American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-5, pp-237-246
www.ajer.org
Research Paper Open Access

The Impact Of Bring Your Own Device (Byod) On Information Technology (It) Security And Infrastructure In The Nigerian Insurance Sector

Oyo-Ita Emmanuel Ubene[1], Utoda Reuben Agim[2] And Asuquo Umo-Odiong[3]
[1]*Assistant Lecturer Department of Computer Science, Cross River University of Technology Calabar.*
[2]*Graduate Assistant, Department of Computer Science, Cross River University of Technology Calabar.*
[3]*IT Program Analyst, Akwa Ibom State Ministry of Lands & Town Planning*
Corresponding Author: Oyo-Ita Emmanuel Ubene

ABSTRACT: *In a bid to forestall the challenges associated with information and infrastructure protection, IT security strategy development has become a focus around the IT infrastructure of organizations. An investigation into some organizations reveals that information security is a top priority for management. However, an assessment of their IT infrastructure reveals that its capabilities do not totally align with management policies on information security thereby posing security risks with the use of personal smart devices termed "BYODs" by employees. This project focuses on critically assessing the IT infrastructure of an insurance organisation using primary data collected through semi-structured phone interview and questionnaires, analysing how it supports organizational policies on IT security. It also investigates the impact of Bring Your Own Device (BYOD) on IT security and infrastructure, with the aim of introducing suggestions that will adequately maintain IT security and Infrastructure even in the face of an ever improving trend in smart phones and intelligent devices*.

Date of Submission: 27-04-2018 Date of acceptance: 12-05-2018

I INTRODUCTION

The dynamic transformation of office technology has produced an overwhelming impact in the Nigerian Insurance sector; by providing tools for work within and outside the office environment, thereby accelerating business operations and driving the achievement of organisational goals and objectives (Chillingworth, 2012). New innovations have phased out the application of old, preceding technologies: early generations of typewriters had long been replaced with the use of desktop computers; email and advanced fax mail servers have also replaced analogue fax machines.

The use of Desktop computers as workstations within offices is gradually loosing preference. This can be attributed to the development of robust, portable and intelligent mobile devicestargeted towards the consumer market. Employees who own these devices are keen about using them for work both inside and outside the office environment. Most organisations even provide these handheld computers to employees as a way of encouraging productivity and work efficiency. The trend that allows the use of consumer based mobile devices for work within and outside the office environment is called Bring-your-own-device (BYOD).

Bring-your-own-device (BYOD) describes an emerging trend in the workplace where employees and other users of IT network resources prefer to utilise their personal mobile devices for office communication and work. It is a paradigm shift in the way office technology is being deployed (Burt, 2011). This implies a transition from the use of desktop computers within the office environment to the total acceptance of mobile devices including smart phones and wearable gadgets etc. The BYOD trend involves the use of any device (simple or sophisticated), with any ownership (personal or official), at any location (within or outside the office environment) (Neil, 2012). This implies that devices used in a BYOD environment are either owned by the employees or are provided by the employers (Rains, 2012).

However, the use of mobile devices for work within the office environment is not hitch free as it comes with its own concerns. Crook (2011) suggests that creating a BYOD environment for employees within an organisation makes it difficult for IT to maintain an acceptable level of visibility and control over data and resources shared. Hence, BYOD can be seen as a challenge bordering around people, technology and processes. Nevertheless, most organisations embrace BYOD due to the enormous benefits that come along with it. Rains (2012) concur that most organisations have implemented BYOD programs, with some supplying their users with the required access devices.

Given the wide acceptance of BYOD in many organisations, this publicationexamines the implementation of the BYOD program within the Nigerian Insurance Sector using a single case study and analyses the impact on IT infrastructure and security.

II RELATED WORK

The consumerisation of mobile devices tends to be the most significant force underpinning the BYOD regime. According to a survey by Weldon (2012), over fifty percent of mobile phone users in the United States are owners of smart phones. These devices are affordable and the mobility factor enables users work from any location. This has also transformed the corporate application of these devices as most employees can now:

- *Log in to databases and perform real time query operations on same.*
- *Attend real time webinars and video conferencing with the use of high resolution devices, etc.*

This advantage somewhat justifies its wide usage and acceptability. Clay (2012) opines that the BYOD concept gives users preference over time, to bring their own devices into the business functional environment, basically for communication purposes as well as operating business applications. Hence, BYOD is an evolving system which seeks to change office technology from the use of company owned technology alone, to the use of portable, user-owned technology with the hope of empowering users and increasing productivity.This support for BYOD sometimes also trickles down from top management to employees over time thereby leaving sensitive official information and other network resources at the risk of being tampered with by unmanaged and invisible devices (Bestmann, 2012).

Interestingly, the use of devices in a BYOD program can be categorised into three categories which include:

- Use of personal mobile devices for work within the office environment.
- Use of mobile devices provided by the employer for work within the office environment
- Use of mobile devices, either personal or provided for by the employer, for work away from office environment through remote access, etc.

Key Concerns of BYOD

Based on a publication released by Optus Business in 2012, there are some major concerns that need to be addressed when the implementation of a “Bring your own device” program is considered. It is important that these concerns are addressed in synergy with organisational objectives and priorities. Some of the concerns include:

Security:describes the high risk involved with issues that may arise from device theft, device loss, malicious attacks and unauthorised data sharing.

Device Type: Due to the diverse devices that function on varying platforms, careful consideration has to be made on the readiness of the organisation to manage the cross platform compatibility issues that may arise. In other words, infrastructure has to be compatible with device.

Cost: The cost of managing infrastructure that supports all the devices is a concern that has to be tackled. While it may be cheaper to manage infrastructure where devices are provided by the company, it is much more expensive to manage infrastructure in a system where users bring their own wide range of devices.

Privacy: Careful consideration should be made to address issues that may arise from user and employee privacy laws. In as much as employees use their devices for office work, they still have a right to their own privacy as it may likely be breached while making efforts to manage devices.

Critical Success Factors of BYOD

Policy: According to Birkland (2010) policies are made towards a goal or a desired state of an entity. It is a set of guiding principles defined in response to a problem. A balanced definition of a BYOD policy is important as the lack thereof may be regarded as an implicit statement of policy. Hertzberg *et al* (2009) also emphasises on the importance of good company policy and administration as it can influence employee attitude towards work. This implies that defining a BYOD policy will guide employees within a BYOD environment, on how to responsibly make effective and appropriate use of personal technology for work within the office. It also guides both management and employees on what to do and what not to do thereby helping organisations effectively optimise the benefits of technology within the office and also implement penalties. Guerin (2011) asserts the need to constantly update company policies in order to support organisational goals and objectives. It is therefore important to develop a regularly updated BYOD policy document in organisation as trends in mobile device innovations change rapidly.

Infrastructure: in this regard, infrastructure could be referred to as software and hardware facilities which are required for the implementation of a BYOD program to succeed (Bashir *et al* 2011: 1722*)*. These tools may include network connecting devices, server machines and the operating system platforms they run on. Mobile devices including laptops and tablet computers are created by multiple vendors, with varying specification and components. These devices also function in different capacities depending on the specification and are no longer exclusive to any individual class as they are massively targeted towards the consumer market (Enterproid 2012). There is need for a highly compatible infrastructure that can meet the requirements of connecting large devices. Infrastructure is therefore an important factor that can affect the successful implementation of a BYOD program.

User Cooperation: the cooperation of users in a BYOD environment is essential as the program is aimed at empowering them to become more productive and efficient while maintaining mobility. According to Bourne (n.d) BYOD is as user-centric as it is also user driven. When implementing BYOD, proper orientation of users is required in order to maintain an acceptable level of organisational and behavioural culture.

Due to the rapid growth of this trend, there is need for a change in strategy and policies adopted to manage the impending changes, maximise opportunities and minimise the risks involved. According to Gentile (2012), the absence of a strong and comprehensive BYOD policy and strategy, dedicated specifically to mobile device management has put most organisations in a vulnerable position where they are open to threats as well as other malicious activities.

Application of BYOD in Schools

According to Christopher Harris (2011), most organisations including schools are considering “going mobile”. The recent release of both the IPAD and hybrid e-reader devices such as the Nook Tablet and the Kindle fire are giant strides in mobile computing that has raised some concern on the BYOD scheme such as device/network resource compatibility, security and ethical issues.According to Steve Jobs in 2010, mobile devices such as the IPAD are a lean back technology. The idea that it can replace the traditional way of classroom learning is a challenge that school systems will have to handle.

There are obviously key issues to consider for such schools that are planning to adopt BYOD. Schools will have much to prepare for, including the new capability of multiple gadgets and devices that will imminently be gained. This will require an upgrade on infrastructure. Usually, the cost of an upgrade is quite expensive depending on the level of compatibility that is expected to be met with gadgets and devices from a wide range of manufacturers.

However, despite the cost of upgrading infrastructure, implementing BYOD is less expensive and is still seen as the most economical way to adopt hardware (Harris, 2011). The aim is to minimize all potential security risks while enabling improved service delivery within the BYOD environment. This implies that the impact of the BYOD scheme can be far more beneficial to an organisation if the potential security threats are eliminated. This is justified by the fact that the lifting of restrictions on student devices, in as much as it encourages students to adopt more technology, is also suitable for a tight budget system whereby schools do not have to incur much expenditure over computing equipment such as PCs.

Academic institutions that adopt the use of BYOD have recorded improvements for far as students with mobile access to information can carry out actual research and produce authentic content for sharing with both peers and the wider academic community. Most of the institutions in this regard have been high schools and colleges.There is need for a review of school board policies regarding student devices, an evaluation of wireless network to avoid connection problems. There is also need for the tutors to be trained on developing and administering content to students, across this platform.

However, BYOD has in some cases, been regarded as a bad policy in schools. According toGary (2012), the introduction of BYOD scheme into schools will result in limiting the creativity of students, restricting the learning opportunities they are used to, and can as well lead to less support for public education in the future. The fact that students look up the internet for answers to academic questions maintains the stereotyped attitude towards learning and deprives the student of the opportunity to use proper human reasoning which can bring about new answers with a different perspective.

In support of an argument raised by Harris (2011), Gary (2012) analysed that the BYOD scheme in schools does not help enshrine equitable study experience for all stakeholders in the sense that the same quality of materials, facilities and learning opportunities are not available to all and sundry. This loophole creates an atmosphere where academic stakeholders who are unable to afford the cost of procuring highly functional personal devices are taken undue advantage of. This issue is seen as being highly problematic especially in a society with growing economic inconsistency.

One other challenge peculiar to implementing a BYOD program is the varying classes of devices and their physical attributes. The capacity of cell phones and other personal devices that employees bring to work are not exclusively comparable to the capacity of the office based PCs. Despite their similarities in component, smart phones and other gadgets can only do the little much they can in satisfying the user experience in terms of processing speed, graphical interface, etc.

General acceptance of BYOD among administrators is low. Most CIOs tend to avoid the scheme as they are unsure of the implications. IT professionals are tasked with the duty of encouraging strategies that will bring about its acceptance and adopted.

III METHODOLOGY

Solutions provided by vendors have failed to take into consideration, the fact that the dynamics involved within industries differ greatly. Hence, there is a gap between the mobile device management offered by various vendors and the experiences of users in industry. The insurance industry in Nigeria has its challenges and dynamics as to how it works. The political terrain and the nature of business also come with its own complications. Having taken these factors into consideration, it was imperative to collect primary data from the case study.

The objective to examine the organisational policies involved with the use of personal devices (BYOD) in the Nigerian insurance sector using a case study provided information on the unique policies that are obtainable within the sector, if they do exist at all. The resulting information was used to weigh against the practices and demands from both users and managers with the aim of driving the need for a review in policy to meet security demands and user needs while also achieving the originally intended business objective of the organisation.

An assessment of the infrastructure was scheduled to provide answers to significant questions such as:

- What infrastructure does the organisation employ?
- Given the infrastructure within the organisation, does the organisation have the capacity to manage the BYOD requirements?
- If no, what infrastructural developments does the organisation need in order to keep up with the current trends and demands in BYOD?

Quantitative data was obtained using questionnaires as it provided an opportunity to discover employee’s thoughts and attitude towards bringing their own device to work.

Results obtained were to be of great significance in driving the infrastructural change and development needed to manage a BYOD system in a modern day business environment.

IV RESULTS

THE ORGANISATIONAL POLICIES INVOLVED WITH THE USE OF PERSONAL DEVICES (BYOD) IN THE NIGERIAN INSURANCE SECTOR USING A CASE STUDY.

This study examined the existing policies as an important prerequisite guiding the implementation of BYOD in the Nigerian Insurance Sector. In assessing the relevance of organisational policy documents, Pareek (2006: 236) asserted that policy documentation was necessary as they helped promote organisational learning and provide action guidelines for employees of an organisation. Policies and procedures are important in organisations as they have significant influence over the behaviour of employees in any work related activity (Newnam, Watson and Murray, 2004).

Study results showedthat there was no policy documentation prohibiting employees from using personal devices for work within the insurance company. There was also no officially recognised policy guiding the implementation of BYOD within the organisation. However, employees were allowed to bring in their personal devices for work within and outside the office, thereby leaving the responsibility of managing the BYOD environment operated by the organisation, at the discretion of the IT/MIS personnel.

Despite the fact that adequate IT support was provided to all users of network resources with personal devices within the organisation and users were routinely sent corporate emails educating them on BYOD, the absence of a policy document guiding the implementation of BYOD cannot be seen to be in the best interest of the company. This opinion was based on the results obtained from the questionnaire, where twenty five percent (25%) of respondents claimed that they could not use their personal devices at all times and also attributed it to the refusal of an IT personnel to provide support at the time required.

Issues identified in this regard were with organisational behaviour and culture, caused by the absence of a policy document which could have clearly indicated the rights of an employee to be provided with regulated access on their personal device at all times and at the same time influence the behaviour of IT personnel when providing support to users with personal devices. Although management decision has encouraged the use of personal devices for work, an effective policy framework is essential for effective BYOD management and utilisation.

SECURITY ASSESSMENT OF IT INFRASTRUCTURE IN THE NIGERIAN INSURANCE SECTOR USING A CASE STUDY.

This objective was designed to provide answers to the question; how capable is your IT infrastructure in coping with security threats, risks and demands associated with implementing a BYOD environment? An infrastructure quality assurance was initiated in relation to its capability on managing security threats and risks, by using a simple three step methodology proposed by the researcher as follows:

- **STEP1:**Draw up a list of possible threats and discuss their impact on IT infrastructure
- **STEP2:**Identify the infrastructure that could possibly be attacked by them
- **STEP3:**Identify the measures taken by company to mitigate these risks

On completion of these processes, the question to be asked will be; do the measures implemented on infrastructure prevent these threats from achieving their targets?According to Chambers & Associates (2012) IT infrastructure quality assurance is targeted at giving both management and employees confidence that an infrastructure will meet the requirements and demands of a service organisation and at the same time, deliver quality service to all users.

Results further showed that no security quality assurance test had been conducted on the company's IT infrastructure although the infrastructure was recently updated to a high quality standard which met all the security demands of the BYOD program. It was further established that no issues had been reported on the failure of an infrastructure to meet the purpose for which it was implemented.

STEP1: Draw up a list of possible threats and discuss their impact on IT infrastructure

According to Presti (2012) some of the threats to security of data and infrastructure include:

External Hackers: these are hackers without access to the organisation's network infrastructure (Thornton, 2009). They are threats as they resort mainly to targeting external interfaces such as web servers and firewalls (Stewart, 2010: 117).

Device loss: These are risks associated with the loss of devices by employee. These devices may contain confidential information thereby making it a threat.

Data leakage: this has to do with data getting into unwanted hands, by malicious means malicious software like virus and Trojan.

STEP2: Using the methodology suggested above, the researcher was able to identify the infrastructure within the Case that could be targeted by these threats identified. They include:

- Databases and Storage Infrastructure:
- Application software packages

STEP3: RISK MITIGATION METHODS

According to Swiderski and Snyder (2004), the STRIDE model for threats implies that threats are targeted at one of five things which include: spoofing, tampering, repudiation, information disclosure and denial of service. As an organisation, it is necessary for the IT/MIS department to create measures which help minimise the risks posed by security threats.

Research data shows that the Casestudy under investigation implements:

- IT security policies like access control which restricts unauthorised entry: This kind of security infrastructure is capable of managing threats from External hackers
- Hardware and software firewalls, antivirus: this is capable of managing the threats from malicious software. Windows defender is also another tool they employ.

Based on this analysis, it was inferred that the infrastructure has been developed with security features which can restrict threats.

THE USE OF BYOD AND ITS EFFECTS IN THE NIGERIAN INSURANCE SECTOR USING A CASE STUDY.

This study objective discusses how BYOD is used within the Nigerian Insurance sector using a case study. It examined the different purposes in which employees engaged personal devices. Furthermore, it analysed the benefits, advantages and disadvantages of using these devices within the organisation and remotely from different a location.

According to a report by Cisco (2012), fifty-six percent (56%) of employees within the UK public sector acknowledged that the key benefit of BYOD was that it improved employee satisfaction on the job. The satisfaction derived contributed to its wide acceptance as Seventy-three percent (73%) percent of organisations in the UK public sector domain have implemented BYOD. The perception of employees within the case study, as gathered via questionnaires and interview result was that IT/MIS was responsible for providing support to all users, giving little consideration to compatibility issues which may arise from products developed by multiple vendors. It was therefore inferred that the use of personal devices in organisations for work has increased due to the intense pressure exerted by employees who are keen about using these devices.

The research further gathered that all employees were allowed the liberty to carry out office related work using their personal devices. The adoption of BYOD is also very flexible as there is no official policy guiding its implementation. However, there is a set of loose guidelines provided by IT/MIS as they are responsible for providing support services to employees that bring in their personal devices. Some of the support provided at the service desk included configuration of devices, connection to network infrastructure resources, user orientation of safety precautions, etc.

Advantages of BYOD identified within the Case Study.

- **It Facilitated User Mobility:** the implementation of BYOD has facilitatedmobility options for users within the Case. Personal device users were able to gain access to corporate mails and software applications from any location. In most cases, impromptu notifications of meetings were received and prompt responses were made. Furthermore, insurance Brokers and customer relationship managers were able to attend to customer queries and solve work related problems while in transit.

- **It was more comfortable and convenient for users**: Research findings showed that fifty percent (50%) of respondents that brought their personal device to work were of the opinion that using their devices was more convenient and easy to use. The high level of convenience is as a result of the continuous use of the same platform over time.

- **It Made work process more flexible**: With the implementation of BYOD in the case study, employees were able to take work home and still gain access to data and information from any location. Marketers and financial advisors can meet work targets from an outdoor field of service.
- **It Improved Employee empowerment and Satisfaction:** the research interview suggested that the implementation of BYOD commenced because employees brought in their personal devices to work and were keen on using them for work. This development generates a psychological sense of empowerment to employees.

- **BYOD as a driving force for Infrastructural Upgrade and Cross platform Compatibility in Insurance**

Findings from this study showed that users within Royal Exchange Assurance Nigeria Plc. owned personal devices from different vendors. Some of the vendors identified included, blackberry (smart phones), apple (tablet computers and smart phones) and Microsoft windows-based laptops. Infrastructural requirements and demands arising from users bringing in their personal devices for work exerted pressure on management to conduct an upgrade on infrastructure. This development (upgrade) in company IT infrastructure can therefore be directly attributed to the implementation of a BYOD program within the case study.

Disadvantages of BYOD identified within the Case Study

- **Cost of Connection:** The cost of remote connection to the company's infrastructure is high and expensive for users. According to the Chief Information Officer of the Case Study, a high speed internet connection was required for users to connect remotely to the company's network infrastructure. It was also identified that the organisation only supports senior management executives by providing with home internet services and mobile access devices. However, the questionnaire results showed that seventy-five percent (75%) of non-management employees that worked remotely used internet supplied by their personal service providers while the remaining twenty-five percent (25%) used any available Wi-Fi service. Both groups were personally responsible for the bills associated with internet supply.

Having established these facts, the high cost of high-speed internet connection is quite challenging for employees. Eleanya (2008) asserts that while it costs about $20 a month for internet access in North America, it cost approximately $100 to get the same service in Africa. This difference in cost makes the use of personal devices outside the office environment very expensive.

- **Problems associated with Device Theft:** Issues associated with device theft can be overwhelming on an organisation. During the research interview, an incidence where an employee lost a laptop computer was reported. This exposed sensitive company data to possible fraudulent activities as these data was stored on the local hard drive of the laptop. It was further reported that the occurrence of this incidence led the company to implement a partially virtualised environment as a measure to manage the reoccurrence of such situation.However, even though users cannot save transactional data to the hard drive, data from word processing and statistical packages can still be saved. This is a gap that could still lead to the leakage of data, hence a major disadvantage of implementing BYOD in this organisation.

How does the implementation of BYOD help Organisations in the Nigerian Insurance Sector gain Competitive Advantage?

Study results show that the implementation of BYOD in Insurance has encouraged the development of IT infrastructure which is necessary to cope with the demands associated with its successful implementation. Within the case study, major benefits gained from its implementation have only been associated with the effects it has had on quality of service delivered, employee mobility options and speed at which work is done, etc. Return onInvestment (ROI) derived from the implementation of BYOD can be deduced from measuring the cost of setting up infrastructure against the yearly increase in company revenue.

- **Enhances productivity of Employees:** According to the Research findings, fifty percent (50%) of employees that bring their personal devices to the office for work suggested that using their own device makes them more productive. The interview results further confirmed that most employees who lacked access to company provided desktop computers could still perform their work obligations and meet targets using their personal laptops or mobile phones. For instance, insurance policy marketers used their mobile devices to send relevant information to target clients in a timely manner. This helped build trust and reliability and also became a factor that encouraged prospective clients to buy policy cover and do more business with the organisation.
- **Increases efficiency in service delivery:** Research findings also proved that employees were able to respond to corporate mails and policy holder's request in a timelier manner as they had handheld devices which were configured and given access to mail services as well as other applications. Customer requests sent via emails and web portals were easily managed and responded to even at moments when employees were not on desk.

In summary, the implementation of BYOD in the Nigerian Insurance Sector as understudied in the case study, has been effective as it has improved Customer support, service reliability, and has also lead to the upgrade and development of IT infrastructure. Employees are willing and are also encouraged by top management to work with their personal devices. However, they still have their concern over the monetary cost involved in using their devices from remote locations.

Theimpact of the use of BYODs on IT infrastructure and security in the Nigerian Insurance sector using a case study.

The effect of IT infrastructure in an organisation cannot be underestimated as ICT is regarded as the hub of every organisation and its infrastructure can shape the strategy and approach adopted in the operation of the organisation (Katz, 2002).

According to Sääksjärvi (2004), every IT infrastructure has an important but implicitly defined role in contributing to the effectiveness and performance of an information system. In discussing the effects of the BYOD program on IT Infrastructure within and Insurance Company, the following characteristics were used as a metric for assessment:

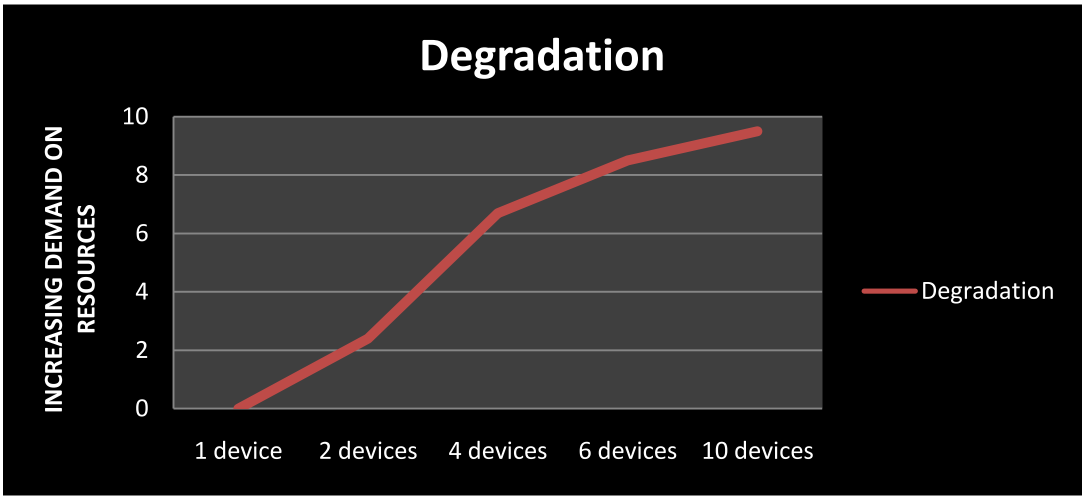
V SCALABILITY:

Scalability deals with the throughput and optimal performance level of an infrastructure when exposed to additional influx of personal devices in a BYOD environment. The influx of devices into the work place could cause high traffic that can affect throughput of the network infrastructure. Based on results from the questionnaire, it was gathered that respondents usually brought their personal devices to the office for work. It was also gathered that some respondents also work from remote locations even during office hours. Assuming seventy five percent of (75%) respondents each brought their device to the office and another twenty-five percent (25%) works from a remote location, it can be expected that the increase in traffic caused by a heavy inflow of personal devices will cease resources like network bandwidth by consistently requesting resources and pulling down packets and processing space.

For instance, Tablet devices usually consume data at a high rate, in addition to the fact that users of network resources within the case study have a culture of streaming data from high density websites. Furthermore, some of these devices automatically pull data from the internet whenever internet service is detected. Such data could be automatic updates of software applications, etc.

The immediate effect of this scenario is that it affects the throughput of a network infrastructure. This can also cause network service disruption and congestion thereby rendering applications that are powered by the network infrastructure stranded as response time to processes reduces.

With an impending growth in business activities over time, these effects on the network infrastructure caused by traffic heavy traffic can eventually cause performance degradation of software infrastructure (the operating system platform which the network infrastructure runs on)



Graph showing the rate at which infrastructure degrades over time with increase in the influx of devices

Reliability

Reliability deals mainly with the ability of an infrastructure to consistently meet service demands even at peak periods or the occurrence of faults with components (Ottawa, 2012). The implementation of the BYOD in Insurance could affect the reliability of a system as the degradation in performance of software and hardware infrastructure does not only affect the infrastructure's ability to cope with growth and increase in number of devices but also affects the ability of a system to consistently achieve optimal performance at peak periods. The lack of a clear policy on BYOD implies that user activities on the company's infrastructure is not properly monitored hence, the influx of devices into the company's infrastructure also causes complications to the availability of infrastructure over time. For instance, before the upgrade of the current infrastructure, the old RAID configured HP servers used within the company had been through rigorous technical stress. There were occasions where server machine failure occurred which in turn affected applications that were hosted by it e.g. the Insurance business application. Therefore, it can be deduced that the implementation of a BYOD program can affect infrastructure reliability if not properly managed.

VI CONCLUSION

The implementation of BYOD is highly user-centric. This study has established a widespread acceptance of the BYOD trend by both employees and management of a case study within the Nigerian Insurance Sector. Its successful implementation creates significant benefits in terms of increased productivity and efficiency; and also puts enormous demands on IT infrastructure and security, scalability, reliability and can cause performance degradation overtime. Consequently, quality of service and work processes delivered and powered with the aid of such infrastructure also suffered a setback.

Research has also shown that employees/users of ICT resources are particularly concerned with their privacy and security of their personal data. However, employers and management on the other hand are concerned with the security of company data and ensuring the efficiency of their infrastructure resources. As such, a partial or poor implementation of policies can create lapses which indirectly expose sensitive data and resources to potential malicious engagements.

The benefits are also significant in terms of productivity and employee efficiency. However, in an insurance company where sensitive financial transactions occur and services provided are highly customer oriented, how can the BYOD program be implemented in such a way that the benefits are positively exploited without having an adverse impact on the infrastructural investments and security of the company?

Suggested Framework for developing BYOD policy in the Nigerian Insurance Sector.

Wallace and Webber (2006) affirm that a policy making process involves policy creation at the initial stages, followed by acceptance, then the review, and update processes. Policy development process should be officially done to enable participation by all stakeholders adopting the following methodology:

- Making a Policy suggestions
- Policy manager works with management to establish relevance and acceptance. Any rejections of suggested policy is sent back for review.
- A level of priority is assigned to the accepted policy
- The requirements of the newly suggested policy is investigated e.g case studies
- A draft policy is created

- The draft is reviewed by management
- Necessary revisions are made to adjusted draft
- New policy is sent back to management for approval
- New approved policy is sent to stakeholders
- This new policy is updated on the master policy manual

Gaining Effective control over infrastructure through Mobile device management software

In managing the challenges associated with the impact of using personal devices at work, the use of mobile device management software would suffice. Mallick (2003: 392) asserts that mobile devices are easy to manage when their use is explicitly defined within an organisation. Johnson (2011) affirms that Mobile device Management (MDM) can be implemented within organisations by using software that secures, manages, monitors and supports the deployment of mobile devices in an organisation. The implementation of this software can also help manage the issues created by an influx of personal devices and prevent the long term impact on infrastructure.

Explaining how MDMs work: when a user device comes into an office environment, it communicates with the network infrastructure, requesting for access. The mobile device manager checks for a unique identity in order to verify and authenticate the device. If authenticated, access is granted. However, granting a device access to the IT infrastructure and resources does not totally summarise the functionality of MDMs as the software further manages the activity of each user depending on the user profile. Restrictive measures and control are being issued to guide users on what to do and what not to do. In other words, it also compliments the BYOD policy by implementing control over a mobile device user's activity.

However, cost of ownership and licensing of are limitations which deter the use of MDMs. Nevertheless, assessing the option of upgrading infrastructure and comparing it with the cost of ownership for MDMs, the difference is vast. Coupled with the understanding of the benefits of BYOD to the organisation, and the expectation of users from both management and IT personnel, financial resources should be dedicated to the successful implementation of BYOD.

Furthermore, the use of open source MDMs can also serve as a way of avoiding initial cost of purchase. Unfortunately, there are few options on open source product varieties as most developing communities have not released software. Examples of the few Open source MDMs include OpenMeap and OMA.

Additionally, an in-house development team within the insurance company could take up the task of tailoring applications to suit their needs. Given the total acceptance of the BYOD program within this organisation, the possibility of developing a software package to serve the need of the organisation cannot be ruled out.

Virtualisation as a tool for Remote connections

Based on the research findings, the case investigated can implement a fully virtualised environment to eliminate the security concerns. A fully virtualised platform helps employees use their personal devices for work remotely, gain access and continue with their work sessions by logging on with their user profiles. With this implementation, the limitations of the current system, where different profiles are used for LAN and WAN connections, will be eliminated as users will require only a single profile name and password to gain access.

Furthermore, risks associated with data theft will be minimised. Research findings showed that transactional data cannot be saved to local storage of employee's personal device. However, the same was not reported about non-transactional data which could also be confidential. Nevertheless, with virtualisation, users that are granted access to the company's domain from their personal devices have the option of using the virtualised data storage which synchronises with the company's database. This therefore eliminates the possibility of storing non-transactional data on the local drive and exposing it to further risk.

Research findings also showed that there was high confidence on the ability of the infrastructure to monitor and terminate malicious attacks from applications as employees were not restricted on the applications they could use on their devices. With a fully virtualised environment, security concern can be minimised as the functionality of these applications are turned off on the virtual networks.

Cost and Support for Employees

Based on research findings, employees would appreciate financial support from their employers on the cost of getting internet access which is a major requirement for working at home. In the researcher's opinion, provision of support from the company should not be focused on management executives only. Considerations for provision of alternate internet connections at locations outside the office environment should be made based on the job description of employees.

However, research findings have shown that the implementation of BYOD can cost management significantly on infrastructural upgrades. It would therefore be financially inconsiderate to put cost of access devices on company funds. Nevertheless, it is suggested that support should be restricted to provision of Internet services. For instance, a marketer who needs to contact target clients could be supported with services that will enable mails and messaging, etc. An employee from the investment unit could also be provided with services that would help him monitor stock market indices and make bids and deals online, etc.

User Orientation

Users of IT resources and infrastructure within the Nigerian Insurance sector have a significant role in the successful implementation of a BYOD program. The activities they indulge in could either support IT infrastructure or put pressure on it. It is therefore pertinent to organise BYOD orientation seminars and lectures to educate employees on their role in organisational success and BYOD.

REFERENCES

[1]. Bashir et al (2011) ‘Information and Communication Technology Development in Malaysia: Influence of Competency of Leaders, Location, Infrastructures and Quality of Services on Telecentre Success in Rural Communities of Malaysia’ Australian Journal of Basic and Applied Sciences [Online]5(9): 1718-1728 Available from <http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=9f02e253-bbe3-4ec3-a064-26b35992b264%40sessionmgr104&vid=8&hid=15> [23 December 2012]

[2]. Birkland, T. (2010) An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making. 3rd edn Armonk: Sharpe

[3]. Bourne, V. (n.d.) BYOD: Putting Users First Produces Biggest Gains, Fewest Setbacks [Online] Available from <http://www.quest.com/documents/byod-putting-users-first-produces-biggest-gains-fewest-setbacks-datasheet-19142.pdf> [30 August 2012]

[4]. Chillingworth, M. (2012) British sport has transformed, technology will lead business transformation [online] Available from <http://www.cio.co.uk/opinion/chillingworth/2012/11/05/british-sport-has-transformed-technology-will-lead-business-transformation/> [22 December 2012]

[5]. Clare, D. (2012) What is BYOD? - An Introduction to Zycko'sSolutions [online] available from <http://www.youtube.com/watch?v=ENXAu3wnr08> [28 June 2012]

[6]. Crook, S. (2011) Embracing Consumerisation with Confidence [online] Available from < http://www.trendmicro.co.uk/media/wp/embracing-consumerization-with-confidence-idc-analyst-whitepaper-en.pdf> [11 January 2013]

[7]. Eleanya, C. (2008) the 4-1-9 Coalition, the Internet, and Nigerian Business Integration in the in the United States Michigan: proquest.

[8]. Gentile, M. (2012) Supporting BYOD with Strong Mobile Device Management Policies [online] available from <http://esj.com/articles/2012/01/30/supporting-byod.aspx> [25 September 2012]

[9]. Guerin, L. (2011) Smart Policies for Workplace Technologies: Email, Blogs, Cell Phones & More. 2edn. Berkeley: NOLO

[10]. Herzberg et al (2009) The Motivation to Work 12edn. NY: Wiley.

[11]. Johnson, M. (2011) Mobile device management: what you need to know for its Operations management.Dayboro/AU: Emereo.

[12]. Katz, R. (2002) The ICT infrastructure: A driver of change [Online] Available from http://net.educause.edu/ir/library/pdf/ERM0243.pdf [4 January 2013]

[13]. Mallick, M. (2003) Mobile and Wireless Design Essentials US: Wiley

[14]. Ottawa (2012) Reliability of infrastructure. [Online] Available from <http://ottawa.ca/en/city-hall/planning-and-development/official-and-master-plans/infrastructure-master-plan/section-4/42> [10 November 2012]

[15]. Pareek, U. (2006) Organisational Culture and Climate Hyderabad: ICFAU University press

[16]. Presti, K. (2012) 7 Security Threats Circling Your Network ‘CRN’ [Online] Available from <http://www.crn.com/slide-shows/security/240002785/7-security-threats-circling-your-network.htm?pgno=10> [10 January 2012]

[17]. Rains, J. (2012) “Bring Your Own Device (BYOD): Hot or Not?” HDI Research Corner [Online] Available from <https://news.citrixonline.com/wp-content/uploads/2012/04/BYOD-Hot-or-Not.pdf> [22 December 2012]

[18]. Sääksjärvi, M. (2004) The Roles of Corporate IT Infrastructure and Their Impact on IS Effectiveness [Online] Available from <http://www.csrc.lse.ac.uk/asp/aspecis/20000086.pdf> [10 september 2012]

[19]. Stewart, M. (2010) Network Security, Firewalls, and VPNS Sudbury: Jones and Barlettinc

[20]. Thornton, G. (2009) Unauthorised access (hacking). I have a problem with unauthorised access; what should I do?[Online] Available from < http://www.grantthornton.ie/db/Attachments/Publications/Forensic_&_inve/Grant%20Thornton-Unauthorised%20access.pdf> [20 December 2012]

[21]. Wallace, M., Webber, L. (2006) IT Policies and Procedures: Tools & Techniques that work

[22]. Weldon, K. (2012) Bring Your Own Device: How to Protect Business Information and Empower Your Employees at the Same Time [online] available from <https://www.wireless.att.com/businesscenter/en_US/pdf/current-analysis-byod-trends1.pdf>[29 July 2012]

Oyo-Ita Emmanuel Ubene. " The Impact Of Bring Your Own Device (Byod) On Information Technology (It) Security And Infrastructure In The Nigerian Insurance Sector”American Journal of Engineering Research (AJER), vol. 7, no. 5, 2018, pp.237-246.