kriativ.tech

Edition Nº 9 – 13-12-2021
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2021-10-67

BYOD – Impact in Architecture and Information Security Corporate Policy

Nuno Miguel Carvalho Galego
Assistent Professor – ISTEC Lisbon
galego.nuno@hotmail.com

Abstract: BYOD is a new business trend where employees are using their own devices for work purposes. This phenomenon has created new challenges in information security. Thus, organizations should adapt information security corporate strategy in order to address this new reality. This paper tries to identify and explore the optimal way to do this rearrangement, evaluating BYOD environment and measuring all relevant factors.

Keywords: BYOD; Mobility; Threat; Risk; Information Security; Corporate Strategy

1. Introduction

1.1 Key Concepts

Bring your own device (BYOD) - Business policy adopted by management where they allow them to use their personally owned devices like smartphones and tablets in order to access corporate resources like mails, databases etc (Singh, 2012).

Mobility - meaning working away from a traditional office setting or fixed location. (Astani, Ready, & Tessema, 2013). Working in anything is now possible anywhere, anytime.

Threat - possible danger that might exploit a vulnerability to breach security and thus cause possible harm. (International Organization for Standardization, 2008).

Risk - the potential of losing something of value, weighed against the potential to gain something of value. Values can be gained or lost when taking risk resulting from a given action, activity and/or inaction, foreseen or unforeseen. (Risk, s.d.).

Information Security - Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability). (ISACA, 2008).

Corporate Strategy – the pattern of decisions in a company that determines and reveals its objectives, purposes or goals, and defines the range of businesses the company is to pursue. (Nicolai, 1997).

1.2 BYOD Trend

Many organizations are adopting BYOD strategy since they recognize that employees have grown up with mobile devices and view these devices as the primary means of connecting, interacting with others, and increasingly using their mobile devices for work-related purposes. (Astani, Ready, & Tessema, 2013).

Recent numbers demonstrate the growing importance of mobile devices at work. According to research, mobile devices are already being used at around 80% of German companies for traditional telephone communication, for functions of a traditional telephone system, for e-mail, and for access to centralized calendars and contact information. 60% of companies in the USA and Europe have set up BYOD programs for smartphones, and 47% have done so for notebooks and tablets. (Disterer & Kleiner, 2013).

This numbers reflect the existence of an increasing awareness by organizations of this trend. An example of this is Intel, the

semiconductor giant, which has more than 39,000 devices registered on its network and about 70 percent of them are personal devices. With the involvement of numerous departments, a strategy was developed within six months. Then the company spent another nine months addressing legal and human resources issues. The objective was to establish a program that was an enabler of productivity and had the necessary safeguards and protections. (Astani, Ready, & Tessema, 2013).

In another perspective, BYOD can be seen as a response to growing pressure from the connected workforce of tomorrow and is a tactic for attracting and retaining top talent.

2. BYOD Risks

Every new technology comes with security issues, and mobile devices are clearly one of the biggest sources of information security issues. According to literature, the main threats associated with BYOD are the use of unencrypted connections, lost devices and virus/malware (Singh, 2012), which can generate the existence of the following security risks:

Data Leakage - The storage of critical data on employee-owned devices poses a great threat to organizations due to the intended or inadvertent disclosure of sensitive information, exposing the organization to the risk of data breach.

Loss of Control and Visibility - The ideia of 'ownership' is the core of this problem. If the employee is using a personal and mobile device, organizations do not have notion of the external security environment for BYOD compared to a traditional networked environment. This can only be avoided if the company involves users in the security strategy.

Ease of Device Loss - The relatively small size and portability of smartphones and tablets exposes BYOD devices, and the information stored on them, to a higher risk of being lost or stolen. In combination with weak passwords and authentication, it can conduct to considerable losses for companies (Dedeche, Liu, Le, & Lajami , 2013).

3. Information Security Corporate Strategy

3.1 Motivation

In order to treat risks and according to (Dedeche, Liu, Le, & Lajami , 2013), "Mobile devices that are insufficiently secured lead to unauthorized use and modification of data due to deliberate or negligent actions. When personal devices are being used, it must be assumed that the negligent or incautious behavior of users during private use will be transferred to business use. Additionally, there are legal stipulations and compliance rules on company use which must be met, such as requirements to document, archive, and back-up." Therefore, an enterprise strategy and an integrated vision for BYOD are mandatory if we want to take profit from them without compromising organization's information security.

3.2 Best Practices

According to Chris Corbet (Singh, 2012) in his article "BYOD: Industry Trends and Best Practices", there are 10 steps that can be followed for the successful implementation of BYOD:

- Creating a comprehensive BYOD policy. It includes decisions regarding which devices to be used, security settings, Applications to be loaded, Passcode etc..
- Measuring your mobile footprint
- Simplify user enrollment
- Configure policies over the air
- Provide self service capabilities
- Protect personal information (PII)
- Isolate corporate data
- Continuously monitor automated actions
- Manage data usage
- Track the ROI of BYOD

A technical approach for implementing these steps is a mobile device management solution. Mobile Device Management represents a central point of administration of all mobile devices (including personal devices) being used at a company with regard to company issues. It offers functions such as central device management,

logging, monitoring, and reporting, simple installation of applications on devices, checking devices for integrity, protecting devices from malware, central control of device settings, role-based authorization system for access control.

However, a technical solution is not enough. It must be included in an overall information security corporate strategy, to align employees' behaviors and actions towards minimizing the risks associated with BYOD. Policies must guarantee secure corporate information on mobile devices without detracting from the usability of the device, and thus productivity gained from BYOD. To achieve this, organizations need to understand their employee's motives to maintain control.

Involve employees in the development process of BYOD policies is necessary to obtain user buy-in and compliance and is an effective strategy for converting a weak link to a strong security control. Policies are more effective when employees understand why they must follow them. Otherwise, employees often find ways to circumvent strict IT policies that they do not agree with. (Disterer & Kleiner, 2013).

4. Conclusion

BYOD trend is a reality that come to stay in the present and grow in the near future, and organizations should explore the opportunities that BYOD brings, instead of rejecting it. In words of David Clarkson, HR manager at Cisco Canada, "Productivity happens where people are comfortable and using devices that are most comfortable for them." (Singh, 2012).

A successful BYOD corporate policy should contain three essential factors:

- Use of a Mobile Device Management solution
- Integration of Mobile Device Management in an overall information security corporate policy
- Involve employees in BYOD policy development

However, companies must always take into consideration benefits versus costs. (Singh, 2012), says that "although the maximum application of this policy is increase of workers performance and productivity but before using it the organization should find out the costs and benefits in order to justify the basis of application of this policy".

There is no that no single IS strategy exists for absolute protection against BYOD threats. (Dedeche, Liu, Le, & Lajami , 2013) Therefore, the purpose of this paper was to clearly identify the threats and risks of BYOD trend, in order to identify the most adequate corporate strategy.

5. References

Astani, M., Ready, K., & Tessema, M. (2013). BYOD ISSUES AND STRATEGIES IN ORGANIZATIONS. *Issues in Information Systems*, 195-201.

Dedeche, A., Liu, F., Le, M., & Lajami , S. (2013). Emergent BYOD Security Challenges. Melbourne, Australia: University of Melbourne.

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013* - (pp. 43 – 53). Procedia Technology.

International Organization for Standardization. (2008, 06 15). ISO/IEC 27005. (I. C. Office, Ed.) Retrieved 02 06, 2014

ISACA. (2008). *Glossary of Items.* Retrieved 02 06, 2014, from ISACA: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Nicolai, F. J. (1997). Resources Firms and Strategies. In *A Reader in the Resource-based Perspective.* Oxford.

Risk. (n.d.). Retrieved 02 06, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Risk

Singh, N. (2012). B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel". *Journal of Business Management & Social Sciences Research (JBM&SSR), 1*, 3.