z_evt=WhitePaperClick
[13] CISCO SYSTEMS, Počítačové sítě bez předchozích znalostí, CP Books, a.s. Brno 2005, s. ISBN: 80-251-0538-5