SECURITY RISKS ASSOCIATED WITH BRING YOUR OWN DEVICE BYOD AND POSSIBLE MITIGATION TECHNIQUES

Ogbene Ehikioya
Computer Science Education Department,
Federal College of Education (Technical) Asaba,
P.M.B 1044,
lupady4u@yahoo.com
08134229338

Binitie, Amaka Patience
Computer Science Education Department,
Federal College of Education (Technical) Asaba,
P.M.B 1044,
Philpat4sure@gmail.com
07035901508.

&

Joe-Obasi Adauzoh
Computer Science Education Department,
Nwafor Orizu College of Education Nsugbe, Anambra State,
08162219628

Abstract
Bring Your Own Device (BYOD) is a technology that encourages employees to use their mobile computing device for both professional and personal purposes. The device is required to be connected to the organization’s network and function like a corporate device implementing the organizational policies but at the same time satisfying the
personal requirements of an employee, because the device basically belongs to the employee. This technology comes with many benefits like increasing the quality of performance and productivity, profit increment, increasing employees comfort among others. It equally has some risks associated with its use. Some of the risks are security breaches, loss of data or device and so on. It is recommended that companies that implement the BYOD Technology need strict policies in place to govern it. It is also recommended that a type of BYOD called Choose Your Own Device (CYOD) is implemented so that the organization can implement whatever security policies they need to protect the device effectively and create more efficiency security-wise.

**Keywords:** Bring Your Own Device, Choose Your Own Device, Employee, Employer, Mobile device.

**Introduction**

Everyday technology provides new ways to make life simpler; the world is now a global village thanks to the internet. In terms of making employees job flexible and easier, one of the main technology that strongly handles the provision of flexibility is BYOD. Bring Your Own Device BYOD is an acronym that simply means “Bring Your Own Device”. It is a technology that encourages employees to use their personal mobile devices at their job, to connect directly to the network of the organization that they work for (Yin and Liu, 2014). It can also be defined as a modern mobile technology that involves an employee bringing his/her personal mobile device(s) to a place of work to be utilized for effective and efficient work, the device is required to be connected to the organization’s network and function like a corporate device implementing the organizational policies but at the same time satisfying the
personal requirements of an employee, because the device basically belongs to the employee. Brodin, Rose and Åhlfeldt (2015) describes BYOD as mobile computing devices which are used in offices, homes or can be used for both professional and private purposes, even if the device was provided by either the employer or the employee. The ubiquity of mobile devices has redirected organizations towards a path of high consideration for the BYOD technology, seeing that mobile devices are now commonplace in the private lives of employed people, this has turned out to be beneficial because it encourages convenience on the job, considering that a company staff will most likely be more comfortable utilizing their personal technology device for work purposes with regards to the fact that they are more familiar with the personal device than any other device provided by the company for work purposes. Prior research has proven that BYOD increases employee productivity, and BYOD also facilitates work that can be carried out during non-working hours, owing to the situation that an employee can work on his/her personal device at work, motivation for work tends to increase even during non-working hours. Brodin et al. (2015) highlighted some virtues of BYOD, such as better personal productivity, improved flexibility of time and place and user satisfaction.

There are many more benefits that BYOD brings to both employers and employees. However, the implementation of the BYOD policy in a corporation attracts an astronomical drawback, this is the issue of security, though this is the greatest challenge in the BYOD technology, it is however not the only one. In this regard, this paper explores the benefits, challenges, and analyzes the security challenge associated with the BYOD technology using illustrations from a network breach simulation, and how to tackle them.
Theoretical Framework

It is common to see most of the employees today in their work environment with their smart-phones, tablets, laptops and so on. For the security of company’s vital information, it is important that the employees abide by the security rules and policies guiding their access to such data using their own device. With Bring Your Own Device phenomenon, employees are free to use the devices for personal and work related issues, anytime, anywhere. Li and Siponen (2011) pointed out that the unique nature of BYOD makes it imperative that workers should categorize BYOD under work and personal domain. This will enable them to abide to the security rules and policies guiding organizational information or data. Alaskar and Shen (2016) proposed five contextual factors relating to work or personal use of BYOD. These factors include; device ownership, activity, place, information sensitivity and time. Some employees find it difficult to strike a balance between personal use and work use of the devices or determine when they are in personal life domain and in work domain. These factors outlined by Li and Siponen (2011) can be used to strike a balance between work domain and personal life domain. Some scenarios might be exceptionally difficult to determine. For instance when an employee is using a personal device outside work environment and time to carry out official work at home or when an employee is using personal device at work and work time, to carry out personal life activities. These scenarios might be difficult for the employer to determine the domain he or she is in. The most important factor in BYOD is security of information. In the research carried out by Mat, Nurazean, Narayana, Pritheega, Hafizah and Roslina (2018), it was confirmed that most important factors to consider in BYOD implementation are, both human and information security.
Benefits of BYOD
The benefits of BYOD are undeniably far reaching. Corporate organizations and private businesses usually desire to increase operations and flexibility in business. The business velocity won’t be constrained by time and place due to the features of BYOD. The unwavering gains of work mobility influence employees positively, both in their personal lives and in balancing their job duties. Due to easy and instantaneous access to the internet, employees can make use of their personal smart phones and other devices for enterprise activities; this appears to be a norm in a lot of organizations in recent times. However this technology that encourages employees to use these devices comes with benefits and risks. Some of these benefits are as follows:

1. **Increase in Quality of Performance and Productivity:** BYOD makes it easier to access organizational data, emails, documents and other information remotely. It has profoundly transformed the way corporate organizations carry out business transactions. Operations are no longer restricted to a particular office, building or computer system. Employees now have the flexibility and comfortability to carry out job functions from almost any location, and at any time of the day. The smart device has been transformed to an office on the go.

2. **Increase in Employee Comfort:** Employees are undeniably more comfortable and satisfied using their own devices for work purposes. Studies reveal that employees that are permitted to make use of the same device for both private and work purposes tend to put in more work than others, and save hundreds of hours each year for their company (Miller and Varga 2011). A company assigned device such as a phone, laptop, or tablet will most likely have restrictions placed on them due to company policy,
but when an employee owned device is used for work, it produces the flexibility and freedom for the employee to utilize their devices for both professional and personal use. The option of personal selection of devices rather than company imposed devices also allows for greater flexibility in performing their job.

3. **Profit Increment**: With BYOD, companies can minimize cost and maximize profit, the employee usually covers the cost of purchasing the device, the problem of maintenance is highly reduced, the responsibility of device maintenance is less on the organization and relies more on the employees, and this also saves the organization the cost of carrying out regular maintenance and device upgrades. It is not the organization that pays for the device acquisition and upkeep. Generally smart phone users tend to update and upgrade their devices more often than a corporation would normally do, companies can benefit from the recent technology and more powerful device capabilities when employees do upgrade and update their mobile devices. Generally, this greatly reduces capital overhead for organizations by reducing the number of devices that the organizations have to procure for the employees to work with, the training process for the devices are also boycotted due to the familiarity that employees have with their own device (Ghosh, Gajar and Rai, 2013).

**Risks/Challenges of BYOD**
BYOD can either be one of I.T’s greatest opportunity or a ticking time bomb, it is classified as such due to the kind of challenges it attracts. Some of the risks or challenges of BYOD are as follows:
1. **Security Threats**: The most prominent risk that organizations implementing the BYOD technology will most likely encounter is that of security breaches, when employees access sensitive company data from an unsecure network, the possibility of malicious attacks, virus attacks, data theft and unprotected sites are all factors than can leave a company’s network at risk for cyber-attacks through employee personal mobile devices, and employees are not always aware of how to detect them. Even though some employees may apply certain security measures, these measures may still not be strong enough to withstand certain attacks. BYOD exposes company network to security threats because the employee devices store sensitive company data on personal devices that are not permanently stationed in the company building. It is difficult for the company to implement certain organizational security measures on employee personal device without interfering with certain employee personal activities on their devices. Security threats are constantly posed on organizational network, Li and Clark (2013) explain that employees may not have the necessary understanding of the available organizational security mechanisms, nor will they be able to properly utilize the protection mechanisms that the organization may want employees to implement on their personal devices to the benefit of both the employees and the organization.

2. **Loss of Data or Device**– Protecting organizational data or employee device from unauthorized access, theft or loss is vital to the network security of an organization. Ensuring that company data is not merged with employee personal data, and that data is recovered and deleted from devices once an employee’s contract with the organization is
terminated are more factors that can complicate data security. According to Pettey and Van Der Meulen (2012) users may most likely reject the approach of a company attempting to wipe data from their device remotely, or encryption of data on the device. Any attempt by the organization to force such implementations may be considered as an encroachment on their employee property privacy.

3. **Device type and Acquisition** - Marshall (2014) stipulates that certain organizations may restrict the device type or device model that employees are allowed to utilize for the BYOD technology implemented in the organization, some organizations may request that only a particular set of devices from a specific manufacturer are allowed, either because of security risks, hardware interoperability concerns, or a requirement for particular applications that only run on particular devices (Marshall, 2014). Research done by Marshall (2014) reflects that at the Ottawa Hospital in Ottawa, Canada, the BYOD technology implemented is restricted to only Apple devices, because the mobile versions of the organization's clinical and electronic health record applications were developed for Apple devices only. Situations like these affect the support of a device owned by an employee by the organization the employee works for. For BYOD to be successfully implemented, organizations have to support a wide range of devices, considering the cost imposed on the employee for device acquisition, and the employee’s desire for certain types of devices that may be more convenient for them. Some employees may find it very challenging to acquire their own device due to cost of acquisition, this can also affect the implementation of the BYOD technology.
Network Security Breach Simulations
A Study done by Kohli (2016) revealed that 24% of organizations implementing BYOD confirmed that they are aware that the BYOD devices have been exposed to malicious Wi-Fi networks, while 48% of organizations are unaware of any exposure that may lead to security threats on their BYOD employees devices. In this regard, a simulation was done to show an example of how an attack can be carried out on a network in an organization that implements BYOD. This is illustrated using the Adsetts library of Sheffield Hallam University as a case scenario, in the Adsetts library students bring mobile devices such as smart phones, tablets and laptops to connect to the university’s network. The software used to simulate the attack is called COLASOFT CAPSA 9. A laptop device was connected to the network of the library and the software in the laptop was launched to begin the process. The figures, 1,2,3,4 & 5 below depict the details of a simulated attack carried out to get details of all the mobile devices at the library connected to the wireless network.
Figure 1

The software shows the various connection types and the connection selected is Wi-Fi because the BYOD technology is a technology based on wireless connections for the devices.

The software has a tool called MAC scanner, what this tool does is to scan the entire network in a particular building and retrieve the details of every device connected to the network in the building.
The picture above displays the details retrieved with the MAC scanner tool, the IP addresses of the devices, the MAC addresses, the Host names, Workgroup, Manufacturers. On top of the page, the subnet details for the organization network are displayed as: 10.65.192.0/255.255.252.0, and the bottom of the page shows the number of hosts currently connected to the network, it found 127 hosts connected at that particular time.

These details acquired can enable a hacker to carry out dangerous attack on an organization network, attacks such as DHCP starvation, DHCP spoofing, Denial of service and the likes. The hacker can easily retrieve company data and valuable information in this kind of situation.

The following pictures show more details of the communication between hosts on the network such as the packets size, speed, and some more statistics.
Figure 3

Figure 4
This last picture shows the IP address of devices communicating with the port number and the various protocols involved;

Figure 5

These illustrations show that a hacker with this kind of software can scan an entire network in a building to reveal all the necessary details, needed to hack any network not properly secured just as can be seen from the illustrations above. With these illustrations, it becomes clearer that severe damage can be done on a network implementing the BYOD technology, if not well secured according to set policies and several other factors. This also shows that security of information is of utmost importance in BYOD scenarios, especial when employees cannot differentiate properly from work and personal life settings.
Possible Mitigation Techniques of BYOD Security Risk

There are certain mitigation techniques that can be implemented to tackle the security risk associated with the BYOD technology. Some of them are as follows:

1. **Company BYOD Policy:** The companies that implement the BYOD Technology need strict policies in place to govern the technology. According to Lord (2016), companies ought to have a BYOD policy that utilizes Mobile Device Management (MDM) which grants or revoke access to mobile devices that can connect to the corporate network, perform a remote wipe on missing devices, and putting in place strict protocols for remote access to the organizational network.

2. **Regularly Educating and Updating Employees on Security Measures:** Employees should be given regular periodic training on how to implement company security measures on the devices being deployed for the BYOD technology.

3. **Network Maintenance:** Certain security measures need to be put in place such as mandatory security protocols for network access, regular backup of data and high level of data encryption for sensitive data, perpetual testing of the security of the network and its systems, so as to discover the loop-holes that need fixing to improve the network strength.

4. **Choose Your Own Device:** Choose your own device (CYOD) is a type of BYOD technology where the organization provides the mobile device for the employee rather than the employee providing his/her own device. The major difference is that the organization provides a variety of devices for the employee to choose from. The main advantage of this is that the organization can implement whatever security policies they need to protect
the device effectively and create more efficiency security-wise. For CYOD, the organization knows exactly how many devices each employee utilizes for work purposes and how much pressure the network has to handle (Brodin, 2016). The organization also gets a higher level of control over that device in comparison to the employee’s personal device; this can result in a better control on the network and a tighter grip on the security of the network.

Conclusion
The BYOD technology brings more flexibility to organizations, it facilitates the achievement of organizational goals in the long run, and it is very beneficial to both employees and organizations. BYOD has proven to be a technology that increases the level of flexibility and work efficiency, while also reducing cost for organizations and maximizing profits, amongst other things. However, the major challenge of security is one that cannot be ignored; it requires strict policies, aggressive tackling of network loopholes and the building of resilient, iron-guarded network. Adequate measures are needed to be put in place and safety precautions needs to be strictly adhered to in order to achieve the best of the BYOD technology.
Recommendation
After careful considerations of security risks of BYOD, the following were recommended:

1. Companies that implement the BYOD technology need strict policies in place to govern it.
2. It is important that a type of BYOD called choose your own Device (CYOD) is implemented so that the organization can implement whatever security policies they need to protect the device effectively and create more efficiency security-wise.
3. Employees should be given regular periodic training on how to implement company security measures on the devices being deployed for the BYOD technology.
4. It is necessary to put in place mandatory security protocols for network access.
5. It required to regularly backup data.
6. High level of data encryption for sensitive data should be implemented.
7. Perpetual testing of the security of the network and its systems, so as to discover the loop-holes that need fixing to improve the network strength should be carried out.
8. Employee’s access to sensitive data should be restricted.

References


