Policy Framework for Adoption of Bring Your Own Device (BYOD) by Institutions of Learning in Nigeria

Oluranti Jonathan, Sanjay Misra, Nichols Omoregbe
Covenant University
Nigeria
jonathan.oluranti@covenantuniversity.edu.ng
sanjay.misra@covenantuniversity.edu.ng

***ABSTRACT*:** *Mobile computing makes access to data and services available anytime and anywhere. The recent increase in the number of mobile devices like smartphones and tablets has given rise to a phenomenon known as "IT Consumerization" that focuses on satisfying the needs of the consumers to improve their productivity for the benefit of their organization. Recent report from mobile trends indicates that in 2014 alone, manufacturers will ship more than a billion Android devices. It is estimated that seven out of every ten employees (7/10) will use their mobile devices for work in corporate environments. Mobile devices according to studies are known to be more vulnerable compared to laptops and PCs due to their small size, mobility and general lack of protection against viruses and malware. The use of these devices therefore can impact negatively on corporate networks unless properly and effectively managed. Organizations are now adopting a program known as 'bring your own device' (BYOD) that will enable them capture, register, and manage the mobile devices that connect and use their corporate infrastructure to guarantee the security of the infrastructure and data of the organization. They achieve this by putting in place strategies and policies that involves all stakeholders. This paper surveys literature to extract useful information that serve to enlighten the community of workers and IT leaders on the current and rapid growing phenomenon of BYOD, including the strategies for deployment, BYOD models, benefits, security threats on corporate and user data and infrastructure. The study presents guidelines and a framework for adoption of BYOD by institutions of higher learning in Nigeria in order to improve learning and provide a better workplace. The study will enable IT leaders formulate policies and guidelines that will guarantee smooth adoption and usage of BYOD by their various organizations.*

Keywords: Bring Your Own Device (BYOD), Mobile Devices, Threats, Risks, Vulnerability, Mobile Device Management (MDM), Data Leakage, Usability, Mobility, IT Consumerization

Received: 28 September 2015, Revised 3 November 2015, Accepted 10 November 2015

1. Introduction

In the past few years, the market for mobile devices like smart phones and tablets has continued to grow astronomically all over the world leaving many organizations contending with how to exploit these consumer-oriented devices in business and organizational operations while mitigating the security risks that can result from their use. For instance, according to TELSUS, communication service provider in Canada, over 27 million people use mobile devices including smartphones and tablets, to communicate, study, work and shop. This has placed Canada as the third highest level of smartphone penetration in the world.

Many corporate entities are now accepting on their networks personally owned mobile devices such as smartphones, iPad, iPhones among others [1]. This is now leading to a development termed “consumerization of IT” in organizations, where users prefer to use their personally owned devices than those provided by their organization[2]. A report by Trend Micro in 2011, stated some reasons users choose to use their personal devices in workplace. Some of the reasons stated were easier to use, more convenient, and allow them to mix their personal and work-related information [3]. The history of IT Consumerization datres back to 2007 when Apple unveiled her first iPhone as the first smartphone with multi-touch interface [4]. There have been several transformations in the smart phone industry since then. For instance, we have witnessed the introduction of Google’s Android operating system, Hewlett Packard’s acquisition of Palm, and Nokia’s partnership with Microsoft to run Windows Phone 7 on new Nokia smart phone hardware [4]. Consumer demand for these devices has also been on the increase since the innovative introduction of Apple’s first iPhone [4]. [5] reported in 2012 that global smartphone sales hit 472 million units in 2011 and are estimated to reach 1.1 billion units by 2015.

Many organizations in most developed world require their employees to more productive and therefore put in place an all-inclusive by mobile strategy that makes it possible for personally owned mobile devices to be used safely in work environment as this has proved to increase employee productivity while reducing operating costs for the organization. It has also been found that applicants for jobs prefer the work environment where employees are allowed to use their devices. Bring your own device (BYOD) is an employee IT ownership model that presents an attractive option to organizations. BYODs are extensions of corporate networks and thus it is essential to secure them in order to protect enterprise networks. The existing security tools such as firewalls, anti-virus software, and anti-spam software do not cater enough for BYOD as it does for normal networks. This is because the coverage of BYOD goes beyond the locality of the organization where physical monitoring may not be available. A number of organizations are now grappling with security concerns as a result of personally owned devices being used on their infrastructure. They have to put in place acceptable procedures that will strike a balance between employees’ needs and the security concerns.

1.1 Level of Internet and Mobile Penetration in Nigeria

According to the Internet World Stats report 2012, about 48 million Nigerians now use internet. This according to the report translates to internet penetration rate of 28.4%. Nigeria is said to be the leader in terms of internet connectivity in Africa and 11th in the world. The number of internet subscribers in Nigeria is about the size of the entire population of Tanzania. Report from Terragon Insights in 2013, said between December 2011 and June 2012, a total of about 3.3 million new internet users were added in Nigeria. The report also shows that the average internet time spent by Nigerians is close to 3 hours. From the report also we gathered that most internet users are youth of age between 19 and 35 years with students representing 45%. A comparison of mobile and desktop internet users was also carried out. It shows there are about 61% of mobile internet users in Nigeria.

With respect to mobile penetration, NCC report of 2012 states that Nigeria mobile penetration stands at 69.01%. Also based on data obtained from NCC, mobile subscribers grew by 18% between 2011 and 2012. TNS also reports that 25% of mobile subscribers use smartphones, 59% use basic feature phones while 16% use advance feature phones. According to [6], there are in all about 110 million mobile phones in Nigeria. A survey by NBS indicates that 84% of urban dwellers have access to mobile phones while only about 59% of rural dwellers have access to mobile phones. Also 60% of mobile internet hits come from feature phone (Gs.statcounter.com).

1.2 Statement of Problem

BYOD is entirely a new concept in Nigeria as a number of organizations and institutions are already practicing without knowing or without formal policy and statement adopting the program. The first obstacle to over in the case of Nigeria is that of creating awareness of the BYOD program to the generality of Nigeria institutions. Most organizations in Nigeria allow employees and other third parties to connect to the infrastructure as they appear to be ignorant the consequences of doing that without a proper management policy and program in place. The educational institutions in Nigeria fall under this category of those that practice BYOD without knowing or without proper policy in place for it. The use of personally owned devices to carry out corporate work poses a number of concerns which include data access and security, device visibility among others. These challenges can be overcome with proper BYOD policy in place. This paper therefore reviews literature that examines general knowledge of personal mobile devices, their levels of threats and vulnerabilities as well as their impact on corporate information security. The paper also reviews literature that concerns the phenomenon called BYOD that is, the use of personally owned mobile devices to communicate study, learn and do business in corporate workplace. The paper also proposes a policy framework for the adoption of BYOD in institutions of higher learning.

2. Review of Related Literature

This section gives an overview of mobile devices, such as smart phones and tablets including their unique features. This section also presents high-level recommendations for mitigating the risks that these mobile devices currently face.

2.1 Mobile Devices and their Characteristics

Mobile device features are constantly changing, so it is difficult to define the term “mobile device”. However, as features change, so do threats and security concerns, so it is important to establish a baseline of mobile device features [7]. According to [7], a mobile device is a device that is small in size and possesses at least one wireless network interface for internet access. A mobile device also has a local built-in (non-removable) data storage, an operating system that is not like full-fledged desktop or laptop operating system. It also consists of applications which can be obtained through multiple methods like operating system, web browser or acquired and installed from third parties. A mobile device also possesses built-in features for synchronizing local data with a remote location. A mobile device may also include interfaces like Bluetooth, voice communication channels, GPS, cameras, microphone, among others.

2.2 Mobile Devices Vulnerabilities and Threats Modeling

Mobile devices typically need to support multiple security objectives. These can be accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure [7]. The most common security objectives for mobile devices include Confidentiality, Integrity, and Availability. According to [7], to achieve these objectives, mobile devices should be secured against a variety of threats. Some of the general recommendations by [7] are presented in this paper.

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (e.g. desktop and laptop devices only used within the organization’s facilities and on the organization’s networks). It is important to evolve a system threat model for mobile devices before designing and deploying mobile device solutions. It is through threat modeling that we identify resources of interest and possible threats, vulnerabilities and security concerns related to the resources. We then determine the possibility of successful attacks and their impacts after which we analyze the information to security controls need to be improved or added. Threat modeling is very important as it enables organizations to identify security requirements and design the mobile device solution to incorporate the controls needed to meet the security requireme nts. [7] presented a number of security concerns along with strategies to minimize or eliminate them. The major concerns are presented below.

i) Lack of Physical Security Controls

Mobile devices are used within and outside the organization’s control. They are easily lost or stolen therefore compromising their data. To mitigate this concern it is necessary to protect sensitive data for example by encrypting the mobile device’s storage so that sensitive data cannot be recovered from it by unauthorized parties, or by not storing sensitive data on mobile devices. The second method may be by enforcing authentication before gaining access to the mobile device or the organization’s resources accessible through the device.

ii) Use of Untrusted Mobile Devices

Many mobile devices lack trust features like those found in laptops and other hosts. There is also the issuing of jail-breaking by bypassing security and operating system-based restrictions on the mobile devices. To mitigate these concerns allow only organization-issued devices to be used on the corporate network. Another method is to secure each organization-issued device before allowing it to be used. It is also necessary to run organization’s software in a secure and isolated sandbox on the device.

iii) Use of Untrusted Networks

Organizations do not have control over other networks used by mobile devices for internet access. The communication systems have tendency for eavesdropping and posing Man-in-the-Middle attacks. To mitigate these concerns it is necessary to use strong encryption technologies to protect the confidentiality and integrity of communications. Another way is to use mutual authentication mechanisms to verify identities of both endpoints before transmitting data.

iv) Use of apps created by Unknown Parties

Unknown third-party mobile applications downloadable by users may not be trustworthy. To mitigate this concern it is necessary to prohibit all installations of third party applications or implement whitelist to prohibit only unapproved applications or implement secure sandbox that separates organization's data and applications from data and applications on mobile device.

Other threats posed by the use of mobile devices include their interactions with other systems, use of untrusted contents and use of location services by the device. All of these have their mitigation strategies as well.

2.3 Impact of Mobile Devices on Corporate Information Security

In 2012, Check Point Software Technologies sponsored a research based on a global survey of 790 IT professionals conducted in the United States, Canada, United Kingdom, Germany, and Japan. The goal of the survey was to gather data to quantify the impact of mobile devices on corporate information security.

The survey was reported in June 2013 and revealed the following:

i) There is extensive use of mobile devices on corporate networks much of which are personal devices and used to carry out work in the corporate environment
ii) Customer information on mobile devices causes security concerns
iii) Mobile security incidences are expensive of which a majority of companies have experienced in last one year
iv) In terms of level of risk to corporate networks, the report revealed that Android is by far the most frequent platform indicated (49%), followed by Apple/iOS (25%) and Windows Mobile (17%).

2.4 The BYOD Phenomenon

BYOD is a rising phenomenon in which employee-owned technologies are used in work environment. BYOD is a subdivision of an expanded idea called "IT consumerization", a phenomenon in which employees use their personal devices and software for both official and personal work within the perimeter of an organization [8]. Some authors are of the opinion that BYOD represents a change from generally accepted perspective of the use and management of terminal devices in the work environment [9]. [10] defined an employee's personal device as "one that has not been configured and locked down by the organizational IT department" and therefore vulnerable. According to [11], corporate bodies are now shifting from a "managed world to an unmanaged or borderless world" where the security perimeter is not clearly marked and not within the reach of the IT department. A recent study by Mobile Enterprise, cited in [12], indicate that corporations are now controlling only 35% of mobile devices in the workplace, while 65% are personal devices that have access to company resources.

2.5 The Emergence of BYOD

BYOD first emerged as a result of organizations trying to respond to a change in the employees demand job flexibility and desire to perform their work with the most recent technology [11]. Also employees are able to access whatever information they require from anywhere which enhances their productivity. [10][11].

The benefits of BYOD to both user and organization are many. The major and common ones discussed in the next section.

2.6 Benefits of BYOD

There are several benefits derivable from the adoption of BYOD by an organization. Some of the benefits include:

i) Increased Productivity and Employee Satisfaction

Employees are able to do more work outside of work hours and leading to more achievement and improvement in the operations of the organization. Where there is flexibility, employees are satisfied as they are free to use devices of their choice.

ii) Attracting, Retaining and Supporting New Talent

Most job seekers now prefer environments where employees are allowed to use tools and technologies they like and are used to. The resultant effect of this is that organizations are more likely attract, employ and retain good workers.

iii) Lower IT Procurement and Support Costs

BYOD enables organizations to save huge amount of costs they would have spent on procuring, maintaining and upgrading devices for employees. Although the initial cost of providing the required support infrastructure may be high, the end result will be lower cost of ownership at the end of the day.

iv) Improved collaboration

BYOD enables employees to cooperating in achieving task most quickly. Many applications now exist that make the collaboration between the employees-owned devices possible. Some of the applications include virtualization, connectivity-everywhere, anywhere-access to corporate data, among others.

2.7 Strategies for Managing BYOD Risks

There are two major strategies for managing the risks posed by BYOD. One strategy is complete avoidance by not allowing BYOD in the organization. Some organizations can weigh the cost of losing data against gain in productivity and decide against BYOD in order to maintain a firm grip of the IT environment [14]. For example, IBM in May 2012 directed that no staff should use DropBox and Siri in the organization for security reasons. IBM claimed that Siri listens to spoken requests and sends the queries to Apple's servers where they are decoded into text. Siri can also create text messages and emails on voice command, but some of these messages could contain very sensitive information. Although total avoidance of BYOD may offer a way out from an information security perspective, it denies the company or organization of the enjoying the benefits of changing employee expectations and other benefits that BYOD brings as mentioned in previous section.

The second strategy is to put in place an Information Security (IS) strategy for the organization in order to exploit the power of BYOD and balance Security and Usability concerns. Many organizations go for this option by embracing a third party application called Mobile Device Management (MDM) to help manage the vast mobile resources on their infrastructure. The adopting a third party application is only a technical solution. A computer Information Security strategy must include both technical and non-technical aspects [11]. This will include a comprehensive BYOD policy that covers various aspects like device types, security, and usability, among others. Such policies must consider the interests of employees in order to gain their support and compliance. The BYOD policy must also make provision for user education and training awareness (SETA).

3. Research Methodology

This research is based on qualitative method of gathering secondary data achieved first by carrying out general searches to determine the extent of literature and related research materials available on the various issues on which the paper is based. The reviewed literature covers recent materials on the topics considered. Key content areas include. To achieve effective and efficient search, keywords were combined to form key phrases which were used to the search. Some of the keywords include: BYOD, BYOD higher education, BYOD management, BYOD policy, BYOD security, BYOD strategies, BYOD user education, Bring your own device, IT Consumerization, MDM strategies, Mobile devices, Mobile device management, Mobile learning. A number of databases were searched using the search terms in order to arrive at relevant journals, articles and publications on the various topics. Some of the databases include ACM Digital Library, IEEE, ScienceDirect, Google Scholar and the internet generally.

3.1 Existing BYOD Models for Educational Institutions

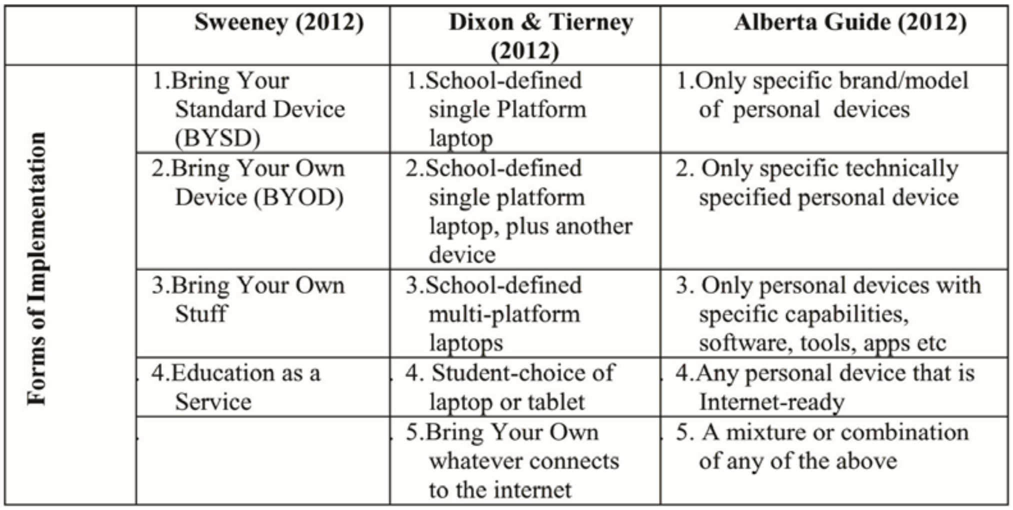
There are various models for BYOD, both proposed and in use. At one end are the highly "locked down" models where the device to be used is dictated by the school. At the other end of the spectrum is the "bring your own whatever connects to the internet" model, where the school does not prescribe any device at all. In this paper, we compare three existing models with their various BYOD implementations. They are [15], [16] and the [17]. The comparison is summarized in Table 1 below.

3.2 BYOD Policy

Implementing the BYOD strategy is only possible with a comprehensive policy. To develop an effective policy, organizations need to define and understand factors such as:

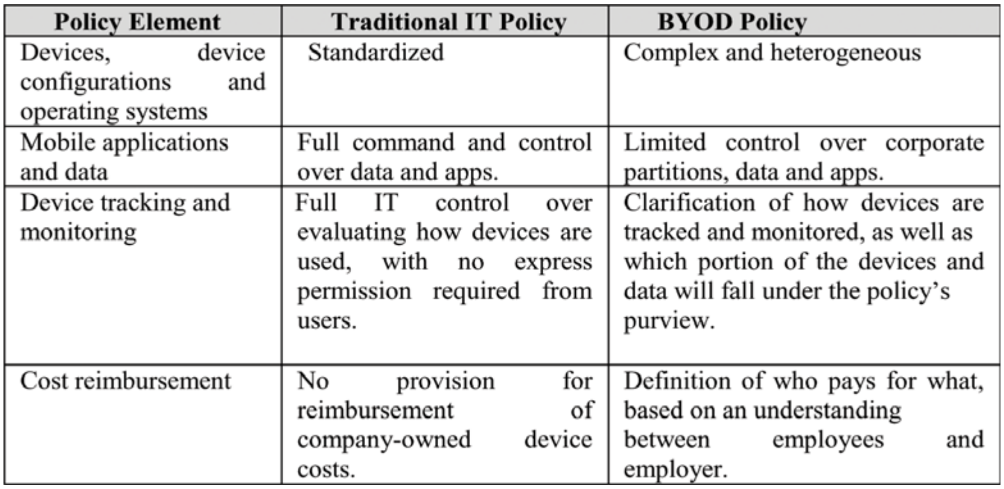
- Which devices and operating systems to support.
- Security requirements based on employee role and designation.
- The level of risk they are willing to tolerate.
- Employee privacy concerns.

The benefit of flexibility enjoyed by employees is changing the IT environments in organizations. IT now has to devise means and policies to manage the traditional IT environment comprising of the normal organization infrastructure and the BYOD IT environment comprising vast number of mobile devices with various operating systems. Some very clear differences between traditional IT Policy and BYOD IT policy are presented in table 2 below:



	Sweeney (2012)	Dixon & Tierney (2012)	Alberta Guide (2012)
Forms of Implementation	1.Bring Your Standard Device (BYSD)	1.School-defined single Platform laptop	1.Only specific brand/model of personal devices
	2.Bring Your Own Device (BYOD)	2.School-defined single platform laptop, plus another device	2. Only specific technically specified personal device
	3.Bring Your Own Stuff	3.School-defined multi-platform laptops	3. Only personal devices with specific capabilities, software, tools, apps etc
	4.Education as a Service	4. Student-choice of laptop or tablet	4.Any personal device that is Internet-ready
		5.Bring Your Own whatever connects to the internet	5. A mixture or combination of any of the above

Table 1. Comparison of BYOD Implementation Models



Policy Element	Traditional IT Policy	BYOD Policy
Devices, device configurations and operating systems	Standardized	Complex and heterogeneous
Mobile applications and data	Full command and control over data and apps.	Limited control over corporate partitions, data and apps.
Device tracking and monitoring	Full IT control over evaluating how devices are used, with no express permission required from users.	Clarification of how devices are tracked and monitored, as well as which portion of the devices and data will fall under the policy's purview.
Cost reimbursement	No provision for reimbursement of company-owned device costs.	Definition of who pays for what, based on an understanding between employees and employer.

Table 2. Comparison of Traditional IT Policy and BYOD IT Policy

4. Adoption of BYOD in Educational Institutions in Nigeria

Education institutions all over the world are turning to BYOD solutions to better enable and provide the benefits of technology with a view to enhance learning and improve student and staff productivity while avoiding the cost of owning the devices themselves. Although, BYOD is not yet recognized as a technology or programme on this side of the world, it has been in use for a long time. For instance, at Covenant University Ota, Nigeria, a number of students use their personally owned devices for learning and accessing corporate infrastructure like internet and datacenter. A BYOD policy will therefore be required to formalize this kind of arrangement.

Educational institutions implementing BYOD must take steps to minimize privacy, security and regulatory concerns. When personally owned devices are allowed to access corporate network without proper management, it can lead to breaches of privacy and data security. Although BYOD has the potential to significantly reduce capital expenditures, it can also increase operating expenditures if not properly deployed and managed. The use of personally-owned mobile devices by students, faculty, and staff for the purposes of facilitating and supporting the academic and administrative roles of an institution is presenting new challenges that require the development of an institution-wide IT strategy that supports BYOD.

4.1 Proposed BYOD Policy Framework

A complete BYOD strategy comprises of a comprehensive BYOD IT policy and other technical components like MDM. In addition, a BYOD IT policy needs to be more specific than in a traditional IT policy so as to guarantee data and network security. It is important and necessary to design the BYOD IT policy with the users in mind. According to Frank Andrus, the CTO at Bradford Networks, the development of a BYOD policy must directly involve users because central IT must have high visibility into the devices used at the institution and how they are used [10]. It is also important for the central IT to educate users as to the implications of using their personally owned-devices at work; Andrus outlines a ten-step process for IT policy development that takes the use of mobile devices into consideration. Also, [18], in their textbook, Management of Information Security, present a general framework useful for developing a BYOD policy. The framework includes seven clearly defined sections like statement of purpose, authorized users, prohibited users systems management, violations of policy, policy review and modification, and limitation of liability. Figure 1 shows the diagram of the proposed BYOD policy framework.

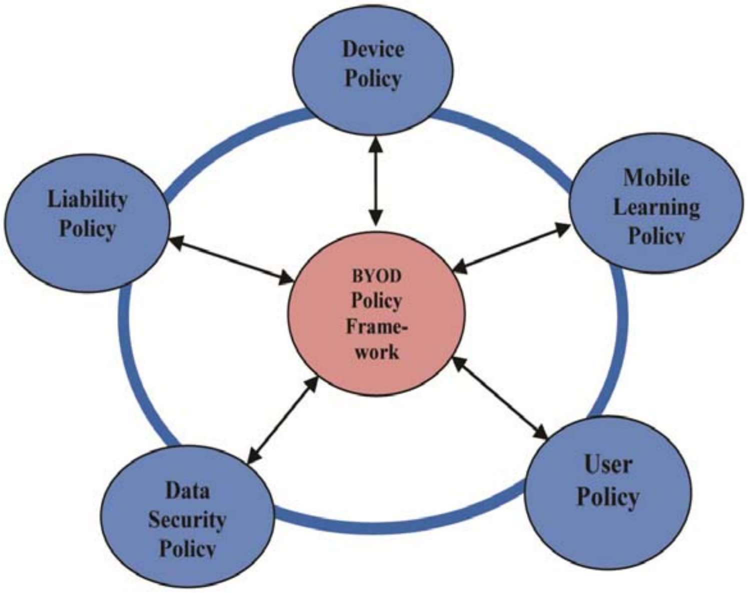


Figure 1. BYOD Policy Framework for Educational Institution

The major components of the proposed policy framework include:

i) Device Policy

This policy is concerned with choice and type of devices to be allowed under the BYOD progamme. There are generally two extremes namely; the highly restricted devices model in which the organization specifies all the details of the devices to used and the flexible devices model in which the user is allowed to bring any device of choice provided it can serve for work [17].

ii) User Policy

The policy category concerns users of the BYOD technology. It usually includes details of authorized and unauthorized users of the programme. The degree of access by users is usually based on responsibilities and roles played by the individual user in the organization. The policy also includes details for user education and training on the use of the BYOD technology. Trainings should be provided to all approved mobile device users to inform them on the appropriate and inappropriate use of their device within the institution [19]. The trainings should cover several issues, including (a) social media usage, (b) personally identifiable information, (c) strong password creation, and (d) privacy settings [19]. This training is necessary for new recruits or when introducing a new resources. The training should also be on a regular basis especially as a user request that his or her device be accommodated on the organization’s network [20].

iii) Data Security Policy

This policy includes guidelines on how corporate and private data is kept secured while using the BYOD technology. The use of personally-owned mobile devices presents security risks to data both within the institution and the user’s data. The mobility advantage of BYOD will be a waste if user-owned devices are not well protected against mobile device security threats. The competitive edge promised by mobility can be wasted if consumer-owned mobile devices are not adequately protected against mobile device security threats. According to Markelj and Bernik (2012), IT organizations identify security as one of their greatest concerns in regard to the extending of mobility. This policy may include guidelines such as segregating user and corporate data; enforcing users to register devices; enabling remote access to a mobile device; implementing data encryption; using strong passwords; and setting up a virtual private network (VPN). Organizations exist that are working hard to incorporate most of these guidelines into third-party applications like mobile device management (MDM) solutions [21].

iv) Mobile Learning Policy

This policy deals with how the functionalities of a mobile device can be used to support learning. The New Media Consortium's higher education edition of the 2012 Horizon Report states that mobile apps are the fastest growing dimension of mobile space in higher education worldwide. BYOD policy consideration for mobile learning may include the following; mobile device use for academic learning; communication anywhere and anytime; micro-application development; benefits for students with learning disabilities; concerns with mobile learning; and Mobile-learning and beyond

v) Liability Policy

This policy deals with the financial aspect in terms of reimbursement or settlement of bills incurred by mobile users on the BYOD platform. Definition of who pays for what, based on an understanding between employees and employer.

5. Conclusion

This study presents and summarizes a number of references, including peer-reviewed articles, reports, journal, theses, and dissertations. The research surveyed various aspects of the IT consumerization phenomenon. The study proposed a policy framework that can help educational institutions to easily adopt the BYOD program. Worthy of note from the all the literature reviewed is the increasing quest for personally owned mobile devices. According to a study conducted by IDC, the revenue from the sales of smartphones first exceeded that of personal computers in the year 2010. [6] also stated that worldwide smartphone sales hit a total of 472 million units in 2011 representing an increase of 58% over sales of 2010 and are expected to reach 1.1 billion units by the year 2015. These mobile devices are now in demand as a result of convenience of use and their outstanding capabilities. We are now in a new era which can be termed an "Age of Mobilism" [22], as every mobile user wants to connected everywhere and every time through their cheap and widely accepted mobile devices. The use of mobile devices by faculty, staff and students of institutions of learning is also rising. This is why IT team and their leaders must rise to design BYOD programs that will address the various risks and challenges the use of these devices pose to the information security state of their institutions. No doubt, a well-designed BYOD policy will go a long way in ensuring that the BYOD program benefits all stakeholders.

References

[1] Trend Micro (2012). *Enterprise readiness of consumer mobile platforms*. Retrieved from http://trendmicro.com/cloudcontent/us/pdfs/business/reports/ rpt_enterprise_readiness_consumerization_mobile_p

[2] International Data Corporation. (2011). 2011 Consumerization of IT study: Closing the consumerization gap. Framingham, MA: Gens, F., Levitas, D., & Segal, R.

[3] Garlati, C. (2011). Trend micro consumerization report 2011. Retrieved from http://bringyourownit.com/2011/09/26/trend-micro-consumerization-report-2011/

[4] Kim, R. (2011, June 29). The iPhone effect: How Apple's phone changed everything. *Gigaom*. Retrieved from http://gigaom.com/2011/06/29/the-iphone-effect-howapples-phone-changed-everything/

[5] Gartner, Inc. (2012). Bring Your Own Device: BYOD is here and you can't stop it. http://www.gartner.com/technology/topics/byod.jsp

[6] Akniwunmi, A. (2013) Minister of Agriculture Denies Plan to Spend N60 Billion but Affirms that 10 Million Mobile Phones will be Bought for Farmers. Accessed from www.bellanaija.com, February 8, 2015.

[7] NIST. (2013). Gudielines for Managing the Security of Mobile Devices in the Entreprise. NIST SP-800-124 Rev1

[8] Niehaves, B., Köffer, S., Ortbach, K. Year. "IT consumerization under more difficult conditions: insights from German

local governments, *In*: Proceedings of the 14th Annual International Conference on Digital Government Research, ACM2013, 205-213.

[9] Armando, A., Costa, G., Merlo, A., Verderame, L. (2012). Securing the “Bring Your Own Device” Policy, *Journal of Internet Services and Information Security (JISIS)* (2:3/4) 3-17.

[10] Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network, *Computer Fraud & Security* (2012:4) 14-17.

[11] Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security, 2, 5-8*. doi: 10.1016/S1353-4858(12)70013-2

[12] Caldwell, T. (2012). Prepare to fail: creating an incident management plan, *Computer Fraud & Security* (2012:11) p 10-15.

[13] Moore, C., Warner, J. (2012). Industry Contexts And Constraints Diversify Approaches To Bring-Your-Own Technology, December 13, 2012.

[14] Sweeney, J. (2012). *BYOD in education: Nine Conversations for Successful BYOD Decision Making.* Microsoft.

[15] Dixon, B., Tierney, S. (2012). *Bring your own device to school.* Microsoft.

[16] Alberta Education. (2012). *Bring your own device: a guide for schools.* Edmonton: Alberta Education.

[17] Whitman, M. E., Mattord, H. J. (2011). *Principles of Information Security, 4th Edition*. Independence, KY: Cengage Learning

[18] Wittman, A. (2011). BYOD? First get serious about data security. *Information Week 1316, 46. Retrieved from:*http://global.factiva.com/aa/?ref=IWK0000020111114e7be0000a&pp=1&fcpil

[19] Harris, C. (2012). *IT executive and CEO survey final report: Mobile consumerization trends and perceptions. Used by permission of Trend Micro for the purpose of this study*

[20] Burt, J. (2011). BYOD trend pressures corporate networks. *eWeek*, 28 (14) 30-31. Retrieved from: http://web.ebscohost.com/ehost/detail?sid=6b0434ee-970c-40b4-

[21] Norris, C. A., Soloway, E. (2011). Learning and schooling in the age of mobilism. Educational Technologies, 51 (6) 3-10. Retrieved from http://cecs5580.pbworks.com/w/file/fetch/50304204/Soloway