Towards a Secure Adoption of Bring Your Own Device (BYOD) Policy in Nigerian Corporate Organisations

Oyelakin, A.M.
Computer Science Unit,
Department of Science Education,
Al-Hikmah University, Ilorin, Nigeria.
Email: moyelakin80@gmail.com
Mobile: +2348062738520

Olanrewaju, M. J.
Department of Computer Science
Faculty of Science and Computing Technology,
Allover Central Polytechnic, Ota, Nigeria.
Mobile: +2348028912300

ABSTRACT

Bring Your Own Device (BYOD) strategy allows employees to use their personal mobile devices to carry out official-related activities while using the organisations's corporate networks. It is a technology-based initiative that is found in enterprises that are IT-driven. Despite the many benefits that this technology strategy has in stock, there are attendant security issues that make businesses, educational institutions, organisations and general IT users fearful of its adoption. This paper seeks to identify the level of readiness of an average worker in an IT-driven organisation in Nigeria concerning the adoption of Bring Your Own Device strategy. The paper then further discusses the measures that have to be put in place so as to make its adoption more secured in Nigerian corporate organisations/work places. A sample survey was carried out among selected employees of business enterprises in Nigeria with a view to determining their level of awareness and understanding of the technology program popularly called BYOD. Lastly, frequency counts and percentages were used for representing the data captured.

Keywords: BYOD, Adoption, Organisation Networks, Network Security, Firewall

CISDI Journal Reference Format
Oyelakin, A.M. & Olanrewaju, M.J. (2016): Towards a Secure Adoption of Bring Your Own Device (BYOD) Policy in Nigerian Corporate Organisations. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 3. Pp 1-6.
Available online at www.cisdijournal.net

1. INTRODUCTION

Mobile devices are not only pervasive in Nigeria but also being used for a wide range of official, business, and personal purposes. The use of these smart devices for both personal and business purposes has greatly influenced the way a concept called Bring Your Own Device is being used by corporate organisations, world over. According to Ann Cavoukian (2013), a Bring Your Own Device (BYOD) is a program that involves employees using their own mobile electronic communication devices to carry out work for their employer through remote access to the organisations's intranet. More and more companies in Nigeria and the rest of the world are allowing their employees to use personalized devices such as mobile phones, mobile systems e.t.c to access organisations's networks, perform work-related tasks and so on. Bring Your Own Device (BYOD) policy in work places is no doubt one of the emerging technological programs that aims at building a smatter and better working world. However, the risks and threats that follow its adoption are many. For this reason, there is a continuous need for corporate organisations to implement tighter security controls that will keep intruders at bay while at the same time engage in increased user advocacy concerning BYOD strategy. Neil Anderson (2012) pointed out that BYOD is about end users being able to use the computer and communication devices they choose purposely to increase productivity and mobility. Deloitte (2013) defined BYOD as the use of employee-owned devices to access enterprise content and the enterprise network.

A BYOD policy not only allows employees access to enterprise data when at the workplace but also allows them to access enterprise data outside the enterprise environment. Citrix (2015) clearly pointed out that with BYOD; employee choice has become a cornerstone of mainstream IT strategy. This is because the concept allows people to choose the best devices for their needs thereby making it possible for organisations to improve productivity and flexibility as well as job satisfaction.

2. REVIEW OF RELATED LITERATURE

Sala et al (2014) extensively discusses the BYOD practices that are prevalent among SMES in Tanzania. In the work, a qualitative approach to establish the fact that the level of understanding of BYOD practices for SMEs is still very low among Tanzanians. According to Armando et al (2013), the diffusion of mobile phones, specifically smart phones and tablet personal computers (PCs) is leading to a paradigm shift in many organisations. Citrix(2015) provides useful and technical guide on how Information Technology executives with guidance to develop a complete strategy for BYOD, CYOD and COPE. Ann Canvoukian (2013) pointed out that once an organisation makes the decision to adopt BYOD policy, it is important to consider Privacy by Design principles. It is argued that such an arrangement will enable organizations to manage the risks involved in implementing a BYOD policy more effectively. Also, Ann Cavoukian (2013) provides organisations with information on how they can identify and address the different privacy and security concerns raised by the growing trend towards BYOD in the workplace. In Michael (2013), the study seeks to determine the extent to which BYOD is used in firms listed in Nairobi Stock Exchange.

The work equally listed threats associated with BYOD in Kenya context and measures that have to be put in place to check them. EYGM (2013) opined that in the BYOD policy, Personally-owned devices are made to interface with the corporate devices as well as networks. According to Citrix (2015), BYOD and similar policies such as CYOD and COPE enable organisations to empower people, protect sensitive information, reduce costs, and simply IT management. Neil Anderson (2012) identified policies such as eligibility, allowed devices, service availability, communication on rollout, cost sharing, security support and maintenance form pars of the elements for implementing a BYOD strategy. Olalere et al(2015) conducted an exhaustive review of the literature on BYOD to identify publications and their methodological approaches and to identify topic areas of BYOD research. EYGM (2013) equally categorizes the security landscapes in BYOD into three. These include: securing mobile devices, addressing application risks as well as managing the mobile environment.

Therefore, as a way of protecting an organisation corporate network against threats that may arise from implementation of BYOD program in such organisation, enterprise protection must be in place. Even after when proper security measures have been put in place there is a need for the organization management. Kathleen et al (2016) reported the varying categories of security challenges that are usually encountered while implementing BYOD strategy in an organisation. The paper mentioned deployment challenges, technical challenges, policy/regulation and human aspect challenges as the main ones that confront such establishments while adopting BYOD program.

3. An Overview of Bring Your Own Device (BYOD) Concept

Armando et al (2013) correctly opines that the diffusion of mobile phones, specifically smart phones and tablet personal computers (PCs) is leading to a paradigm shift in many organisations. A successful BYOD initiative should be able to combine simplicity for users (employees) with effective security without actually limiting the productivity of the user. The technology solutions that have been supporting the implementation of BYOD are many and vary. Giant and world-renowned IT organisations like Cisco Corporation, Citrix Systems Incorporated and so on are good examples of IT organisations that have been supporting wider growth and adoption of BYOD in the world. The business trends that are driving BYOD are many and varied depend on the nature of the business. For instance corporate organisations want their employees to achieve maximal productivity and be able to work from remote locations. In a BYOD implementation, the device can be provided or paid for by the employee (user), organisation (employer) or by both.

The ownership of the device used in BYOD policy clearly introduces some fundamental difference as required security policies that will be introduced by the organisation. For instance, if the device is owned by the corporate organisation, it is very likely that there will be a policy in place o guide usage or restricts certain usage. In the case of allowing the user to provide the device for a BYOD implementation, then one may assume that the user may be using the device for both personal and official purposes depending on the usage policy enforced by the organisation. For a BYOD to be very effective, organisations tend to adopt a concept called Mobile Device Management (MDM). Ann (2013) defines MDM as a software based solution for managing mobile devices in the workplace, which area able to establish configuration settings, apply policies, carrying out remote diagnostics, track location info, control the applications as well as providing reports and inventory mgt on the device (Ann (2013). BYOD policy can bring a number of benefits to organisations. These include but not limited to: lower hardware costs, giving employee greater flexibility in terms of their working hours and thereby improve their productivity.

Figure 1: BYOD Pictorial representation (Source:www.shutterstock.com)

4. PURPOSE AND METHODOLOGY OF STUDY

4.1 Purpose of Study

The study aims at evaluating the level of awareness and usage of sampled employees in Nigerian corporate organisations in respect to BYOD strategy. It equally tries to determine the general attitude of employees to the wide-scale adoption of BYOD policy in the country's business circle. Finally, useful guides on how corporate organisations can adopt a more secured Bring Your Own Device program that will incidentally bring about increased productivity, reduction in hardware ownership costs, achieving robust corporate networks and maximized profits.

4.2 Methodology of Research

The research instrument is a questionnaire. The population of the study is randomly sampled employees of forty selected business and corporate organisations in Lagos, Nigeria. The questionnaire was specifically designed to evaluate the level of awareness of the sampled respondents in respect to BYOD concept understanding and readiness as well as general attitude to its wide scale adoption in Nigeria. The questionnaire consists of three sections which captures the demography information of the respondents, their attitude towards BYOD policy and their readiness to continue using varying business enterprises benefits. Frequency counts and percentages were used for depicting the data captured. Suggestions were made on how the adoption of BYOD by organisations by organisations can be more secure and gain confidence of both the employees and employers. Also, the paper provides salient points on how BYOD program can better be adopted by corporate organisations in the country.

4.3 Experimental Design

Purposive sample technique is used to aid in the ease of data collection of the members of the sample size. The respondents are members of staff of organisations that use IT to drive their businesses. Each respondent expresses his/her experience, and awareness concerning the perceived benefits and security risks associated with BYOD program in enterprises. A total of 120 questionnaires were administered among the employees in the said organisations in February, 2016. Out of this, the 118 questionnaires that were returned and properly filled were used for this study.

4.4 Findings

The Tables below presents the data/findings from the research

Table 1: Do you have BYOD in place in your organisation?

Responses	**Frequency**	**Percentage**
Yes	86	72.88
No	26	22.03
Cannot say	8	6.78
Total	118	100

Source: Field Data 2016

Table 2: Level of awareness of BYOD concept in Nigerian organisations

Responses	Frequency	Percentage
Very Aware	62	52.54
Aware	38	32.20
Fairly aware	12	10.17
Unaware	6	5.09
Total	118	100

Source: Field Data 2016

Table 3: Respondents according to business categories

Responses	Frequency	Percentage
Aviation	12	10.17
IT Solutions and Services	65	55.08
Finance	5	4.24
Education	20	16.95
Others	16	13.56
Total	118	100

Source: Field Data 2016

Table 4: BYOD poses serious security issues to corporate organizational networks

Responses	Frequency	Percentage
Very Aware	62	52.54
Aware	40	33.90
Fairly aware	10	8.48
Unaware	06	5.08
Total	118	100

Source: Field Data 2016

Table 5: The benefits of BYOD concept outweighs its security risks

Responses	Frequency	Percentage
Strongly Agree	72	61.02
Agree	20	16.95
Fairly Agree	08	6.78
Disagree	06	5.08
Strongly Disagree	12	10.17
Total	118	100

Source: Field Data 2016

Table 6: Do you have concerns on using your personal devices for BYOD program?

Responses	Frequency	Percentage
Yes	66	55.93
No	49	41.53
Undecided	3	2.54
Total	118	100

Source: Field Data: 2016

Table 7: End user advocacy program should be stepped up so as to make BYOD program successful in organisations

Responses	Frequency	Percentage
Yes	94	79.66
No	11	9.32
Undecided	13	11.02
Total	118	100

Source: Field Data: 2016

Table 8: I support a wide-scale adoption of BYOD concept in businesses

Responses	Frequency	Percentage
Yes	93	78.81
No	14	11.86
Undecided	11	9.32
Total	118	100

Source: Field Data 2016

5. DISCUSSIONS

From the data collected, the following deductions were made:72.88% of the respondents claimed that BYOD is already in place in their organisations because the establishments allow them to use their mobile devices for business-related activities. This indicates that there is growth adoption of BYOD strategy among Nigerian corporate businesses. The level of awareness of BYOD program in corporate organisations in Nigeria is high considering the percentage of respondents that are "Very aware" and "Aware" which are respectively 52.54% and 32.20%. IT solutions and Services sector recorded the highest number of respondents who are currently using BYOD strategy in the country. 62 respondents representing 52.54% claimed that they are aware of security issues that BYOD poses to corporate organisation networks. 72 respondents which represent 61.02% of the sampled population reported that the benefits of BYOD outweigh its security risks. However, 55.93% still expressed concerns for using their personal devices for BYOD Program in their organisations. Out of the total respondents that participated in the survey, 94 representing 79.66% campaign for the need to step up end-user advocacy program so as to make BYOD policy more successful in oragnisations.

6. COMMON ISSUES IN ADOPTING BYOD IN CORPORATE ORGANISATIONS

For an organisation to have a successful BYOD experience the following strategies must be in place: Sustainability, Device Choice, Trust Model, User experience and Privacy, Liability, Application Design and Governance and so on (Mobile Iron). Similarly, it is required that the organisation specifies the choice of device that are allowed and supported on the network while adopting BYOD policy. This, it is believed will help the employee to make the right choice by procuring mobile devices. Consumer or user Device Ownership Phenomenon is a very serious issue that can militate against the implementation of Bring Your Own Device (BYOD) policy in an establishment and must be well handled. For instance, a user may have varying personal information on his personal device that is intended to be used in A BYOD program and this must be carefully handled by the IT department of the oragnisations at the initial stage of implementation. In all, there is a need for adequate security management by oragnisations that adopt BYOD in order to safe guard security management pitfalls which may arise thereafter.

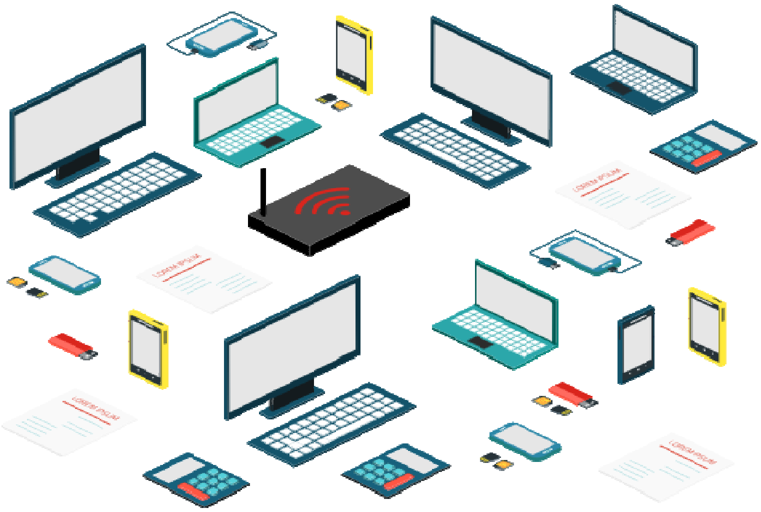

Figure 3: Enterprise Network (Source: http://ethnosit.net)

7. CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

This paper identifies that BYOD adoption is gradually being adopted in many corporate businesses in Nigeria despite the attending security issues. The work then carefully spelt out measures that can be put in place by varying business establishments, institutions and any other corporate work places while implementing BYOD policy on their networks. As reported in varying literature and captured in this paper, with adequate security measures in place, it is believed that the adoption of the technology strategy will reduce cost, bring about flexibility in work places, make their employees more productive and incidentally make businesses to remain competitive.

7.2 Recommendations

Enterprise-wide protection such as: User Layer Security, Access Layer Security(Access Control, Firewalls, Authentication, Virtual Private Security) , Source Code analysis, Vulnerability detection and management, Network Layer Security, User Advocacy and related others should be provided in a BYOD implementation. Furthermore, Ann (2013). recommended that once an organisation makes the decision to adopt BYOD policy, it is important to consider Privacy by Design principles. This will enable oragnisations to manage the risks involved in implementing a BYOD policy more effectively. BYOD programs that bypass outbound filters elevate risk of non-compliance with data privacy laws and regulatory requirements Lisa (2013).

According to RSA Security, the BYOD agreement checklist are as follows:

- Ensure that end users are responsible for backing up personal data;
- Clarify lines of responsibility for device maintenance, support and costs;
- Require employees to remove apps at the request of the organization;
- Disable access to the network if a blacklisted app is installed or if the device has been jail- broken; and specify the consequences for any violations to the policy.

Continuous sensitisation of employees in organisation regarding how to use their mobile devices that participate in BYOD program in safe environment that will not to violate company regulations should be sustained. Finally, all the participants in a BYOD implementation in an organisation should be more concerned about a successful implementation that guarantees device freedom without compromising the Information Technology Networks.

REFERENCES

1. Armando A., Costa G. and erlo A. (2013)."Bring Your Device, Securely," In proceedings of the 28th Annual ACM Symposium on Applied Computing, 1852-1858
2. Ann Canvoukian (2013).Bring Your Own Device. Is your organisation ready? Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-byod.pdf
3. Kathleen Downer, Maumita Bhattacharya (2016).BYOD Security: A New Business Challenge retrieved from *arxiv.org*
4. Citrix Systems Inc Whitepaper (2015). Best Practices to make BYOD, CYOD, and COPE Simple and Secure retrieved from https://www.citrix.com/products/xenmobile/byod-best-practices.html on January 2016
5. Deloitte (2013).Understanding Bring Your Own Device Landscape. Deloitte Research Report
6. EYGM (2013).Bring Your Own Device-Security and Risk Considerations for your Mobile Device Program retrieved from ey.com/GRCinsights on March 12, 2016
7. Eschelbeck G. and Schwartzberg, D. (2012).BYOD Risks and Rewards retrieved from https://www.sophos.com/en-us/medialibrary/.../sophosbyodrisksrewardswpna.pdf on April 4*, 2016*
8. Kathleen Downer, Maumita Bhattacharya (2016).BYOD Security: A New Business Challenge
9. Lisa Phifer (Jan 2013).BYOD security strategies: Balancing BYOD risks and rewards
10. Michael Etale Mbalanya (2013).Bring Your Own Device and Corporate IT Security: Case of Firms Listed on the Nairobi Securities Exchange Limited
11. Mobile Iron (Undated). BYOD Strategies retrieved from https://www.mobileiron.com/en/solutions/byod on March 23*, 2016*
12. Neil Anderson (2012), Cisco Bring Your Own Device
13. Morufu Olalere et al (2015).A Review of Bring Your Own Device on Security Issues available at DOI: 10.1177/2158244015580372
14. RSA Security (2012). Realizing The Mobile Enterprise, Security for Business Innovation Council, retrieved from https://www.rsa.com/content/dam/rsa/PDF/.../h11109-rsa-realizing-mobile-enterprise.pdf
15. Sala Babanda, Irwin Brown (2014). Bring Your-Own-Device (BYOD) Practices in SMEs in Developing Countries-The Case of Tanzania 25th Australasian Conference on Information Systems, Auckland, New Zealand
16. http://ethnosit.net
17. http://www.shutterstock.com