International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Empirical Survey on BYOD Security and Usage

P.Soubhagyalakshmi, K. Satyanarayan Reddy

Abstract - Recently, Bring Your own Device or BYOD has become one of the most popular models for enterprises to provide mobility and flexibility in workplaces. The emergence of new technologies and features of mobile devices makes them integral parts of every aspect of daily business activities. Also, mobile networks are now well integrated with the Internet (e.g. 3G, 4G and LTE technologies), therefore, in BYOD, the personal devices (i.e. mobile devices) can be used to increase employees' satisfaction and reduce an organization's device costs. Mobile devices are not well protected compared to computer and computer networks and users pay less attention to security updates and solutions.

In this paper, the work focus on identifying the willingness to adopt BYOD in Companies in Bangalore by conducting a Questionnaire Survey so that their views are understood appropriately

From this survey, it is possible to identify the importance and requirement of the BYOD deployment in various business verticals in near future. Even, it gives the understanding of the usage of types of BYOD schemes or policies adopted by the employees in various organizations. This survey paper helpful and led to the origin of research by analyzing BYOD policies to avoid the security breaches with better capabilities of policies. Using the employee own devices at workplace causes the security risks. This paper highlights the need and necessity to mitigate the security issues related to the sensible data as the employees are willing to make use of their own devices at workplace. This paper conveys that, there is a need of security as the use of BYOD usage by the employees in the various organizations.

Index Terms: BYOD, Security & Deployments.

I. INTRODUCTION

These Days, staffs expect to use personal smart phones and mobile devices at work, making BYOD security a priority for IT teams. Many firms that allow workers to use their own mobile devices at work implement a BYOD security policy that clearly outlines the company's position and governance policy to help IT higher manage these devices and guarantee network security is not compromised by workers practice their own devices at work.

BYOD security could also be addressed by having IT supply elaborate security wants for each quite personal device that is utilized within the point and connected to the corporate network.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
P. Soubhagyalakshmi*, Research Scholar, Visvesvaraya Technological University, Belagavi, India.
Dr. K. Satyanarayan Reddy, ISE Department, Cambridge Institute of Technology, Bangalore, India.

As AN example, it ought to need devices to be designed with passwords, veto specific forms of applications from being place in on the device or want all info on the device to be encrypted. Different BYOD security policy initiatives would possibly embody limiting activities that workers unit allowed to perform on these devices at work (e.g. Email usage is prohibited to company email accounts only) and periodic IT audits to form positive the device is in compliance with the company's BYOD security policy. Bring Your Own Device (BYOD) was first perceived by Ballagas et al., [8] at UBICOMP in 2004.

This idea is frequently alluded to as BYOD and alludes to utilizing one's own cell phone for non-individual or business-related exercises. BYOD can bring change to the social insurance benefits by expanding correspondence and coordination increment constant access to the information, actualize integrative workforce forms which is exceptionally significant in the present human services condition [9].

As indicated by Figure 1 below, the portability plan that is joined with association's methodology and IT which deliver those results that run the associations to its objective and achievement [10].

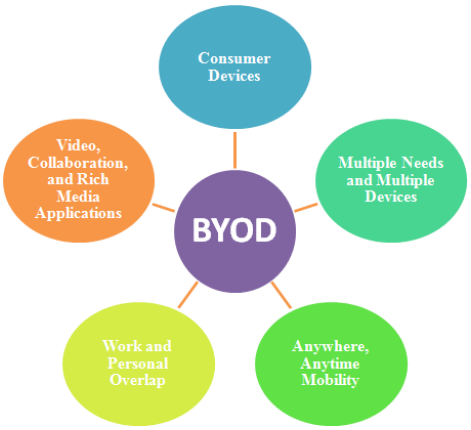


Figure 1: Use of BYOD

Handheld PCs and cell phones give moment access to immense sums and sorts of helpful data for medicinal services experts. Their diminished size and expanded preparing speed have prompted the quick reception in social insurance [11]. Handheld PCs or Personal Digital Assistants (PDAs) offer compact and unpretentious access to clinical information and applicable data at the purpose of consideration [12] [13]. The across the board reception of cell phones in human services establishments, while advantageous, can make security worries for specialists.

Specialist's security chance observation is identified with different emotional convictions which would in a roundabout way affect their conduct goal in both utilizing the devices and embracing security controls in the working environment [14].

II. LITERATURE REVIEW

Kerravala Zeus [1] in her study on Bring Your Own Device needs new network strategies discloses the importance of BYOD in IT field. It offers rise to 3 transitions like: evolution of devices, migration to cloud primarily based applications and fast advancement of wireless technologies.

ZK analysis recommends the following: have an optical maser target user expertise, embrace client technologies and BYOD, be willing to just accept amendment and develop new strategic relationships. As airlines have doubled result of worker owned device and traveler in hand device. One affects the performance of the company and also the different influences on the sales. [1, 2].

A comparison has been created by the research worker on the basis of information collected through. As compared, three outcomes were expected like positive, negative or unknown. If information is inaccessible then it's considered as unknown, regeneration reflects that organization pays attention on that and negative says that organization. The devices were categorized into two types like mobile communication devices: smartphones, tablets and mobile workstations: laptops, netbooks or immoderate books. Enterprise quality is often accumulated with the employment of devices at work place.

It gives following advantages like improved business continuity, effective mobile management and seamless business operations in conjunction with another advantages like property, versatile communication, collaboration and sharing of information, swift and enlightened business choices. Software package development kit includes: Advanced add-on alters businesses to develop their own enterprise applications with access management practicality. So that, high- level security providing protection for employee's mobile devices and company information. A range of SDKs obtainable on the Samsung Developer web site facilitate businesses simply realize the right SDKs and develop applications Microsoft EAS (Exchange ActiveSync):

A communication protocol designed for the synchronization of emails, contacts and calendars between an electronic messaging server and mobile devices enabling seamless association to business functions. Cisco Jabber: A communication tool that streamlines communication and enhances productivity with integrated IM, voice, video, voice electronic messaging, desktop sharing and conferencing [3, 4].

BYOD is pervasive and staff need to figure with latest and best hardware and computer code at their work place. BYOD utility at the side of the reduction in price of production and up-gradation of organization additionally edges in the sort of improvement within the productivity, worker satisfaction, morale, loyalty, flexibility of their work, standardization. Consumerization of IT and speedy development within the mobile technologies within the surroundings makes the work of organization mobile, paperless and wireless. It was additionally found throughout the study that BYOD is growing quickly owing to telework and mix of domestic and private life. [3, 6].

The development that has emerged within the business surroundings is BYOD which suggests that staff use their personal device to access company resources for work, within or outside structure environment. This new development brings new opportunities however it has several risks related to it.

As the mobile devices are used for both personal and professional work, more opportunities for security risks that require to be eased. The aim of this work is to produce varied quality methods, defenses and measures, control aspect, management and governance facet to seem forth in implementing a B BYOD strategy in a corporation. [7, 8].

III. RESULTS & DISCUSSION

A.Analysis & Interpretation:

Using IBM SPSS software, following sequence of operations are performed to derive the results which supports the conclusion.

a The Questionaries' data collected has been primarily tabulated & Master table was prepared.

b Sample was tested for reliability using Cronbach's alpha test technique available in the software as built-in.

c Percentage analysis is the basic tool for analysis of each questionnaire and the data is tabulated from Table I to Table V.

d Regression analysis a statistical process for estimating the relationships among variables is used and data tabulated in Table VI, Table VII.

Table I: Descriptive for question Job Title in IT Department

What is your job title in IT department?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Application development /software/hardware programmer Related	36	30	30	30

	Data center related	24	20	20	50
	Customer Support related	12	10	10	60
	Desktop Support related	24	20	20	80
	Network architect related	12	20	20	100
	Total	120	100	100	

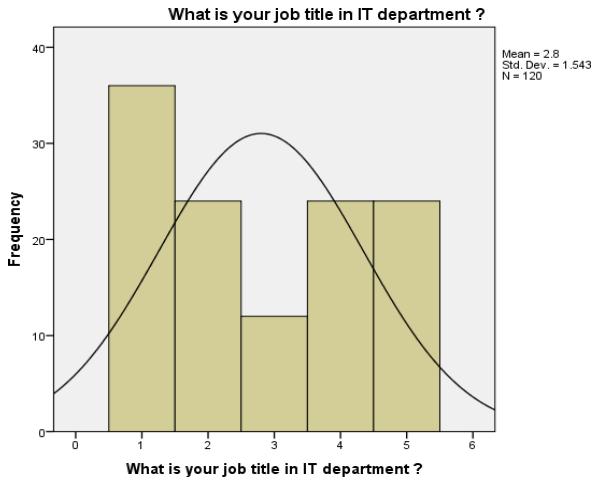


Figure 2: Descriptive for question Job Title in IT

Considering Table I & Figure 2, it can be viewed and observed that for a total of 120 respondents who are software professionals with the question on their roles in the company, Majority were application developer whereas other department's desktop, network & data center participants were lesser in number and equally distributed to twenty.

Table II: Company Implement BYOD Policy

Does Your Company Implement BYOD Policy					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	72	60.0	60.0	60.0
	No	36	30.0	30.0	90.0
	Not applicable	12	10.0	10.0	100.0
	Total	120	100.0	100.0	

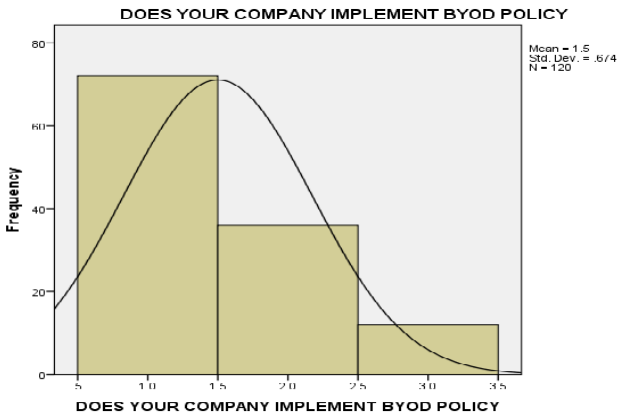


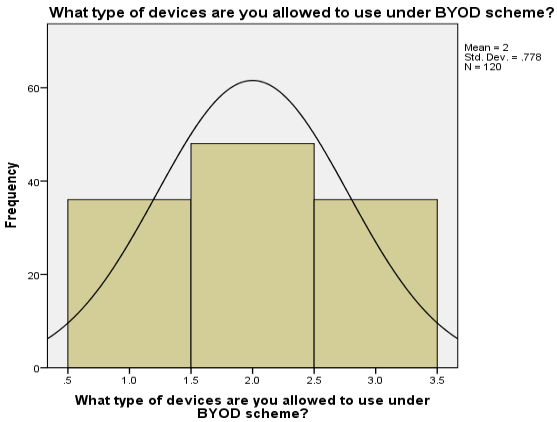
Figure 3: Company Implement BYOD Policy

Considering Table II & Figure 3, it can be observed that for a total of 120 respondents who are software professionals with the question on Implementing BYOD Policy, 60% of the respondents said yes, 36% of the respondents said no & 10 % of the respondents told its not applicable.

Table III: Descriptive for question Usage of devices under BYOD Scheme

What type of devices are you allowed to use under BYOD scheme?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Smart Phone	36	30.0	30.0	30.0
	Tablet	48	40.0	40.0	70.0
	Laptop	36	30.0	30.0	100.0
	Total	120	100.0	100.0	

Figure 4: Descriptive for question Usage of devices under BYOD Scheme



Considering Table III & Figure 4, it can be observed that for a total of 120 respondents who are software professionals with the question on their usage of devices in company with respect to BYOD, tablet, laptop & Smartphone were used almost in equal proportions, highest being tablet around 40%.

Table IV: Descriptive for Question Working under BYOD Scheme

How long have you been working under BYOD scheme?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 - 3 Years	84	70.0	70.0	70.0
	4 - 6 Years	12	10.0	10.0	80.0

	More Than 6 Years	12	10.0	10.0	90.0
	Not Applicable	12	10.0	10.0	100.0
	Total	120	100.0	100.0	

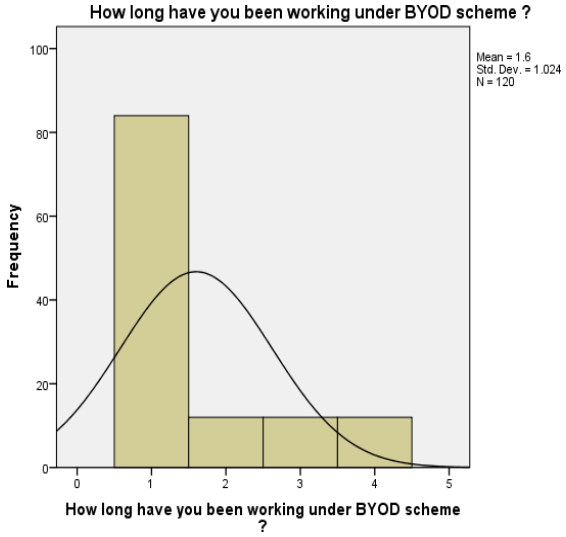


Figure 5: Descriptive for Question Working under BYOD Scheme

Considering Table IV & Figure 5, it can be observed that for a total of 120 respondents who are software professionals with the question on experience in working on BYOD Scheme, Majority had been working since 0 – 3 Year, which constitutes to around 70 %.

Table V: Willingness to adopt BYOD Policy

Are you willing to adopt/accept BYOD policy?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	96	80.0	80.0	80.0
	No	24	20.0	20.0	100.0
	Total	120	100.0	100.0	

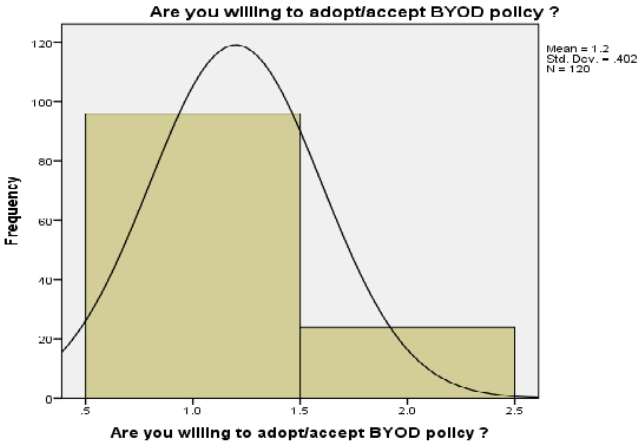


Figure 6: Willingness to adopt BYOD Policy

Considering Table V & Figure 6, it can be observed that for a total of 120 respondents who are software professionals with the question on their willingness to accept/adopt BYOD Policy, 80% of the developers were interested in continuing with BYOD Scheme.

IBM SPSS software used in getting the regression values given in the Table VI: Model Summary-1 and table VII: Model Summary-2. This software generates the regression values for the chosen Dependent Variable(X) and Independent Variable(Y). Regression technique identifies the relationship between these variables as whether positive or negative and how it is.

Table VI: Model Summary -1

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.890[a]	.792	.791	.488

Dependent Variable (X)**:** How long have you been working under BYOD scheme?

Independent Variable(Y)**:** Does your company implement BYOD Policy?

R^2, the Coefficient of Determination, tells how many points fall on the regression line. In Model Summary 1 – 0.792 means that 79% of the variation of y-values around the mean is explained by the x-values. In other words, 79% of the values fit the model and explains that BYOD scheme is implemented in large scale. So that, hypothesis H1 holds. Hence, H1–BYOD Scheme is implemented in large scale and H0 –BYOD Scheme is implemented in lower scale.

H1, Alternate Hypothesis is accepted.

Table VII: Model Summary – 2

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.839[a]	.704	.703	.588

a, Predictors: (Constant), Does your company implement BYOD Policy

Dependent Variable(X): Are you willing to adopt/accept BYOD policy?

Independent Variable(Y): Does your company implement BYOD Policy?

In Model Summary 2 – 0.839 means that 83% of the variation of y-values around the mean is explained by the x-values. In other words, 83% of the values fit the model and explains that more number of employees are willing to adopt the BYOD policy at workplace. So that, hypothesis H2 holds.

Hence, H0 –There exists no relationship between Employees wanting to implement BYOD Scheme and H2 –There exists a positive relationship between employees interested in implementing BYOD Scheme.

H2, Alternate Hypothesis is accepted.

I. CONCLUSION

It can be observed that carrying out a Questionnaire survey, on BYOD Usage & Security to understand the current scenario in the market, 120 Software Professionals filled the questionnaire which belonged to 13 different software companies. Majority of the professionals like the technology and want to continue using it. There exists a positive relationship between employees interested in implementing BYOD Scheme & it is implemented in Large Scale in spite of the security risks.

Hence, it is needed to evolve BYOD schemes with better enhancements to resolve the security risks. The empirical evidence supports that, there is need of BYOD usage in various business organizations and also better BYOD schemes need to use to protect the sensible data of the organizations.

ACKNOWLEDGMENT

The authors extend their sincere gratitude to the Management, Principal of Cambridge Institute of Technology (affiliated to Visvesvaraya Technological University, Belagavi), K R Puram, Bangalore, Karnataka State. Further authors express heartfelt thanks to the HOD of Dept. of CSE for having extended Library Facility. Authors are indebted to the Authorities of VTU RRC for having extended all the facilities for carrying out the current research work at their Laboratory facilities.

REFERENCES

1. KerravalaZeus, Sita Absalom, R. (2013) International Data Privacy Legislation Review: A guide for BYOD Policies. Ovum. vol. 1, pp. 1-23.
2. HensemaMartijn Astani, M., Ready, K., Tessema, M.(2013) BYOD Issues and Strategies in Organisations.Issues in Information Systems. vol. 14, issue 2, pp. 195- 201.
3. Osterman, Amoroso, EG. (2013). From the Enterprise Perimeter to a Mobility Enabled Secure Cloud. Security & Privacy, IEEE. vol. 1, pp. 23 - 31.
4. ARNAB GHOSH, Australian Government, Department of defence: intelligence and security. (2014) Bring Your Own Device (BYOD) For Executives. Paper explaining guidelines for corporate BYOD policies, submitted online, February 2014, Australia, pp. 1-3.
5. Barker, J (2014) Kensington Survey: Majority of organizations report BYOD creates greater security risks. Close-Up media Inc, Coventry, USA, November 2014. pp. 1-2.
6. Beaver K (2012) The BYOD Security Loophole. In Security Technology Executive. Vol. May 2012, pp.20.
7. Bradford Networks (2012) Ten Steps to Secure BYOD. Whitepaper by Bradford Networks, MA, USA, 2012. pp. 1-4.
8. Chen, H., Li, Hoang, T., Lou, X. (2013) Security challenges of BYOD: a security education, training and awareness perspective. The University of Melbourne, Australia. pp. 1-8.
9. Dell Inc (2015) Dell Offers Top Five Best practices for Overcoming BYOD and Mobile Security Challenges. Paper presented to ENP Newswire Publishing, UK. pp. 1-3.
10. Denman, S. (2012). Why multi-layered security is still the best defence. Network Security, Vol 2012. Issue 3. Pp. 5–7.
11. Disterer G and Kleiner C (2013) BYOD Bring Your Own Device. Procedia Technology Vol. 9, 43-53.
12. Dongwan, K., Changmin, J., Taeeum, K., Hwankuk, K. (2015) A Study on Security framework for BYOD environment. Institute of Research Engineers and Doctors, USA. Pp. 89-92.
13. Eschelbeck G and Schwartzberg D (2012) BYOD Risks and Rewards: How to keep employee smartphones, laptops and tablets secure. Whitepaper by Sophos, Oxford, UK, June 2012. pp. 1-7.
14. Eslahi, M., Naseri, M., Hashim, H., Tahir, NM. Mat Saad, E. (2013) BYOD: Current State and Security Challenges. Universitii Teknologi MARA, Malaysia Pp. 1-4.

AUTHORS PROFILE

P.Soubhagyalakshmi secured her M.Tech in Computer Science & Engineering from JNTU, Hyderabad in 2006. She is pursuing Ph.D. (Computer Science) degree in VTU, Belagavi, and Karnataka.

Dr. K. Satyanarayan Reddy secured his M.Sc. & M.Phil. (Mathematics) Degrees from Nagpur University, Maharashtra State, and M. Tech (CSE With specialization in Computer Applications) from **I**ndian **S**chool of **M**ines [now **IIT (ISM)**], **Dhanbad**, Jharkhand in 1987, 1988 and 2000 respectively. He was awarded PhD (Computer Science) degree in the year 2012 from School of Science & Technology, Dept. of Computer Science at Dravidian University, Kuppam, AP, and India. He is currently working as Professor in the dept. of Information Science & Engineering, Cambridge Institute of Technology (affiliated to VTU Belagavi), Bangalore, Karnataka State, India. His current areas of research are High Speed Networks, Data Communications, Network Security, Wireless Sensor Networks, Big Data, and Artificial Intelligence. Currently he is guiding 7 PhD Scholars under VTU, Belagavi, KN, and India. He has 46 publications to his credit in various National & International Journals and International Conferences.