The Future of BYOD in organizations and higher Institution of Learning

Onyechere Ugochukwu Franklin
School of Engineering and Computing Sciences
FTMS College, Technology Park Malaysia
Bukit Jalil, Kuala Lumpur, Malaysia
activate4u@yahoo.com

Mr. Mohamed Ismail Z.
Programme Leader cum Senior Lecturer
School of Engineering & Computing Sciences
FTMS College, Technology Park Malaysia
Bukit Jalil, Kuala Lumpur, Malaysia
ismail@ftms.edu.my

ABSTRACT

B.Y.O.D. (Bring Your Own Device) or B.Y.O.T. (Bring your own technology) is a new trend that has been perceived where staffs and students bring their personally-owned mobile devices to their study and workplace to access institutions resources such as email, file servers, databases, do other academic work or research as well as their personal data. The conception of 'Bring your Own Device' is gaining trust at the workplace and also study environment. According to Priya C. N. (2012), stated that most of the institutions and organizations abroad have started to implement this policy since the year 2012. A well organized questionnaire was distributed among 70 students and staffs chosen from various FTMSGlobal Departments of the College under study with response rate of 50 percent. The present study demonstrates and elaborates the various aspects of BYOD use, such as awareness of BYOD, the frequent use of BYOD, purposes for which the BYOD is used, collaborative tools used for academic purposes, concerns/problems faced by the users and satisfaction level of users with the BYOD facilities provided in the College. Using personal devices at work or study is beneficial in some ways like more productivity, flexibility, freedom and choice etc. Though, the policy has some risks as well like the prime issue of data security. It can be seen in the literature reviews that the
organization who clasps BYOD policy have seen that their employees and students are happier, productive and collaborative. Henceforth it was conducted with the primary objective of finding the views of respondents from different sectors and institutions.

**Keywords**: BYOD, Personally owned mobile devices, collaborative, Productivity, risks, threats, benefits.

### 1.0 Introduction

Currently mobile devices such as smart-phones, iPad, E-book readers, and tablets are being used by students and employees for personal use. The increasing demand for using these external portable devices in the context of the work and study environments is a valid question. The ongoing consumerization of information technology (IT) products in general plays a vital role in this situation, acknowledging the considerable personal investment of students and staffs in this hardware. Since the inception of information technology, there have been a lot of transformations both in human life and every other institution. The invention of smartphones, Tablets, iPads, Laptops etc. have transformed the thinking of individuals both working class, students and even our old school parents who were in the analogous world and now in the digitalized world. The growth in the telecommunication technology, with regard to 3G/4G network services and smartphone’s has created new ideas for communication and file management, data processing capabilities to do business. One of the ideas that has emerged in business world, IT and school environments is BYOD (Bring your own device). According to **Alberta Education** (2012), this new trend is referred as a “technology models where staffs and students can bring their own personal owned device to school or work for the purpose of learning or accessing organization resources for work”, inside or outside the institution’s environment. This new trend brings new opportunities and risks. Bring your own device (BYOD) is a new trend in information technology industry which enhances employees and students in institutions as well as organizations to use their personal mobile devices to access resources, their respective institutions materials for both work, studies as well as personal use. The tasks may range from accessing corporate documents, applications, emails, database and network etc. This
The concept was first introduced by Intel since 2009 when they recognized the importance of employees using their own devices for accessing corporate resources and network. Students are increasingly going to class with technology such as mobile phones, E-book readers, iPods, iPad and also small tablet computers in their pockets. The aim of this research work is to investigate the importance and the needs to implement BYOD in the higher institutions of learning and also in the organizations.

1.1 Research Questions
The following questions are formulated to guide the researchers in this study:

1. What are the various purposes for which BYOD is being used by the FTMS students and staffs?
2. What is the level of students’ and staffs satisfaction regarding the BYOD services in FTMS?
3. What are the impacts of BYOD on students’ and staffs learning, research and working?

1.2 The objectives

1. To create awareness about the BYOD policy amongst educational professionals.
2. To examine the needs and benefits of BYOD in the organization’s BYOD policy implementation.
3. To determine the level of students’ satisfaction with the BYOD services in FTMS.
4. To examine the impact of BYOD on students’ learning and research.

The basic idea of BYOD is this, instead of the schools or organizations providing technology for students or workers to use (Laptops, E-book readers, and tablets, access to computer room), the students go to class with technology they already have and use at home. The technology includes iPod, iPad, tablets, E-book readers, and laptops. This is to enable the students to carry out their own research work during lessons, take notes in the class, and record some audio or video and also consults dictionaries. BYOD refers to the staffs and students bringing their own devices chosen from a range of devices which are authorized by the institutions. For example, the institutions may allow individuals to bring their own USB devices, laptop, smart-phones and not gaming consoles. For organizations and institutions to face the competitive challenges in the information technology worlds, they
will need to facilitate any kind of technological advancement at the end user side which has to do with their employees and also students but not compromising with the security of the corporate information and the privacy of the end users.

2.0 Literature review

Information and communication technologies (ICTs) are taking on an ever greater fame in education and also at the working places. Now many governments’ institutions are emphasizing the basic need to turn out digitally literate, technologically able graduates who are employable in the global information economy (Buchanan, 2011). Many instructors have emphasized the creative, student-centered educational approaches assisted by the use of digital tools, while others stress the role of online communication and collaboration in creating well-informed and well-connected global citizens (Pegrum, 2009). Nevertheless certain tensions between the goals of governments and those of educators, ICTs are becoming more and more entangled in teaching and learning.

Many advocates of m-learning and u-learning favour a 1:1 model, i.e., where each student can use at least one personal device (Looi, Seow, Zhang, So, Chen, & Wong, 2010). In educational contexts, there is a drive for a Bring Your Own Device (BYOD) or Bring Your Own Technology (BYOT) idea, based on the idea that students must be encouraged to bring their personal devices, laptop, E-book readers, iPad or smartphones, to class (Kolb, 2008, 2011; Nielsen & Webb, 2011; Richardson & Mancabelli, 2011; cf overviews and commentary in GSMA, 2011a, 2011b; Traxler, 2010) and to use them for learning purposes across a range of formal and informal contexts.

The BYOD policy is a way to achieve social activities in an institution or organization. According to Savitz, Eric Karayi and Sumir,"Students and staffs seems to depend so much on using any of their personal devices like laptop, E-book readers, iPad, smartphone, USB device for their work just because they consider their own device more reliable to compare with the one that is been provided by the organization". However, the organizations/institutions are also shaking hands and moving towards making a collaborated, communicated and staffs satisfaction.
In the world of Golia Nathan, the BYOD have almost five vital benefits in field of health care educational and financial industries/institutes. The benefits include saving cost, booming connection, accessibility, flexibility and adaptability.

According to the study by Yun Haejung, Kettinger William J, Lee Choong, it is found that the use of Office Home, personal devices, smartphones lead to increased work-to-life warfare and thus created job stress and users resistance to use office home smartphone (OHS). Hence productivity is gained and it also reduces workload. Social in this aspect means to keep staffs happy, Business i.e. keep processes running smoothly and effectively, Financial to manage costs and Risk Management i.e. to stop bad things from happening.

According to Silicon India, most of the Indian business activities are adopting BYOD in their organization. However, in the consumerization study conducted by IDC (2011), it is discovered that despite security threats and the support issues BYOD trend continues. In a paper by Burt and Jeffrey, they have noticed that increased adaptation of BYOD have changed the attitude of the staffs towards corporate network safety of business activities. It says staffs are successfully using personally owned mobile devices including smartphone, iPad, and tablets etc. as well to access business software applications.

According to McNeill, M. Diao, M.,Gosper (2011), discussed the exploration of the technology usage in students’ daily lives, how they use it whether at home or at school and at work to facilitate their learning, working. Their results reveals “that this generation of students and staffs prefer receiving information swiftly, have a low tolerance for lectures, prefer active rather than passive learning and rely heavily on communication technologies to access information.” Technology is a tool for attracting intellectual learning and critical thinking in the school and organizations. Jonassen, D. and Crismond (2008), found out that with BYOD use lecturers are in a better position to look for suitable techniques to communicate with their students by representing ideas, beliefs, simulating real-world problems ,accessing information, and even assisting their students represent what they have learned. Additionally, technology advances students’ success since it can support the instructors produce teaching material suitable for all learning styles. Likewise, audio and video technology can present the educational material to life, which helps the students
understand and ascertain the reasons why the material taught is very important in actual life.

BYOD in education has come to stay. Pupils of today are becoming addicted to technology they have grown up with and they want to continue using it in whatever they do in their lives on daily basis which includes academic activities, working activities which become even more interactive. Meanwhile many institutions have the infrastructure to support wireless devices; they should be encouraging the students on the use of it since they cannot do without BYOD which has the abilities to positively affect educational and organizational outcomes.

2.1 Managing BYOD

There are two models to consider when talking about managing BYOD within an organization which are:

a. Mobile Device Management:

The mobile device management tool helps every organization or institution to fully control the devices which are generally supported by API’s of smartphones used these days. However, the MDM is a tool that is in a centralized state which helps to control the devices and can do over the air configuration remotely to those devices that are connected to the network. With the help of the MDM tool organizations can lock down devices, enforce the BYOD policies on the device, can also encrypt the data and even wipe any data on the device locally or remotely. The MDM tool will help on the security threat and management of device by monitoring, controlling and protecting the device. It can do so by enforcing security settings, management of passwords, installing digital certificates for data authentication. It can monitor applications software installed on the device. The MDM can also push for installation of applications on the device and enforce policies for the usage of the application. It can also uninstall any software applications on your devices. The MDM can generate reports and can manage the inventory of devices and software applications. It can create groups for the devices and classify the files. It also restricts user from downloading and install certain software applications. It also helps to backup data and provides recovery services.
Figure 1: MDM architecture

The mobile devices are connected to the corporate network through an encrypted channel. The device platform can be Android, Apple, Symbian, and Blackberry etc. The MDM is placed at the DMZ which is public facing so that devices who are trying to communicate from external network can be enrolled and configured by the MDM.

b. Cloud services

Figure 2: Cloud Architecture for Mobile Devices

According to the figure, the client on the mobile device will be able to access the service through a middle or broker which will be guiding the delivery to the end user. When a staff will try to access the data using his or her phone, the person will undergo a verification process which can be through certificates, tokens, smart cards or also SMS along with form based username and password tool which would ultimately be following a multi-factor verification approach. Single sign-on
functionality can also be incorporated easily; the staff that login will have an access to all the necessary resources according to his/her privileges for that session.

2.1.1 The issues that MDM considers while managing the devices are as follows:

a. Device Management: The device management helps to the manager to manage the software applications on the device. This involves in the inventory of device. The Management of the various licenses is also done by it and it also manages the devices configuration based on the organizations policies. It will remotely control the device like locking and wiping. And also manages the session of the devices to communicate with the corporate network.

b. Security Management: In the MDM, it also considers various aspect of security such as configuring the MDM itself, managing of data security and applications.

c. File Synchronization: The MDM will help to stores backup, manages the file session to synchronize file transfer and various documents.

However, MDM can act as a really solution for an organization to manage staffs owned devices.

According to Chris C (2011), stated that BYOD is Information technology industry trends which have 10 steps of Best Practices that can be followed for the successful implementation of BYOD in organizations. They are:

i. Creating a comprehensive BYOD policy: Every organizational head should be able to take decisions on the devices which will be used or allowed for staffs and students of the institutions, security settings, software Applications to be loaded, Passcode etc.

ii. Measuring your mobile footprint

iii. Simplify user enrollment

iv. Configure policies over the air

v. Provide self service abilities

vi. Protect personal information (PII)

vii. Isolate corporate data

viii. Continuously monitor automated actions
ix. Manage data usage
x. Track the every activities of BYOD

The implementation of BYOD is not just enough to start with it. The most important and complex part of it is the security issues. For the organization to get the best results out of BYOD the organization will have to look into some security issues which has been depicted by Bernard and Ho in form of Security Architecture Framework (SAF) with eight layers (Bernard & Ho, 2007, p.10)

Figure 3: Security architecture Framework (Bernard & Ho, 2007, p.10)

In this diagram each step of security indicates an area like strategic policy securities, Operational security, Physical security, Infrastructure security, Information and data flow security etc. and all plays important role in overcoming the BYOD related threats.

2.1.2 Pros AND Cons of BYOD
In order for every organization to overcome all the security Threats related to it following are the few steps that can be followed:
• **Wi-Fi:** It has been observed that most people in the organization assess the network through Wi-Fi connection which is unencrypted hence according to **Michael Buckna**, Communications engineer, Voice-over-IP provider organization systems group “It is the distribution of IP and managing Virtual Private Network (VPN) solutions for all the handheld mobile devices or smart-phones.

• **Credential information:** The second risk is the phone theft or the stolen devices; it’s the most tedious one to face. The user credentials like username and password, installed certificates, banking personal information, web accounts, and E-mail account can be accessible if the device is stolen. This aspect can be handled by changing email, drop-box, passwords etc.

• **Malware:** The antivirus and malware which are dangerously in used by users and the system as well. To overcome and prevent these security threats, the systems and devices should be well equipped with the latest anti-viruses and anti-malwares.

• It has been said that BYOD reduces cost but there are examples when the organization has faced the requirement of upgradation more especially in a company, where they gave their staffs ipads as app resultantly, the organization needed progression because more staffs were assessing it.

• **Spam:** Unwanted messages and emails are being received from unknown or known sources causing wastages resources such as memory spaces and bandwidth.

• **Phishing:** This can be conducted possible through an email or short messages (SMS) phishing to trick a user to access fake website to access business accounts.

• **Confidential Business Data:** Confidential organization data like documents, reports, files, email, database etc. is at risk if there is an unauthorized access on the device that take place due to device compromised.

### 2.1.3 Benefits of BYOD:

• **It has been observed that staffs and students who use mobile devices for work, studies and personal issues put in 240 more hours per year than those who do not.**

• **It reduces the cost incurred and ongoing end-user management i.e. the maintenance and upkeep of the devices and gadgets are now the responsibility of the organization or institutions. Hence the company or institutions don’t need to look**
after the hardware and software as this is now done by the staffs and students
tselves.

- It will be much easier for users to switch to the latest version in time being which is
  not possible for institution or organization and it will gives time to focus on strategic
decisions then to spend time in operations.

- It will acts as a competitive advantage over others and it will attract staffs from the
  market and offers flexible timings. The BYOD application will attract top performing
  staffs because it enhances flexible work time and also work-on-the-go.

- It will reduce the training time thereby increasing the efficiency and productivity of
  the staffs and students.

- The implementation of BYOD increases the engagement of the staffs and students in
  the work and study places and after hours.

According to Christian Childs (n.d. Marketing director, Dell), “The idea of BYOD is a more
business decision than that of IT decision. By applying BYOD, the organization or
institutions gets benefits from being more productive and collaborative end user
environment, this is the ability to retain and hire top talents, for end users, and it will give
him more work or study flexibility.”

3.0 Methodology
The researcher distributed questionnaires randomly to the respondents at the various
FTMSGlobal College in order to collect data from the respondents. Questionnaires were
also distributed randomly to the respondents at the TPM premise. The questionnaires for
BYOD users were filled up by the students and staffs of the various Universities and
colleges. A total sample of 70 students were chosen for the research study. For sampling,
random sampling process was followed for data collection. The sample was random in the
sense that the students and staffs were randomly selected from the various FTMSGlobal
(Faculties) of the College. Out of Seventy (70) questionnaires were distributed to the
respondents, fifty (50) were returned. With this, eighty percent (71.4%) of the respondents
returned their questionnaires while twenty nine percent (28.5%) could not return theirs. Descriptive statistics was used to analyze the findings. The responses of the students and staffs were analyzed using simple percentages and information were drawn which answered the research questions.

### 4.0 Findings / Discussions

<table>
<thead>
<tr>
<th>Question 1. Awareness of BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aware</td>
</tr>
<tr>
<td>Not aware</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

As it is evident that only 48% of respondents were aware of the BYOD while 52% are not aware of BYOD. The institutions will need to implement the BYOD policy and also create awareness of the need for the BYOD and the benefits.

<table>
<thead>
<tr>
<th>Question 2. Faculty/Department distribution of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Information Systems (BIS)</td>
</tr>
<tr>
<td>Software Engineering (SE)</td>
</tr>
<tr>
<td>Hospitality</td>
</tr>
<tr>
<td>Marketing/Admin</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>
The table above shows that 38% of the respondents were from the Faculty of Software Engineering. Faculty of BIS have 32% respondents; 20% respondents were from the Faculty of Hospitality; Marketing/Admin have 10% respondents each. This is an indication that all the faculties within the college were well represented in the survey.

<table>
<thead>
<tr>
<th>Question 3</th>
<th>Amount of time spent using the device?</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 hours a week</td>
<td>5</td>
</tr>
<tr>
<td>9 hours a week</td>
<td>9</td>
</tr>
<tr>
<td>20 hours a week</td>
<td>23</td>
</tr>
<tr>
<td>More than 20 hours a week</td>
<td>13</td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
</tr>
</tbody>
</table>
This shows that the maximum number of respondents i.e. 23 (46%) spend more than 20 hours a week using BYOD Device. 13 (26%) use the BYOD for more than 20 hours. Only 9 (18%) respondents have indicated that they use BYOD for 9 hours a week, while 5 (10%) respondents use the BYOD for 6 hours a week.

<table>
<thead>
<tr>
<th>Question 4 What is your comfort level using computer technology?</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning User, uncomfortable, need a lot of assistance.</td>
<td>7</td>
<td>14.0%</td>
</tr>
<tr>
<td>Average User, comfortable, need a little assistance</td>
<td>10</td>
<td>20.0%</td>
</tr>
<tr>
<td>Above Average User, very comfortable, provide some assistance to others</td>
<td>13</td>
<td>26.0%</td>
</tr>
<tr>
<td>Expert User, extremely comfortable, coach and mentor others</td>
<td>20</td>
<td>40.0%</td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
<td>100%</td>
</tr>
</tbody>
</table>
The question was asked to find out the facts about the level of FTMSGlobal students and staffs comfort in using the BYOD. It was found that 20 (40%) of them are extremely comfortable and they even coach other students. Another 13 (26%) respondents are above average users; while 10 (20%) respondents indicated they are average users; only 7 (14%) of the respondents are not comfortable because they are beginners. It is evident that the majority of respondents are very comfortable in using the BYOD.

<table>
<thead>
<tr>
<th>Question 5... which is the biggest threat while applying this policy in an organization?</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate IT Security</td>
<td>35</td>
<td>70.0%</td>
</tr>
<tr>
<td>Complexity of set up</td>
<td>3</td>
<td>6.0%</td>
</tr>
<tr>
<td>Increased cost</td>
<td>6</td>
<td>12.0%</td>
</tr>
<tr>
<td>Lack of control over</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Potential threat to IP</td>
<td>6</td>
<td>12.0%</td>
</tr>
<tr>
<td>Total</td>
<td>50</td>
<td>100%</td>
</tr>
</tbody>
</table>
Hence it is evident from the data that the most risky factor that is the biggest threat amongst all is the Corporate IT security and all these factors can be arranged in the sequence, starting from the biggest threat, of there risk as follows:
1. Corporate IT Security
2. Potential threat to IP
3. Increased cost
4. Complexity of Set up.
5. Lack of control over devices

| Question 6 To what level you think is it lucrative to apply BYOD policy in an organization? |
|---------------------------------------------|---|---|
| FULLY AGREE 1                               | 3 | 6.0% |
| 2                                           | 20 | 40.0% |
| 3                                           | 15 | 30.0% |
| 4                                           | 9  | 18.0% |
| FULLY DISAGREE 5                            | 3 | 6.0% |
| Total                                       | 50 | 100% |
Similarly, the third part of the data analysis discusses about the lucrative factors of BYOD those are: Improved efficiency and productivity, higher job satisfaction, Enjoy Increased mobility and competitive advantage over others.

5.0 Conclusion and Recommendations

The results of the questionnaire so far revealed that BYOD is an inseparable part of today's educational and organizations system. The reliance on BYOD is growing day by day and the users of FTMSGlobal too are depending more and more on the BYOD for their various educational purposes. BYOD has enabled the students to enhance their academic excellence and also workers to improve on their services by providing them with the easiest and convenient way to access worldwide information for learning. In order to make the BYOD more beneficial, there is need for the Information Technology Division (ITD) unit of the College to brace up and improve the BYOD services to facilitate the learning process of the numerous students and staffs of the College.

There is a huge scope for future research in different types of users’ behavior and comparison of users' behavior and attitudes towards the BYOD. The use of the BYOD is an evolving phenomenon at this stage. According to David Clarkson, HR manager at Cisco
Canada stated that "Productivity happens where people are comfortable and using devices that are most comfortable for them." Cisco was the first to apply BYOD in its organization and other organizations have also started implementing BYOD.

6.0 References

Indian firms embrace the BYOD trend (2012).SiliconIndia Vol 15 Issue 6, p 9-9
IT Managers in BYOD deadlock (2012).SiliconIndia Vol 15 Issue 2 p 10-10
British communications (BT). Indian firms embraces BYOD. Lets_talkBT
Forrester Research , Inc. (2012). Key Strategies to capture and measure the value of Consumerization of IT. Forrester Consulting, July 2012, pp 1-17