BYOD adoption – still a big challenge for organizations

Siddhartha Shyam Vyas
Research Scholar, Dept of CSE, JNU Jodhpur
siddhartha.svmarc.im@gmail.com

***Abstract*—Technologies & innovations which have tremendously impacted every aspect of person's life – from personal to workplace through the convergence of electronic media, digital equipments – all integrated in one has led to the growth of digital revolution. However, as technology has become an important part of our lives, security has become a major challenge for the organizations. There are a list of security challenges for businesses when it comes to adopting BYOD program.**
However, past journals & research papers have identified risks and indicated the strategies & frameworks in relation to BYOD adoption, but despite all this, organizations are still lagging behind in proper BYOD adoption. This research paper primarily focuses on: challenges in BYOD adoption & identification of available frameworks.

Personal devices are entering the workplaces- so there is a challenge for companies to carefully devise their BYOD policies and BYOD management systems.

KEYWORDS: BYOD, Bring Your Own Device, BYOD Security, Information Security, BYOD adoption.

I. INTRODUCTION

The use of mobile devices represents a new information age. All the confidential data & information are managed and accessed via technology and applications. These applications serve as a bridge between the user and the data / information to be accessed. The information can be easily copied, transported, disseminated, and lost. BYOD *(Bring Your Own Device)* is still a new concept for the organisation in many areas. This increases scope altogether for an employee to use one's owned and familiar technology at work, but in turn creates many challenges for the organization.

Before deploying BYOD in any organization, it is very important to consider the risk landscape of a BYOD mobile device deployment.

However, managing security for devices on multiple platforms has become a major challenge. The BYOD ability to retain talented employees & attract the best became a major part of competitive advantage for the organizations – which led to the increasing popularity of BYOD. Hence many savings accrue to organizations as a result of BYOD adoption. Familiarity and awareness of challenges in safe implementation of BYOD will help organizations and their employees understand the critical areas which can help secure their mobile devices.

The paper will help in knowing the various challenges that organizations are facing in adopting BYOD. Various strategies & frameworks are available, but still many organizations are lagging behind. It also intends to find ways to improve the existing conditions and find new ways for it.

This introduction section is followed by a literature review & methodology. Finally, the discussion of findings will be followed by recommendations and a conclusion.

II. LITERATURE REVIEW

BYOD is a rapidly evolving concept – which has become a big challenge for business organizations and IT cultures to tackle. Instead of having all devices supplied by the employers, employees can bring in their own devices like: smartphones, tablets, laptops etc. etc. at the workplace. Due to the gainful benefits provided by BYOD, it simply cannot be ignored. There aren't industry that isn't putting the mobile revolution to work, but BYOD acceptance would come with adopting a secure policy – which is still a major concern.

Simt (2009) said that good policy will encompass standardized rules for the safest usage of mobile devices.
ENISA (2010) inspired to take a step toward better security in terms of being aware of the various threats to information systems and their consequences.

Ernst & Young (2012) gave various information security strategies for BYOD adoption. They talked about methods of preventing security risk & technical challenges. Whereas, **Markeli & Bernik** (2012) said that mobile devices are targeted by blended threats, which can pose a problem or danger to individuals and organizations.

According to **Thomson (2012),** BYOD devices include any device that is purchased by the users themselves such as laptops, netbooks, e-readers, smartphones, tab devices – which are facing lot of challenges.

As per the survey conducted by **Schulze (2013),** 60% of organizations have not yet adopted BYOD, but are considering it. Only 10% of non-adopters are ruling it out. 24% are actively working on policies, procedures & infrastructure for BYOD**.**

Cognizant Co. (2014) in their report stated that BYOD Adoption is a necessity for all organizations, to survive in this dynamic world. They also faced various challenges like BYOD cost, their security, data protection & support system.

J. Gold Associates (2015) reported that about 25 – 35% of corporations currently have a BYOD policy and the numbers are expected to exceed 50% over the next two years, they are going to consider it more for implementation in developed cities.

Results of research carried out by **Langhom D (2015)** shows that the malware applications has increased upto a large extent in the past six months – by 14% in comparison to threats from spyware.

III. OBJECTIVES

1. To identify challenges faced by organizations in adopting BYOD
2. To suggest measures for overcoming these challenges

IV. RESEARCH METHODOLOGY

The paper focuses on the challenges that organizations are facing with reference to BYOD adoption. An attempt was made to find out results from various articles, journals & paper that suggested various strategies & framework that are adopted by organisations successfully.

V. FINDINGS

BYOD is a phenomenon that many organisations are concerned about since it's implementation would require framing of proper policies. With availability of benefits like cost savings, employee satisfaction to work anywhere – anytime, more technology familiarity, still organisations are unable to adopt it. It has been analysed that organizations are facing various challenges like:

- Data Security Challenge – The main fear for organizations is the lost, stolen & misuse of their data. To allow employees to bring their own devices is a matter of security concern.
- Technical Challenge – The various challenges related to technical aspects are data access control, maintaining stable network connections, protecting cloud storage, controlling data distributions, etc. is a big task to provide 24/7 ongoing support to devices.
- Human Aspects Challenge – Owners of devices are hurdles in implementing BYOD policies. It is mandatory for organizations to train employees and face their reaction & compliance against policies.
- Deployment Challenge – These are related with deployment of BYOD security into existing networks. They determine which department within organization would be requiring BYOD & how BYOD would be necessary there while implementing policies.
- Policy & Regulation Challenge – would define the rules incorporated into organization's BYOD policy as regards to the corporate data. This means that global organizations would have to adjust their BYOD policies as per the laws of different countries.
- Financial Challenge – would be to ensure the financial viability of the BYOD program. It has to be clearly defined within the BYOD policy what financial support would organization be providing to their employees and to what extent.

VI. RECOMMENDATIONS

.After analyzing the challenges faced by organizations and knowing about the pros & cons of BYOD adoption, some measures have been suggested to make organizations easily adopt BYOD policy. With little efforts, company can easily prepare themselves for successful BYOD adoption. Here are some points that will help:

- It is required to instate a strong password policy on network board, so that it can be saved from hackers to steal data.
- Every device bought into the company should be registered with all details, to help in tracking.
- Proper framework & strategies must be adopted for a secure BYOD program.
- Training of employees is required to prevent their devices from malware & threats.
- Network security should be of main importance with effective firewall.
- Good option is to create a company cloud, so that data can be accessed by users outside the network.
- It is important to redefine your support policies for end users about organizations responsibility with regards to device, data lost or security.

VII. CONCLUSION

A successful BYOD policy allows employees to be productive outside the work schedule, allowing them

flexibility. With changing time, organizations need to have a formal policy & framework to adopt BYOD & enforce it. Although various policies & framework are suggested, still some aspect are left. Many large organisations are in middle of term, whether to accept it or not. The real challenge, therefore, is the acceptance of BYOD readiness on the part of top-level management – which can be achieved with the help of proper research, analysis and knowledge-sharing between industry and academia.

REFERENCES

1. Cognizant, (2014). Making byod work for your organization. Banglore: Whitepaper.
2. Ernst & Young's *2012 global information security survey 'Fighting to close the gap*" AUDIT AND RISK: , pp 10-11.
3. European Network and Information Security Agency (ENISA). (2010). *The New User`s Guide: How to Rise Informations Security Awareness.* Luxembourg: Publications Office of the European Union.
4. Gold, J. *Mobile device strategy* 2015 May 5 available from URL: http://searchconsumerization.techtarget.com/tip/Mobile-device-strategy-bypassed-as-enterprises-face-tablet-invasion
5. Langhorn D. *The mobile workforce and BYOD maturing* Business Trends December 2015 New York
6. Markelj B, Bernik I. *Mobile Devices and Corporate Data Security*. International Journal of Education and Information Technologies [Online] 2012 Available from: URL: http://www.w.naun.org/multimedia/NAUN/educationinformation/17-591.pdf
7. Schulze, H. *BYOD & MOBILE SECURITY* Online [1-26. Available from URL: http://blog.lumension.com/docs/BYOD-and-Mobile-Security-Report-2013.pdf
8. Simt (2009).BYOD implementations & Framework. Acquired 11. 10. 2011 on http://www.simt.si/informacijski_sistemi.html.
9. Thomson, G. (2012). BYOD: Enabling the chaos. Network Security, 2012(2), 5-8