International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 4, ISSN No. 2455-2143, Pages 36-40
Published Online August 2019 in IJEAST (http://www.ijeast.com)

BRING YOUR OWN DEVICE (BYOD) PROGRAM

Md Haris Uddin Sharif, Ripon Datta, Siva N Sankarasetty, Hari Garikapati, Mounicasri Valavala, Suchit Maraboyina
University of the Cumberlands,
United States

***Abstract*— The drastic changes in the global technology have also led to the shift of how resources are accessed into organizations. The discovery of cloud computing, the implementation of Bring Your Own Device (BYOD) by most organizations is going to impact the way that and company carries out its IT security. This paper will focus on both the risks and the benefits which are associated with bring your own device (BYOD) a practice which has become so much common in most organizations. Various literature reviews of different established academic journals were conducted to show the key points, arguments as well as the supporting evidence to bring in the conclusions. The paper found out that BYOD is a part of the modern technology is inevitable, and it is applied through the business practices. This adoption is going to increase due to the adequacy in support of the business operations. The research also found out that there are substantial risks in BYOD which can also be harmful for the organization. Thus, the ability to control BYOD is important for curbing and mitigation of the risks. The paper will also contribute to current literature by emphasizing which is in order to fully find out the potential ongoing benefits of BYOD, the control of strategies must also be applied and the human factor must also be taken into account since it plays a major role in the adequacy of the safety efforts.**

Keywords— Access Control, BYOD policy for your business and employees, BYOD technology and risk involved, Benefit of using BYOD.

I. INTRODUCTION

Bring your own device (BYOD) is characterized as the entrance of workers to the corporate data of an organization using their own possessed cell phones. A portion of the keys reason which are considered for receiving BYOD in an association are; adaptability, portability, fulfillment of workers and versatility. Nature where BYOD has been embraced will work in the support of the association since it will likewise help in the decrease of the expense. The BYOD will lessen the cost which an organization will acquire to introduce the IT device and aides in regions where the refreshment of corporate gear makes issues [1].

Regardless of the many thought's BYOD starts different weights that may be hard for the IT security control measures to manage. The information of the association is ordinarily downloaded to the client device and subsequently BYOD will extend parameter of security in the association [2]. The force of security issues will be expanded by reasons, for example, assortment of cell phones being utilized, the disappointment of security in the device that are being utilized and the way that the device that is being utilized can be shared. This has prompted the assessment of the legitimacy of the security reviews that are as of now in presence, control and some other arrangements of data the executives in the association [3].

II. LITERATURE REVIEW

A. Bring Your Own Device is Cost-effective –

Cost decrease and improving profitability addition is the indispensable motivation behind why most organizations sort to Present to Your Own Device (BYOD). Today, most organizations have come about into utilization of BYOD with more prominent level of laborers working with claim devices. In that capacity, the program has turned into an imperative apparatus in overseeing working expenses in many organizations. In many organizations, BYOD program has joined more noteworthy points of interest on territories of cost sparing and improved profitability among others. Coming up next are routes through which BYOD program has encouraged cost decrease in many associations [4].

B. Hardware costs -

The BYOD program has huge benefits when it comes to savings and costs. The program implementation ensures that savings are immediate for the implementing organization [5]. The company is implementing the program no longer needs to purchase or replace employees' devices which generally leads to hardware cost saving. Normally, the devices sell at about
$950 per device and are supposed to be updated with the most advanced technological advancements. The repeat cases of such instances lead to repetitive expenses which are costly in the long run for the company. In this case, the company can avoid these expenses which are a benefit for the company.

C. Telecommunication costs saving -

Most media transmission suppliers are ceaselessly diminishing information utilization costs. Accordingly, they are giving constrained information designs that are financially savvy. Most organizations don't pay for the expense of information in most representatives' contraptions and all things considered, the proprietors of the device foot such charges. The organizations in this way can diminish on the expenses of activity on workers' device. The Aberdeen Group
[13] contends that broadcast communications costs, specifically, can grow with BYOD in light of the fact that

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 4, ISSN No. 2455-2143, Pages 36-40
Published Online August 2019 in IJEAST (http://www.ijeast.com)

organizations lose the customary volume limits they got when they acquired the two gadgets and administration from a solitary supplier. In a report a year ago, Aberdeen said that an organization with 1,000 BYOD gadgets would pay $170,000 more all things considered every year [13].

D. Training and Support Savings-

Preparing and bolster costs in many organizations are generally costly and a weight. BYOD program gives an open door where representatives are utilize their own device wherein they are utilized to and never again need preparing and bolster administrations [6]. Moreover, representatives are allowed the chance to work with device and innovation where they are well familiar with in conveying their obligations. The preparation costs for the particular organizations significantly decline and consequent addition in the efficiency because of the subsequent coordinated effort among representatives.

E. Time Saving-

The program has been vital in facilitating time saving in most organizations. Time spent on training sessions and updates can be used in other activities that are productive for the company. The scenario is further enhanced by the fact that most employees are well versed with the technology and software that are installed in their device. In this case, they are able to use the device effectively and easily saving more time and costs of operation. Moreover, the time that the company uses in updating the devices is spent on other business goals enabling the company to improve on its service delivery, production and other organizational dealings. Employees can adopt BYOD to achieve the benefits of agility for the first time [8].

F. Improved Workers Retention Rate-

BYOD program empowers most workers to have increasingly adaptable time and alternatives while working with their devices. All things considered, this prompts more joyful specialists who with less representative turnover rates. In this manner, representative enlistment systems expenses are impressively brought driving down to supportable human asset offices.

III. RISKS ASSOCIATED WITH BYOD

Despite being the most effective techniques, BYOD is faced with various risks. These risks are as discussed below:

A. The devices could get lost and be stolen -

There are millions of smart phones which are stolen every year. Other gets lost and might end up in bad hands. It has been predicted that 22% of the mobile phones which are produced are going to be lost and 50% of these lost phones will never be recovered [7]. Most of these mobile phones are stolen since they have a high value of hardware on the second hand market. On the contrary, most of the stolen phones have the content in them being accessed by someone else who is not their owners. As a result, this shows how important the security features are which include the password protection, encrypting and also using the robust procedures to wipe the device once it has been lost.

B. Easy physical accessibility-

The many stolen and lost devices mean that the attackers already have physical access with the main device hard ware. This threat is more serious than in stationary hardware such as the work stations and servers where the physical accessibility is not likely to happen. Once the attacker has gained access to the device, it will be hard to secure that device. As a result, the operating system, hardware and apps will affect the total security of the device [9]. The risk is even higher when the employees decide to bring old and insecure devices into the organization. In the cases of BYOD, the risk will be accentuated. If the organizations which refuse to set the required status for personal devices are more likely to b insecure while accessing the data in the organization.

C. Lack of knowledge-

The majority of the clients don't have the learning which ends up being the most noteworthy benefactor of dangers being acknowledged in the association. Upkeep of mindfulness and compelling methods on how the device ought to be taken care of is essential to the security of the information that is being utilized by the device. The danger of this device should be tried among the hazard system evaluation of the organization [10]. Laborers ought to be educated regarding that it is so critical to upgrade security of the device.

D. The responsibility of the end user device ownership-

For this situation there are two situations that happen. In one case the representatives will be relied upon to be with their very own device to work and they should utilize similar device on their own information and applications. In different organizations, the workers will be given the device and use them on their own organizations. In any of the case the representatives will utilize similar device in the workplace. It is highly unlikely that will be halted and the rather it will just develop. The businesses should grasp that propensity and use it to deal with the dangers and welcome the employments. Therefore, the clients will feel they have more feeling of responsibility for device which they use at work. Among the feeling of possession will incorporate the worker approaching the working arrangement of the device and along these lines they could expel the most working arrangement of the security highlights (Souppaya and Scarfone, 2016). The suspicion that all is well and good is going to make the client to be increasingly disposed to the quickly notice that the device is lost. Cloud provides enough tools for secure development, operation and administration of system deployed on its platform [11]. Workers no need to software installation to perform on duties responsibility. Therefore it automatically reduces the employee, worker's responsibility. BYOD is also capable to monitor detected status at reorganization environment, responsible admin user have to be proper authorization to monitor data. Example: Some events occur frequently [12] e.g., in the airport people are meeting, embracing, splitting up, putting objects, getting objects, sleeping on the waiting benches, and etc [12].

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 4, ISSN No. 2455-2143, Pages 36-40
Published Online August 2019 in IJEAST (http://www.ijeast.com)

E. It always has an increase in the access of data-

One of the greatest benefits of the mobile enabled work force is the fact that the employees are always connected unfortunately it also increases the risks. Once the employees have the left their data at the work place it means that they are now travelling with crucial information of the company. In case the device is stolen the business, data will be compromised. In that note, the company should take as its initiative to secure the devices of its employees. The following steps should be considered. First the company is supposed to evaluate the usage of the device scenarios and also carry out an investigation of the leading practices to prevent every risk occurrence. Next, the company is supposed to invest on the mobile device management solutions. This will help in the monitoring of policies and also monitor the usage and the access. Additionally, the company is supposed to enforce the industry standard security policies as a minimum. This will involve the use of pin-code, whole device encryption, remotely wiping among others. The company can also set a baseline of security. This will help in certifying the hardware or the operating system for the use of enterprise with the baseline. Moreover, the company is supposed to know the difference between both the trusted and entrusted devices that might attempt to access the company's network. This means that the company should layer the infrastructure in the right way.

IV. METHODOLOGY

This study applied a quantitative research methodology which used a case study approach. Due to their ability to assist the case studies effectively, both interviews and web-based questionnaires instruments were created and would be used in the collection of data. The surveys were then distributed in a company that agreed to take part in the in the research. I0 participants agreed that they would take part. The face to face interviews were held where 3 of the executive's staff and later, 7 of the other web-based questionnaires were distributed to other general employees. The detailed notes and the interviews which had been recorded were later transcribed. The main reason for using the quantitative method of obtaining data is that it provided an opportunity to discover the thoughts of employees and also their attitude towards bringing their own device at work. The results that were obtained would be crucial in driving the change in infrastructure and the development which is required to manage a bring your own device system in the modern business environment.

V. RESULT

This study examined the effectiveness of bring your own device at the work place. The study results from the interviews showed that majority of the employees agreed that it was the technique was effective and yielded benefits in the organization. Out of the 3 executives interviewed, 2, of them agreed that they had noted benefits related to the BYOD program and it was effective for use in the organization. The employees too agreed that BYOD is effective and have even made most of their work easier. After analyzing their responses, 5 out of the 7 employees who took part in the study were in the support of BYOD program. However, the participants did not fail to notice that, although the decision of the management has encouraged the use of personal devices to carry out task in the work place, it is important to come up with an effective framework to enhance the management and the utilization of BYOD program.

VI. DISCUSSION

From the outcomes above, it was affirmed that BYOD is successful and its application in the organization has broughtpositive results. Among the adequacy which the representatives and the administrators couldn't neglect to notice are that the usage of BYOD has encouraged the client portability. The versatility choices of the clients for the situation have been improved. The individuals who utilized the individual devices for the situation were in a situation to increase individual access to corporate sends just as the use of programming inside the area. Much of the time, it was conceivable to get off the cuff warnings about a gathering and afterward the reactions would be given right away. The representatives likewise let it out was anything but difficult to take care of the inquiries of customers and still work any business related issue while they are still on travel. The representatives additionally noticed that BYOD is advantageous and agreeable for the clients. As indicated by the examination, half of the reacts accompanied their own device at work and they conceded that utilizing the device was helpful and furthermore simple to utilize. The abnormal state of the comfort was because of utilizing a similar stage extra time. Also, the worker's fulfillment and strengthening were improved. From the exploration interviews, recommended that actualizing BYOD in the association began since the representatives got their own device to the work spot and they were cautious on how they utilized these device. This advancement came about to a mental feeling of strengthening to every one of the workers who utilized the individual devices.

Be that as it may, the representatives couldn't neglect to recognize the difficulties related with utilizing BYOD at work. The organization felt unreliable in enabling their representatives to utilize their own device in regulating their obligations. For example, enabling private device to access organization's IT frameworks is a risk itself and ought to be taken care of capably by the administration. BYOD program contributes colossally to the accomplishment of generally associations. In any case, it has genuine difficulties that make it unsafe to use in many associations. In any case, its usage requests expanded security checks and included approaches which make most associations to spend much in verifying it frameworks. They should be constantly checked and observed. In any case, unscrupulous representatives can store organization's passwords and move touchy information which can be unfavorable to the eventual fate of the organization.

Furthermore, it is more hazardous if the private devices are stolen with respect to the organization. The contraptions are typically claimed and conveyed by their proprietors which make it badly designed for most IT chiefs to verify the information in the event that they are stolen or lost. The devices are past most organization's security controls which make BYOD program hard to execute. Then again, the

devices are utilized for other individual exercises which make them progressively inclined to malware assaults. Social destinations and uncertain downloaded applications may contain malware which could thus taint organization's frameworks making it a genuine risk for the organization information.

BYOD program gives most organizations various hardships such security issues, preparing and support among others.

Moreover, in situations where the representative stops or is terminated by the association, it has been hard to recover information from their device. All things considered, the greater parts of them take with them classified documents which are hurtful for the organization. In such manner, associations are constrained uphold consistence strategies which on occasion bother representatives influencing their efficiency. IT supervisors need to do this to shield hierarchical information and agree to the expected guidelines to maintain a strategic distance from punishments which could hurt the survival of the organization.

VII. SUMMARY

The company could use various step to improve the use of BYOD program among the workers since it has proved to be an effective tool to use in the company. These measures include but are not limited to creation of a policy for BYOD which has a business case and its goals should be well stated. With the change of technology and the impact on the way people live and work, the flexible mobile strategy is going to give the companies the chances of exploring innovations as well as empowering their work force and also drive greater productivity. The next measure will be to ensure that the stakeholder's area involved early enough which will be achieved by creation of mobility group. The mobility group will be used in vetting the needs of the business. This group should consist of the executives, legal support among other stakeholders in the organization. For the group to be successful, key success factors should be established as they will assist the group to assess the performance of the implemented policy and how it can be improved.

VIII. ACKNOWLEDGEMENT

Completing this project would not have been possible without the support as well as well as the moral support from various people. I thus take this opportunity to extent my gratitude to them all. To begin with, I thank God for granting me good health and taking through the entire course. I am indebted to my professor for the professional advice throughout the course and for enriching my research for laying a strong theoretical background. Finally, my appreciation goes to my classmates whom we have been working together and encouraging each other and for their positive criticism.

IX. CONCLUSION

From the discussion above, it is evident that BYOD has benefited most organizations positively. The program has leveraged most leading practices in the organization. By practicing a well thought of BYOD policy and adopting the strategies which are both flexible and scalable, the organizations will be much better placed in dealing with any forthcoming policies to their security infrastructure exposed by the devices owned by employees. The invention of the right measures as well as regular testing will assist companies to be smarter and create awareness among its employees of the threats that can be posed to the organization due to the use of personal device.

X. REFERENCE

[1] Blokdyk G. (2018).Bring Your Own Device (Byod) Standard Requirements. Retrieved From URL: https://www.amazon.ae/Bring-Your-Device-Standard-Requirements/dp/0655337911

[2] Hayes B., and Kotwica K. (2013). Bring Your Own Device (BYOD) to Work: Trend Report. London, England: Newnes. E-book ISBN: 9780124116108, Paperback ISBN: 9780124115927.

[3] Creeger D. (2015). Educational Impact of Bring Your Own Device Programs in 1:1 Schools. Dallas Baptist University. Education (Page 123)

[4] Plummer DA (2019). Cost and Benefit Analysis of Bring Your Own Device Programs.Retrieved from Url: https://www.workplaceprivacyreport.com/2019/03/articles/byod/cost-and-benefit-analysis-of-bring-your-own- device-programs/

[5] Keyes J., (2016). Bring Your Own Devices (BYOD) Survival Guide. Boca Raton, FL: CRC Press. Retrieved from url:https://pdfs.semanticscholar.org/57e3/f35b897bface64 7cf667db354bdef86de96e.pdf

[6] Kohne A., Ringleb S., and Yücel C. (2015). Bring your own Device. Retrieved from Url: https://www.springer.com/de/book/9783658037161. doi:10.1007/978-3-658-03717-8_2. ISBN 978-3-658- 03717-8.(Page 7-23).

[7] Kumar L., and Holt C. (2016). Bring Your Own Device or Bring Your Own Distraction. International Journal of School and Cognitive Psychology, 03(01). Retrieved from URL: https://www.longdom.org/open-access/bring-your- own-device-or-bring-your-own-distraction-2469-9837- 1000170.pdf. doi:10.4172/2469-9837.1000170

[8] Loucks J., Medcalf R, Buckalew L, Faria F. (2013). The Financial Impact of BYOD. A Model of BYOD's Benefits to Global Companies. Internet Business Solutions Group (IBSG).Retrieved from URL: http://www.webtorials.com/main/resource/papers/cisco/pa per235/BYOD-Economics_Econ_Analysis.pdf

[9] Souppaya M., and Scarfone, k (2016). Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST Special Publication 800-46. Retrieved from URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIS T.SP.800-46r2.pdf

[10] Souppaya M. P., & Scarfone, K. A. (2016). User's Guide to Telework and Bring Your Own Device

(BYOD) Security. doi:10.6028/nist.sp.800-114r1. Retrieved from URL: http://dx.doi.org/10.6028/NIST.SP.800-114r1

[11] Sharif MHU., Datta R. (2019). Software as a Service has Strong Cloud Security. International Journal of Research in Engineering and Management. Vol.1, No.2, 2019, pp.18–27. Retrieved from Url: https://www.ijrem.in/Downloads/Docs/IJREM%20-%20906%20-%20Revised%20Paper.pdf

[12] Sharif MHU., Saha AK., Arefin KS., and Sharif MH.(2011).Event Detection from Video Streams. International Journal of Computer and Information Technology. ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 01, ISSUE 02, MANUSCRIPT CODE: 110759Retrieved from URL: https://www.researchgate.net/profile/Md_Haidar_Sharif/publication/265290040_Event_Detection_from_Video_Str eams/links/5646d1cd08aef646e6cde39f.pdf

[13] Ackerman E. (2013).Calculating The True Cost of BYOD. Retrieved from URL: https://www.forbes.com/sites/eliseackerman/2013/05/28/c alculating-the-true-cost-of-byod/#20d8d6a51a5c