Is Bring Your Own Device an institutional information security risk for small-scale business organisations?

Kudakwashe Madzima
Computer Science Dept
University of Venda,
South Africa
kmadzima@univen.ac.za

Moses Moyo
School of Computing
University of South Africa
South Africa
mosesm50@gmail.com

Hanifa Abdullah
School of Computing
University of South Africa
South Africa
abdulh@unisa.ac.za

***Abstract* - The use of employees' own mobile devices, under the pretext of 'bring your own device' (BYOD), to access vital information assets has far reaching implications for an organisation's information security. BYOD is a potential solution to information technology budget constraints and also a means to increase employee satisfaction regarding the usage of one's own devices at the work place. This practice challenges the conventional philosophy that only an organisation's devices should be used to access critical organisational information. However, BYOD practice has security concerns associated with it. An organisation that adopts BYOD may find it difficult to account for and manage the various devices employees may use, and control how those devices are used. There are fears that some small-scale organisations may adopt the BYOD strategy too soon placing themselves and their data at risk. BYOD could be an additional security problem which an organisation has to contend with.**

This paper acknowledges the positive contributions that BYOD could make to organisations. It also discusses the bases on which BYOD could be treated as an institutionalised information security risk for many small-scale organisations which adopt it. The purpose of this paper is to critically analyse and assess both the benefits and risks associated with BYOD that may militate against its adoption by small-scale organisations in emerging economies. The paper also seeks to establish whether BYOD is an institutionalised information security risk or not.

Keywords - Bring your own devices (BYOD), small-scale organisations, information security, risks and institutional risks.

I. INTRODUCTION

In today's world, mobile devices such as smartphones and tablets are the most common medium used all over the world to access all sorts of electronic systems for corporate or personal use. The quest for enterprises to increase collaboration among its employees and their productivity is now practically achievable through the use of laptops and mobile devices that employees can easily access. Given the affordability of mobile devices, they are increasingly finding their way into people's lives and hence into the work place. This has also resulted in a rise in the number of employees who use their own devices to do their personal work or even company work. This is a new trend that has developed in which employees prefer their own devices to company devices, and is called bring your own device (BYOD).

Given the capabilities and functionalities offered by mobile devices, most employees who own these devices also feel they can rely on these devices just like they traditionally would rely on their work computers. Some organisations actually provide employees with mobile devices to use at home, others actively or passively encourage employees to bring their own devices to use at work and even use them to access critical information assets such as the network, databases and other applications. This promotes the practice "Bring your own device" BYOD in many organisations today.

This increase in the adoption of computing devices, from laptops to smartphones and tablets by individuals, and their influx into the workplace might bring convenience and increased productivity to individual employees but with this BYOD trend also surfaces new range of security challenges for organisations. Hence the use of employees' own mobile devices, under the pretext of 'bring your own device' (BYOD), to access vital information assets such as e-mails, databases and networks has far reaching implications for an organisation's information security. Securing corporate networks and data, mobile device management, and implementing security controls and policies that cater for corporate and employee devices becomes a real headache for the IT administrators and it can be worse for those who work on small scale organisations.

Besides the larger companies realising the value of the BYOD concept, smaller companies or start-ups are also buying into this idea and incorporating it into their business strategy [1]. However, these small scale organisations may lack the technical know-how in implementing proper security strategies and the adoption of BYOD presents real security challenges and this may really compromise their information systems security. The new risks this ecosystem poses need to be studied and understood in order to create security strategies that can effectively protect 1) the users, their devices and their data and information and 2) corporate systems, devices, data and information.

In the next section we give a brief definition of BYOD, in section III we summarise the factors favouring BYOD

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

adoption, section IV looks at the promises, section V presents the key issues and challenges of BYOD, section VI then looks at the resonating questions of BYOD, and lastly, we present our conclusions.

II. BYOD DEFINED

BYOD (bring your own device) sometimes called BYOT (bring your own technology) or "the consumerisation of IT" is the practice of allowing employees to bring to workplace their own mobile devices that are capable of connecting to the Internet. BYOD allows employees to use personal devices for work-related activities. The devices can include laptops, netbooks, tablets, smartphones, Portable Digital Assistance, e-readers and gaming devices [2]. BYOD also refers to company policies drawn out to enable employees to bring their personal mobile devices, such as smartphones, laptops and tablets, to their place of work and also make use of them to access data and information exclusive to the company they work for [3]. Basically BYOD is an approach whereby employees of an organisation use their own ICT equipment to do their job rather than equipment provided by their organisation.

BYOD is increasingly gaining popularity across all sizes of business, from small scale organisations to large corporates and this is mainly due to the fact that BYOD enables employees to use mobile devices of their choice. This leads to a reduced IT investment on the part of the business. Most small scale organisations usually have very small IT budgets and so BYOD seems a very attractive approach to solving device problems.

III. FACTORS DRIVING BYOD ADOPTION

These days many employees own better and more capable devices than what can be found in their offices or what can be made available to them by their IT departments. There is a growing trend of employees always going for the latest mobile technology on the market. The devices are now seen more and more as fashionable or trending. They are now somehow influencing people's perceptions on lifestyle. Some people see the devices as a reflection or definition of one's social class or status and Osterman Research in [4] uses the term 'Executive Jewellery' to refer to these devices. For example by mid April 2014, some employees already had the Samsung S5 that was recently launched here in South Africa. However in small scale organisations the devices can be seen as luxury items.

Osterman Research in [4] argue that many IT departments cannot afford the latest and greatest hardware because of tight IT budgets. This means that the IT departments are somehow caught in between forcing employees to stick to the use of old corporate computing equipment versus allowing them to use their latest technology. According to McQuire in [5] many companies are realising that the BYOD practice is already happening and the perception is that it cannot be stopped. The same author argues that organisations feel that BYOD, if deployed to the correct work style, can expand mobility access to a wider number of workers thus enabling the organisation to capture productivity and agility benefits on a greater scale.

As pointed out in [5] another important contributing factor is the growing trend for employees to have an expectation of always being connected and of always having access to all of their work-related and personal content on a mobile device or in the cloud. Hence, the increased number of requests to IT departments, for personal devices to be connected to corporate networks. Some IT departments, as pointed out in [4] are embracing BYOD tactically and using it as an opportunity to have more diverse, multiple mobile operating system environments in their organisations. Another important contributing factor is the continuously increasing number and availability of personally deployed and managed applications for mobile devices. Users can easily access these applications with ease.

McGuire in [5] argues that many of these tools (cloud based apps, mobile apps and other tools) permit employees to be more efficient or they provide supplementary capabilities that IT departments cannot or will not implement. Some services provided by these tools include email services, cloud-based file storage and synchronisation, content collaboration, ability to transfer large files, etc. IT departments may not deploy or support such services usually due to a constrained by budget or due to bandwidth limitations.

Osterman Research in [4] found out that some organisations are using the BYOD hype as part of their corporate strategy to deal with their competition on issues of employee recruitment, retention and satisfaction by being 'Employer of choice'. This way BYOD could to some extent help them to win "the war on talent". In justifying the popularity of cloud- based tools Osterman Research [4] argued that some users are simply not satisfied with the capabilities offered by their IT departments and so want to provide their own superset of features and functions that will make them more efficient and productive.

IV. THE BYOD PROMISE

BYOD can be a good thing [4]. BYOD has a high potential of reducing costs for IT equipment, increasing employee satisfaction and productivity and catalysing the rate of technology adoption in the enterprise [4], [6]. Brooks in [7] cites three major reasons for an organisation to encourage BYOD, namely, boosting productivity, cost reduction and improving employees' morale. For smaller organisations that may not be able to afford latest technology, BYOD enables employees to still use technology without cost to the company [8]. With the BYOD environment, mostly the employees willingly supply the devices (smartphones and tablets) and also the applications that they will use in doing their work and this in turn greatly reduces the overall IT costs for the organisation. It is assumed that when small scale organisations adopt and implement a BYOD strategy they technologically empower their employees.

The aspect of employee working efficiently is possible in the BYOD era because they are continuously connected to their work anytime and from anywhere. A contributing factor to this is that employees will no longer need to stay behind in their offices till late because they want to finish their work. They can leave office early and still be able to work from anywhere as long as they can connect. This leads to improved employee productivity. Most users can be more efficient and effective in their work if they have capabilities that give then access to all

their files, communication tools and other services from any platform or any location [4].

BYOD adoption allows for a diversity of mobile operating system environments within organisations. There is evidence [4],[9],[10],[5] that in today's world mobile technologies are changing the way people work. Mobile technologies are now assuming a new role as they are now the primary platform for many employees, enabling them to get their work done faster and probably better through access to the right tools and technologies from wherever they are. BYOD has a competitive advantage appeal. Some organisations would want to be amongst the first adopters or leaders. Osterman Research found in [4] that one-half of companies surveyed saw mobile as truly transformative, a way to get ahead of the competition and maintain competitive advantage. This means that companies are probably viewing the adoption of BYOD or mobile devices as an aspect of innovation.

With the BYOD environment employees have some power and freedom to select the device and possibly application which they will use to do their work unlike having to use a device with which they are not comfortable or familiar. This can positively boost employee morale and retention. Employees who are permitted to use their own devices and applications will likely have higher morale and will be less likely to seek employment elsewhere [4]. Employees who are comfortable are more productive and efficient [1].

V. KEY ISSUES AND CHALLENGES POSED BY THE BYOD CONCEPT

Today, businesses and their IT managers must balance the desire to give employees the freedom to use a range of devices, including ones they own (BYOD), to access company network resources against the very real threats those devices pose to the health and safety of the network and its data assets [9]. According to [6], the BYOD trend is one of the more dramatic results of the consumerisation of information technology (IT), in which consumer preference, not corporate initiative, drives the adoption of technologies in the enterprise. The danger is that most of such technologies were not designed with enterprise requirements in mind; therefore, information technology teams are sceptical about security and supportability of these platforms.

From an information security standpoint, BYOD has some security implications for an organisation. Enterprises that adopt BYOD face challenges on how to manage employee owned devices [10] . This may compel enterprises to put in place mechanisms on how to distinguish employee-owned devices from those of the organisation and manage them separately. The portability, communication and storage features supported by hardware and software components of mobile devices may give a sense of privacy, and even anonymity, to the millions of users that every day share family pictures, activity calendars, professional profiles and other personal information online but this sharing is not without the risk of the user's privacy and security being compromised [11].

The use of a single smartphone or tablet to store and process personal as well as business information presents a serious security challenge to the employer and potential privacy concern to the end-user. The fact that most of these devices are employee owned means that the employers may not have full control over these devices yet they want to allow organisational data to be on these devices. Any form of control may lead to employees feeling uneasy and worrying about being watched.

However, small to medium scale organisations that adopt this practice are bound to face more security challenges in their daily operations. Most small scale organisation lack technical know-how in implementing security techniques and as a result their information systems security may be compromised with BYOD adoption. In the section below we discuss some of the challenges and possible approaches.

VI. RESONATING QUESTIONS ABOUT BYOD

Unlike other strategies that arise from enterprise demands, BYOD is driven by consumerisation and hence presents a new dilemma that requires new approaches to an organisation's information security risks. Therefore, this paper addresses the following questions about BYOD which will give the reader a clearer insight into the issues lying deep below this new practice.

A. To what extent should BYOD be practised in small scale organisations?

BYOD is now a common practice in different organisations regardless of their sizes. However, the extent to which BYOD is utilised productively is a matter of speculation. An organisation can utilised BYOD in a number of ways as discussed below:

- *BYOD - corporate devices hybridisation*: In this situation, employees are given a chance to choose the device that the employer provides them with. The fact that employees already own some devices that they use at home, and have found them reliable may make them see no need to get the same devices from the organisation. Instead they advise the organisation to buy alternative devices. A good case is a situation where an employee owns a laptop but does not have a smartphone; the employee may ask the employer to buy the smartphone. In this case hybridisation takes place in that the employer owns the smartphone and the employee owns the laptop. The owner is expected to responsibly use the smartphone and the laptop as if they are all theirs.
- *BYOD adding to corporate devices*: Some employees hardly have access to corporate devices because the corporate cannot provide adequate devices. To alleviate shortages, the corporate may permit the use of employee-owned devices for individual employees who cannot have exclusive access to an enterprise device. The corporate may also pool available devices and redeploy its devices to those employees who do not bring their devices. This helps to optimise the utilisation of devices in the corporate as those devices which were underutilised will be redeployed to those who need them. Allowing employees to use their own devices and applications may also create a range of problems for the IT department. Many IT departments

have not implemented the processes and tools necessary to support users who are employing their own devices and applications [4].

- *BYOD replacing corporate devices:* An enterprise can replace its own devices with employee-owned devices. This has implications to the organisation and to the employees whose devices are being used. When a corporate replaces its own devices with those owned by its workers, it runs a big risk of control. Control of devices is easier when the devices are owned by employers, although the employee is free to use the device for private use as well issues of privacy and monitoring will still arise.

B. *What information security risks will BYOD bring to an enterprise?*

Proponents of BYOD strongly argue that BYOD trend is likely to change the hardware and security landscape in the enterprise world permanently [12]. By embracing BYOD, small scale organisations increase the use of mobile devices and mobility of their workforce, this situation raises new security concerns and requirements. This means that demand for remote access to organisations' data and information grows forcing organisations to safeguard off-premises applications and data, as well as an array of new client devices [13]. BYOD practice allows more flexible access to the corporate network and data, something that makes most IT administrators feel uncomfortable with and as a result are obliged to protect data and information blocking the adoption of workers bringing their own devices to work.

Ruggero Contu in [13] also argues that the evolution of new threats and working practices, such as BYOD, is driving spending on security. This puts organisations with budget constraints at a worse financial position than before adoption as more funds will be channelled towards securing information systems. In this instance, organisations that provide security thrive at the expense of those they are supposed to secure. BYOD practice is likely to complicate the existing security situations in small scale organisation where there is already a shortage of information security personnel.

We discuss the security risks associated with BYOD below.

1) Malware

Mobile devices in an enterprise are always prone to a variety of information security threats if left unmanaged in a networked environment. Cisco Security in [14] argue that online attackers have devised new methods for embedding their malware in networks, remaining undetected for long periods, and stealing or disrupting critical systems. Such threats may include exploits by malware targeted at the device's operating system or applications; unauthorised connections; exploitation of software vulnerabilities by malware that exposes data or causes unexpected behaviour; and compromise or irrecoverable loss of corporate data. Some of the employee owned devices are used to access the internet and social network sites, emails, downloading data from the internet, etc. Therefore, BYOD practice is likely to expose an enterprise to malware attacks which are difficult to detect in time. These security risks can affect the integrity, availability and confidentiality of corporate information and data. The Cisco Security in [14] argues that cybercriminals and their targets share a common challenge for they both try to find out how best to use BYOD and mobility trends for business advantage. However, the criminals have an advantage due to two factors namely: the maturation of mobile platforms that make mobile devices to resemble traditional desktops and laptops that makes it easier for cybercriminals to design malware for them; and the frequent downloading of mobile apps by users without thinking about underlying security issues [14]. Viruses and worms intended to access confidential data from various mobile platforms are always being developed. Most of the mobile devices are exposed to these security risks by ignorant users. Small-scale organisations will certainly fail to cope with such challenges. Under these security risk situations it becomes extremely difficult for a small scale organisation to manage all the types of mobile devices considering their budget constraints. This makes BYOD an institutionalised security risk which small scale organisations need to assess and evaluate before blindly embracing the practice.

2) Data theft and leakage

BYOD always brings about changes in the manner a corporate stores data and how it is likely to be accessed by non-corporate devices. This means that BYOD and mobility now offer new ways users and data could be compromised. For devices on the network, criminals can use many hacking tricks to break into the system and compromise the whole data. Lack of proper security techniques to detect and deter hackers might hamper the organisation's reputation and cause a great loss to it. Under such circumstances an organisation can easily lose intellectual property and sensitive data if an unsecured employee owned device is lost or stolen. A laptop with corporate data can easily be stolen or the authorised users give access to unauthorised users whose intentions are to sabotage an organisation. Employees can forget mobile devices in public places during rush hours. It is reasonable for enterprises to expect a lot of data leakages that may occur due to BYOD but some of the damages may be irreparable to an organisation. This makes mobile devices and BYOD be liabilities from a corporate standpoint owing to theft and potential loss. Therefore, corporate data stored on BYOD is highly susceptible to espionage.

3) Software bugs

Mobile devices and laptops require regular software updates for operating systems and applications. This could be the least thing for employees to worry about. The implication is that these devices will lag behind in software updates thereby creating security loopholes. Secondly, employees may install as many applications as they want on their devices. There is a security risk in that employees may install applications with undetected bugs or malware. In this way BYOD exposes an organisation to information security risks that will compromise the availability of data and information through system crashes or malware infections.

4) Network access

Small scale organisations that embrace BYOD end up opening access to their networks for non-corporate devices. An increase in the number of employee owned devices that get connected to an enterprise network may also imply an increase

in network security risks. In the first, place it is difficult for a small scale organisation to decide which employees can use own devices to access the enterprise network, and also what they can access once on the network. These BYOD devices will become the security weak link through which cybercriminals will launch attacks to an enterprise information system. Some of the devices connected to the network may have flaws. Therefore, if an enterprise network has many operating devices, it becomes difficult for IT personnel to detect those devices which have flaws [14].

5) No control over what is on employee devices

An enterprise may have no control over the types of applications on their employees' owned device making it somehow difficult to enforce security. The enterprise has no power to stop an employee from downloading numerous types of personal applications on their device. BYOD makes it difficult for an organisation to enforce standard security as device owners may be not prepared to cooperate with the organisation in areas of security. Despite the promising benefits of BYOD, this practice is likely to pose significant threats to small scale organisation's information security. Personal devices for BYOD use a variety of technology, applications and operating systems, therefore their security is not guaranteed. It could be argued that an enterprise which embraces BYOD practice is relinquishing control of its data and creating a potential security nightmare [15].

6) Bandwidth problems

Bandwidth is another problematic area in an organisation where BYOD is practiced. Most employees will want to use Wi-Fi for BYOD connectivity to the enterprise network. The network may fail to cope with the amount of devices connected to it making some essential devices slow thereby affecting an enterprise's business objectives. For an enterprise which depends own 3G/4G, coverage and performance become real issues of concern due to connectivity problems.

7) BYOD practice's overlooked security risks

BYOD practice can increase the risk of having a security breach on an enterprise's important data. Small scale organisations tend to overlook important security issues that will arise in the event that employees leave the organisation. If employees leave the enterprises that have adopted BYOD, the employees take with them their personal devices. An enterprise may not have time to remove corporate data and applications from these devices. This implies that the enterprise's data is no longer secure. The ex-employees can still use their devices to access their former employees' data and information using their devices making the enterprise data unsecure. By allowing many BYOD devices an organisation may fail to comply with essential regulations governing the use of electronic devices by business organisations.

In light of the foregone discussions on security issues related to BYOD practice, there are constraints that may militate a small scale organisation from implementing BYOD. The following subsection discusses the constraints that may militate against the implementation of BYOD in small scale organisations.

C. What constraints could militate against the implementation of BYOD by small-scale organisations?

Small and medium enterprises are struggling to keep IT infrastructure up to date with mobile working and the increasing volume and sophistication of cyber threats [15]. As small scale organisations increase their adoption of technologies such as mobile devices and the cloud they realistically face more security challenges from cyber criminals who use malware that are dormant while entering a secured network and then become active. BYOD exposes an organisation to more security challenges and complexities [16]. Small scale enterprises that want to implement BYOD may face the following constraints:

- Lack of control on what to let users access when they use their own devices. Instead of using the BYOD devices for corporate purposes, employees could be using them for social networking purposes.
- Lack of control on the number of employee owned devices each user may bring can be a headache to the enterprise. Employees may start to compete in the number and types of devices to bring to work.
- Inconsistencies in the devices which employees may bring can give an organisation some unanticipated problems. Employees may borrow their friends' devices which are used in other BYOD settings. This may also lead to compromises of data and information of an organisation.
- Lack of trust on who will access the device away from work and what corporate information will be accessed. Employee owned devices cannot be trusted with corporate information. They are more exposed to abuse at home than at work. Data integrity and confidentiality are more likely to be compromised at home than at work.
- An enterprise has little control over employee owned devices. For example, an employee who has access to key enterprise data and information may leave the device at home, sell it, give it to a friend or have it stolen.
- Data and information can be stolen from mobile devices while in transit or left unattended, or through deliberate switching of devices by thieves.
- Most employees lack information security awareness and as a result most of the personally owned devices that they may bring to work are often used in ways that would never be acceptable if they were enterprise-owned devices.
- Inability of small scale enterprises to provide proper risk management for fast changing computing environment is another challenging aspect of BYOD

BYOD functionality may leave the organisations exposed to many risks. Regardless of the mentioned constraints, BYOD has caught up with the majority of the organisations. Small scale enterprises should strive to overcome these constraints in order to implement BYOD in the most appropriate way they

see fit. The following subsection discusses ways by which small scale enterprises can implement BYOD.

D. How best would small scale enterprises adopt BYOD without compromising their information security postures?

According to Solomon in [17] , mobile security has become the mainstream problem and mobile device users expect more from their IT and security programmes. This calls for concerned organisations to exert some form of control over how employees use their personal devices in the workplace and at home. An enterprise could put in place a number of strategies that can possibly make the use of BYOD security friendly to the concerned enterprise. These include the following:

- *Training employees on BYOD*

  Data security may remain one of the key challenges of BYOD but there are other equally significant barriers that enterprises should address [18]. Time for training employees has never been a priority for small scale organisations. There is a dire need for enterprises to train employees on BYOD-related security risks [18].

- *Designing and Implementing a BYOD policy*

  Policies have always been regarded as the good starting points for gaining and exerting control on an enterprise for they provide the framework for formalising guidelines for BYOD adoption and the use of employees owned devices. According to Burgess in [19], technological solutions can hardly stand alone; there is a need to combine them with appropriate BYOD policies, those policies that protect the enterprise's intellectual property, trade secrets and customer data. A good policy should neither be overly restrictive on how employees may use their device nor overly relaxed to the extent of granting the enterprise access to the employee's personal data. A BYOD policy will specify the types of devices that an enterprise permits, procedures followed to authorise the use of the devices.

  Armed with a policy, an enterprise would know what to do in the event that a device is lost, an employee resigns from the company, and also how to manage data and network access for all the BYOD devices. A BYOD risk policy is likely to improve compliance by educating employees the risks associated with their devices. It will be easy to implement certain rules and practices. Overall, a good policy is an aid that helps to clarify pending risks and to govern employee-owned devices [18].

  BYOD policy can be supplemented by Terry Greer-King's three-step process: audit, amnesty and adding security [12]. According to Gebreel in [12], this process can be implemented as following:

  1. Auditing devices – this is intended to establish all devices it uses to handle corporate data including those owned by its employees.
  2. Amnesty – the Enterprise IT personnel tell employees which personally owned devices they should bring to be added to the enterprise networks and security features.
  3. Adding security – Enterprise IT personnel configure all employee owned to devices to meet enterprise security requirements.

- Tolerate, provide or clamp-down approach to BYOD

  The final discussion of possible ways of adoption BYOD by small scale organisations could take the form of the model suggested by Deloitte in [20], tolerate unmanaged BYOD, provide a managed BYOD programme and attempt a clamp down on unmanaged BYOD. The basic underlying principle of this model is to bring order to BYOD practice in an organisation. An organisation such as an academic institution can tolerate unmanaged BYOD to some of its non-critical areas like accessing the Internet using students' personal devices. The institution can provide managed BYOD for a group of workers in some critical areas. Any unmanaged BYOD could be clamped if it attempts to access critical assets like account information systems or records management information systems. However, the problem with clamping down is that it drives BYOD underground thereby increasing the risk the unmanaged BYOD infiltrating the critical information systems of the organisation.

Contrary to this, Lui in [21] argues that for BYOD policy to function effectively there should be no restrictions placed on which device employees can bring into the company but specify the minimum requirement that all personally owned devices have to meet.

It is our view that at the stage of BYOD policy formulation, there is need for the enterprise to understand how employees owned devices will be used and how they will be linked to the corporate networks. There is also need to clarify in the BYOD policy how the employee owned devices to be connected on the network will interact with the corporate's existing IT infrastructure and systems. Information security risks envisaged should be identified so that the enterprise develops security practices that best reflect the risk management profile which is compatible with the needs of the business to operate effectively. An enterprise which anticipates adopting BYOD needs to provide sufficient training to its managers and employees so that they are well informed of the risk, aware of the boundaries set on the employees and on the employer in the agreed policy. This is intended to make sure that the parties involved act consistently and act appropriately to any risk situation likely to occur.

Finally, we suggest that the BYOD policy should provide evidence of employees' knowledge and agreement to the use of their personal devices to perform enterprise work. It is also important that the enterprise BYOD Policy covers areas of potential conflicts between the employees and employers.

VII. IMPLICATIONS OF THE PAPER

Although BYOD may have overwhelming advantages to an enterprise, it remains an institutionalised information security for small scale organisations. By accepting BYOD practice, an enterprise implicitly accepts the risks associated with it. It can be assumed that all risks likely to be experienced due to BYOD are "official risks".

Organisations should put thorough considerations prior to the adoption of BYOD so that whatever consequences that are likely to arise from the practice cannot be apportioned to employees. It has been demonstrated that the big risk factor for organisations with BYOD practice is the loss of control over the devices being used by employees to access corporate information systems something which the organisation would have implicitly institutionalised. Most enterprises are left in the dark pertaining to what data are stored on the employee owned devices, the type of data security vulnerabilities and risks they are exposed to, and how to secure access to their networks. Once an enterprise loses control over its networks, through devices accessing its data through the BYOD practice, it becomes automatically prone to a host of privacy and data security issues. Overall, data confidentiality, integrity and availability are compromised.

On the other hand, all employees who voluntarily bring their personal devices for use at work should share control of these personally-owned devices with an enterprise so that both the device and data are protected by the enterprise. The employees may be obliged to allow the enterprise to access the employee owned device without compensation. There, however, could be a risk in that the enterprise may access an employees' private information, or change configurations to lock the owner out of the device or even delete all employee data from the device.

Once an enterprise adopts BYOD the IT and Security personnel should be compelled to review security measures frequently and thoroughly. The enterprise should ensure that its data is well protected by frequently monitoring its active email accounts, virtual private networks, intranet applications and databases to detect unauthorised access and suspicious activity. Access to confidential data whether for an enterprise or employee owned device should be secured and only accessed through proper authorisation and authentication procedures.

Batters in [22] concurs with our fears that BYOD is an institutional information risk by saying that while many organisations believe that they have sound security measures in place, the reality is that often these are implemented in a piecemeal way with point solutions only addressing specific needs. However, this disjointed approach is not sustainable. Therefore, it would be futile for an enterprise to blindly embrace the BYOD practice due considerations in existing data security challenges and those that will be imposed on it by BYOD.

VIII. CONCLUSIONS

Despite the benefits of BYOD, security remains a huge concern and factor that may hinder adoption. BYOD and its related mobility trend require organisations to rethink their information security policies and procedures in order to ensure that their sensitive corporate data does not become vulnerable to a variety of breaches [8]. The bottom line is that, through BYOD, employees are significantly influencing the tools that are deployed in the enterprise and this brings with it more satisfaction on the part of employees and in turn more productivity in their work [4].

Basically, it is assumed that when small scale organisations adopt and implement a BYOD strategy they technological empower their employees thus simultaneously institutionalising inherent BYOD security risks. However, many organisations are still sceptical about adopting BYOD although it may be practised with or without the management's knowledge.

By adopting BYOD, an organisation will be compromising security of its systems to a large extent. At the same time, IT departments are forced to make major adjustments in order to support the strategy. Rather than support a predictable set of standard devices and applications, they must now cope with rapidly changing hardware, operating systems, applications, and even an array of service providers and plans. Increasingly, their approach must be to guide and influence rather than to dictate and control.

Given the rate at which people are adopting and using mobile devices (smart phones, tablets, etc.) organisations need to carefully re-design their security policies so that they incorporate strategies such as our proposed device hybridisation (see section VI A). Clamping down and forcing employees to stick to the use of organisation IT infrastructure and applications might also not be the best way to deal with the problem. Osterman Research in [4] found out that many leading "consumer focused" applications had been deployed by IT, but quite often they are deployed without IT's knowledge or consent.

There is no single agreed model to BYOD adoption that an organisation can implement, therefore, a BYOD practice should be influenced by an organisation's technology culture. There are many constraints that can prevent an organisation to prematurely adopt BYOD as demonstrated above. Organisation should put paid BYOD strategies before institutionalising inherent information security risks.

REFERENCES

[1] Srilagna, S. (2013), "BYOD gaining popularity among small companies," TJinsite, [Online]. Available: http://content.timesjobs.com/byod-gaining-popularity-among-small-companies/. [Accessed: 07-May-2014].

[2] Evans, D. (2013), "What is BYOD and why is it important?". [Online]. Available: http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088#null. [Accessed: 07-May-2014].

[3] Viswanathan, P. (2014), "Bring Your Own Device (BYOD) Definition". [Online]. Available: http://mobiledevices.about.com/od/glossary/g/Bring-Your-Own-Device-byod-Definition.htm. [Accessed: 07-May-2014].

[4] Osterman-Research. (2014), "Living With BYOD in Your Organization".

[5] McQuire, N. (2012), "Global BYOD Attitudes and Best Practice for Multinational Organisations".

[6] MobileIron (2011), "Building 'Bring-Your-Own-Device' (BYOD) Strategies". [Online]. Available: http://www.webtorials.com/main/resource/papers/mobileiron/paper1/byod_part_1.pdf. [Accessed: 05-May-2014].

[7] Brooks, C. (2013), “What is BYOD (Bring Your Own Device)?,” BusinessNewsDaily, May 22. [Online]. Available: http://www.businessnewsdaily.com/4526-byod-bring-your-own-device.html . [Accessed: 20-Apr-2014].

[8] Mitchell, F. (2014), “Safeguarding your corporate information in a BYOD world,” IT News Africa, April 30 2014. [Online]. Available: http://www.itnewsafrica.com/2014/04/safeguarding-your-corporate-information-in-a-byod-world/. [Accessed: 30-Apr-2014].

[9] Symantec (2012) “Meeting Mobile and BYOD Security Challenges”.

[10] Webb, G. (2012), “BYOD & BYOC Security Concerns may Change Everything”. [Online]. Available: http://www.cioupdate.com/technology-trends/byod-byoc-may-change-everything-about-security.html. [Accessed: 06-May-2014].

[11] Mandujano, S. (2013), “Privacy in the Mobile Hardware Space: Threats and Design Considerations.” [Online]. Available: http://www.mostconf.org/2013/papers/11.pdf. [Accessed: 17-Apr-2014].

[12] Gebreel, A. (2014), “Identify and exploit the opportunities of BYOD”. [Online]. Available: http://www.microscope.co.uk/feature/Identify-and-exploit-the-opportunities-of-BYOD. [Accessed: 07-May-2014].

[13] “Global security software market revenue reached $19.2 billion in 2012” The Economic Times, New Dehli, 2013.

[14] Cisco. (2014), “Annual Security Report”.

[15] Ashford, W. (2012), “SMEs struggling in the face of BYOD and new cyber threats” Computerweekly. [Online]. Available: http://www.computerweekly.com/news/2240157952/SMB-struggling-in-the-face-of-BYOD-and-new-cyber-threats. [Accessed: 28-Mar-2014].

[16] Cisco. (2014), “Cyber criminals using malware that act as sleeper cells,” PTI Times Internet, Mar-2014.

[17] Solomon, M. (2013), “Threat-centric security: Before, during and after an attack”.

[18] Qing, Y.L. (2013), “BYOD on rise in Asia, but challenges remain,” ZDNET. [Online]. Available: http://www.zdnet.com/byod-on-rise-in-asia-but-challenges-remain-7000010660/. [Accessed: 28-Apr-2014].

[19] Burgess, C. (2013), “Absent Appropriate BYOD Policy, Individual Users May Be IT’s Worst Nightmare”.

[20] Deloitte, “Understanding the Bring-Your-Own-Device landscape A Deloitte Research report,” 2013.

[21] Lui, S. (2013), “Case study: How Dimension Data is reaping the benefits of BYOD,” ZDNet. [Online]. Available: http://www.zdnet.com/au/case-study-how-dimension-data-is-reaping-the-benefits-of-byod-7000010457/. [Accessed: 29-Mar-2014].

[22] Batters, R. (2013), “How Secure is Your Organisation?”. [Online]. Available: http://letstalk.globalservices.bt.com/en/security/2013/06/how-secure-is-your-organisation/. [Accessed: 11-Apr-2014].