Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 179 – 184

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)

Madhavi Dhingra

Amity University Madhya Pradesh, Gwalior – 474011, India

Abstract

Nowadays use of smart phones, tablets, laptops has become an integral part of schedule of work in most organizations and corporations. Many of them are adopting a new policy of allowing the employees to use their own devices at workplace.Despite the economical and usage benefits, Bring Your Own Device policy can pose some serious security risks and have negative impacts depending on employee ethics and lack of safeguards in framing company regulations. This paper investigates the legal issues regarding the implementation of BYOD policy and suggests the solutions to overcome those incidental problems.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:BYOD;Legal issues in BYOD; BYOD Policy; BYOD Security

1. Introduction

BYOD allows employees to bring their own computing devices such as laptops, smart phones, and/or tablets to work and incorporate them into the corporation or organization network rather than using company-owned devices. Numerous corporations and organizations have taken the lead in adopting BYOD namely Intel, Citrix Systems, Unisys, the White House, Apple and now it can't be denied that BYOD policy is going to be increasingly adopted by premier organizations[1].

BYOD's benefits are clear: employees are more familiar and satisfied while using their own device(s), and employers save money by not having to pay for high-priced devices and data plans. Companies' goals with BYOD are to increase the flexibility, convenience, and portability of devices in order to cater to their employees' workflows, which increase their productivity and morale[1].

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.030

The adoption rate of BYOD in organizations improve on the basis of three main key factors i.e. Employee code of conduct, security programs installation and efficient management rules[1]. All these are driving factors responsible for the overall performance of BYOD.

According to the study conducted by Tech Pro Research[2], 74% of respondents are saying that their organization is using or planning to use BYOD, refer (Fig.1).

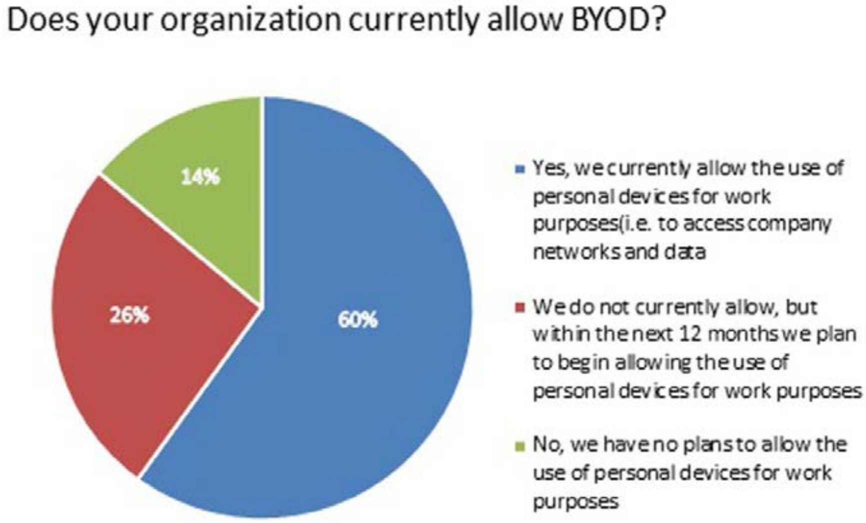

Fig. 1. Current BYOD Usage (TechPro Research)[2]

An efficient and effective BYOD policy must clearly state all the objectives and constraints related to the usage of the company assets. It should describe all the activities that are permitted on the devices when they are working in the corporate networking systems. Many companies do not have any proper architecture of information, system hardware and other resources which are to be utilized[3]. To overcome this problem, several models are developed to provide the software tools and security strategies in order to reduce the challenges and risks. At present, three security models are used for BYOD – Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Information Management (MIM). These software's help in controlling the employee owned devices in their personal and work purposes[4].

BYOD can bring in many risks and challenges and the biggest of them all being data loss. In this paper a number of legal concerns within corporate Bring Your Own Device (BYOD) programs are reviewed. Section 2 provides the current and predicted statistics of BYOD. The figures show that BYOD will exist in near future with Internet of Things(IoT) and thus its challenges need to be overcome. Section 3 will cover the legal concerns and its solutions.

2. Current status of BYOD

Some of the stats of BYOD are defined below[5,6]

- Gartner predicts by 2017, 50% of employers will require employees to have their own device for work purposes.
- Over 70% of mobile professionals will conduct their work on personal smart devices by 2018.
- A further study by Juniper Research concluded that by 2018, there will be more than one billion devices used in BYOD programs worldwide.

- Analysts have forecasted that, by 2016, worldwide shipments of smart phones will reach 480 million, with 65% being used in bring-your-own device environments.
- 38 percent of companies are expected to stop providing devices to workers by 2016.
- Smart device popularity drives opportunity for mobile app stores which by 2016 will reach 310 billion downloads and $74 billion in revenue.
- Gartner estimates that tablet production will grow from slightly fewer than 120 million units to more than 370 million units in 2016. Smartphone production to increase from approximately 650 million units in 2012 to more than 1.3 billion units in 2016
- 90% of IT professionals express strong concern about sharing content via mobile devices.
- Just 30% of companies have approved BYOD policies.
- Only 15% of companies sanction use of consumer-grade cloud services—yet 58% of employees use them anyway.
- 85% of organizations allow employees to bring their own devices to work.
- More than 50% of organizations rely on their users to protect owned devices personally.
- 53% of information users use their own personal devices for work; install unsupported software; or use unsupported Internet based services like Dropbox, Skype, Twitter, or Facebook to help them do their jobs.

3. Legal Issues with BYOD

3.1. Maintaining and Storing Data

When the organization data is kept in the employee's personal devices, then decision of sending and receiving data from the corporate network is also on the organization. It becomes very difficult to maintain the integrity of data when it is on the public network and accessed by the public access point. Another possibility of data leakage is the storage card used on mobile devices. The usage of storage card is very common today and very few persons use encryption methods to protect the stored data[7].

Solution of this issue can be done by accessing corporate networks by virtual private networks that are available in corporate editions. It creates a secure channel between source and destination and provides protection to all the data travelling over the network. This ensures the confidentiality of information in the network. Full disk encryption is the solution to secure data stored on the secondary devices. The maintenance and storage issues are fewer when organizations have complete control over the devices and all the terms are legally mentioned in the consent document.

3.2. BYOD Security

Organizations implementing a BYOD strategy need to explore the concept of reasonable security for personal computer devices. A tedious process is adopted for development of security policies so as to uncover, detect and avoid any security risks. The output is the set of highly effective and technical controls or programs. The security policies to be followed are different for an enterprise owned device and an employee owned device. For example, company can implement system configuration according to the need, can encrypt data or perform investigation on the device, can monitor the data usage to detect misuse or hacking, and can perform other system security related tasks without any problem. But when it comes to the employee own device, all these things are not possible. Controlling power of the organization is very weak and thus they are totally dependent on the employee for securing the device[7].

Often, organization employees are unwilling to implement suggested security policies thereby increasing the security and legal risks. In such cases, the organization fails to implement its own security control thus providing a loophole to the intruders. This presents a serious problem in the BYOD context.

3.3. BYOD and Employee Privacy

Another major issue in implementing BYOD policy is employee privacy. Employee's personal device contains private content like photos, movies, account numbers, user names, and passwords, etc. and the same device will be used by the organization also. Organization has all the rights to monitor the activities related with the device. In general conditions all the devices are attached at network and organizations monitor the networked devices, but when personal devices are considered, such monitoring activities is not possible.

Investigation of personal device is also a matter of concern affecting the adoption of BYOD policy. If any data is needed to detect the security breach, the private or personal information of the device is also captured. If organizationsets the limit on capturing the data, then actual investigation could not be done effectively. All these issues direct the organization to secure their employee details while maintaining their monitoring goals.

Organization's should make their employees aware of the privacy trade-offs and the reasonable expectations of privacy related to their use of a personal device for work. If monitoring or an investigation is necessary, organizations should design their efforts in a manner that seeks to minimize the potential exposure of personal and private information[7].

3.4. Breach Response, Notification and Investigation

Handling of the organization data is one of the most difficult tasks. All these complexities are managed by the data loss prevention DLP software that provides the ability to tag their data in order to track its movement within the network. All the details will be recorded in the log file. Normal security breach avoidance plans focus on the data that is travelling in the network and directly attacked by the attacker. BYOD plans focus on those data also that has not been transferred to anywhere and yet accessible to public mistakenly.

There are some more challenges in context of incident response and investigations that are affecting the security, privacy issues. Personal devices are not possessed fully by the organization, due to which if any security breach occurs, it becomes difficult to access them. Once a breach occurs, organization will perform the notification procedure and risk assessment to identify the potential loss of data.

This will also become problematic for the employee himself who is unable to use their own personal device during the period of investigation. Furthermore, all the images or data that will be taken from the device during investigation will violate the privacy of the individual[7].

Thus, proper BYOD strategies are to be developed and to be informed to the employees by the organization to overcome the foresaid issues in incident response and investigation. Employees should be made aware about the consequences of previous security breach incidents and their responsibility of following procedures after the incident happened. Employee should understand that proper notification will decrease the severity levels of data loss. Category of employees will also affect the level of confidentiality of data, like a Director will be having large amount of sensitive and confidential information in comparison with the first grade employee.

3.5. Remote Wiping and Blocking

When personal devices are to be used for the benefit of the organization, there are certain restrictions which are imposed so as to secure the confidential and sensitive data of the organization. This will be a challenge for the employee who wants to use certain programs or applications for their personal use. In order to block certain contents, employee must load certain software in his personal device. Wiping off the content is also a major problem, where organization wants to wipe certain data from employee's personal device. Wiping, bricking or blocking of a device could damage the device or could remove the personal data of the employee.

Employees must be aware about the consequences of blocking; wiping data caused by the software's to be installed in their own devices. All such conditions must bespecified in personal device use policy and the necessary consent forms.

3.6. Secure destruction of corporate data

The requirement of destruction of data comes when either the company wants an updated configured device or the employee wants to upgrade their personal device. In both cases, the old device contents need to be removed in order to avoid the loss of important data. An unscrupulous employee can harm the company by passing on sensitive company data to public.

One of the solutions is to remotely reset an employee’s device by using Mobile Device Management tools. These tools are capable of deleting the partitions of data. Terms of employment must contain this clause so that when required, the complete reset of the device can be done without surprising him or her.

4. Recommendations

Organizations BYOD policy should include policies for[8]-

- Securing mobile devices
- Encryption and user passwords
- Data categorization
- Antivirus software
- Wireless accessing
- Security breach incident and its response
- Remote working
- Privacy preserving

It is important to understand that designing and implementing security policy for company owned device and employee personal device are different. Policies should be clear regarding the platforms to be used, services that are to be provided, risks and responsibilities to be handled, and minimum device requirements or configurations. For maintaining the policy, organizations must utilize the key technologies to make a separation between the enterprise and personal data. These tasks will be accomplished by using device management systems that help in securing shared data and collaborating among mobile devices.

Also user support, third party cloud services are to be used for effective implementation.Service staff should be properly trained and forums, emails and social networking tools should be there for user support.

5. Review Results

BYOD comes under consumerization of IT. Organizations cannot stop their employees from bringing their own devices at the workplace. And allowing the devices at separate levels need serious security measures to be taken. There comes various issues that are affecting the BYOD adoption. The chart below describes all the possible concerns.

Table 1. Factors affecting BYOD adoption

Factors Affecting BYOD Adoption	Description
Company Allowing to use BYOD	According to published stats[5, 6], 84% companies are allowing BYOD. There still 16% companies left not wanting to adopt BYOD.
Company Size	Medium size companies with 1500 to 2000 employees adopting BYOD Smaller companies and larger have lower adoption rate
Industry Category	Education industry is using BYOD at a large scale.
Device Type Used	It can be Laptop, Smartphone or Tablet.
End Point Security	BYOD increases the end point risk by connecting more personal devices to the open network.
Device Control	Security policy are installed in the device for controlling it.
Device Management	Security measures are used for preventing devices from attacks.

The top concerns with adoption of BYOD is security, data loss, compliance, personal data and privacy.

For managing all the stated concerns organizations are planning and implementing layered approach of policies to handle each of the concern. They must determine the security and control policies and make a balance with the employees' rights to deal with the changing scenario and to gain the consumerrelated benefits. These policies should containthe layers for policy, user awareness, management and technical controls.

Thus the organization must make a balance between the control and freedom of the employee-owned devices for increased productivity and data protection.

6. Conclusion

Bring your own device (BYOD) has proved to be a successful technology nowadays. Organizations are adopting it thereby reducing their infrastructure costing and increasing the flexibility of the users. The enunciation of mobile policies has always been a tough task, as companies need to manage the productivity as well as has to avoid the security risks. The decision of choosing the purpose built device or BYOD device is not so clear-cut. There are many risks associated with BYOD policy that can be managed to a greater extent by preparing effective security policies and using device management software's. It is up to company to develop such BYOD policy that not only protects sensitive data but also take care of employee rights. For doing this, organizations need more systematic integrated procedures for managing threats as well as maintaining the employee devices and the legal implications of the BYOD approach take into account all the relevant factors to harvest the benefits for the organization.

References

1. Current Status, Issues, and Future of Bring Your Own Device (BYOD), Aaron M. French, Article published in Communications of the Association for Information Systems, Volume 35, Article 10, November 2014, pp. 191-197
2. Part Of A Zdnet Special Feature: Ces 2015: The Big Trends For Business, Research: 74 percent using or adopting BYOD, Teena Hammond | January 5, 2015, Available online at: http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
3. Pedro Pavón, Risky Business: “Bring-Your-Own-Device” and Your Company, Available online at: http://www.americanbar.org/publications/blt/2013/09/01_pavon.html
4. Penang, Malaysia, Meisam Eslahi, Maryam Var Naseri, BYOD: Current State and Security Challenges, 2014 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) , April 7 - 8, 2014,
5. Byod Top 6 Trends You Need To Know About In 2015, Article published in Macquarie Telecom. Available online at: http://www.macquarietelecom.com/resources/blog/25/06/2015/byod-top-6-trends/
6. 10 Stats That Show It's Time To Prepare For Byod Network Design, Article published in Secure Edge Networks. Available online at: http://www.securedgenetworks.com/blog/10-Stats-that-Show-it-s-Time-to-Prepare-for-BYOD-Network-Design
7. Robert J. Mavretich, Legal Issues within Corporate "Bring Your Own Device" Programs, Sans Institute, May 2012
8. David A. Willis, Bring Your Own Device: The Facts and the Future, Gartner Report 11 April 2013
9. Prashant Kumar Gajar, Arnab Ghosh, Shashikant Rai, Bring Your Own Device (Byod): Security Risks And Mitigating Strategies, Volume 4, No. 4, Journal of Global Research in Computer Science, April 2013
10. Drury, R. Absalom, BYOD: an emerging market trend in more ways than one, 2012. Available: http://ovum.com/research/byod-anemerging-market-trend-in-more-ways-than-one/
11. K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, 2012, pp. 53-55.
12. Morrow, "BYOD security challenges: control and protect your most sensitive data," Network Security, vol. 2012, 2012, pp. 5-8.