Introducing BYOD in an organisation: the risk and customer services viewpoints

Zoran Mitrovic, Ivan Veljkovic

(University of Western Cape, South Africa)

Grafton Whyte

(Polytechnic of Namibia, Namibia)

Kevin Thompson

(Mitrovic Development & Research Institute, South Africa)

ABSTRACT

With the recent technology advances and the rapid adoption of tablet computers and smartphones, it has become increasingly common for employees to use their own personal devices to perform various tasks in their work-place. This phenomenon is better known as Bring Your Own Device (BYOD). This new concept is seen as twofold: as not that simple to handle and, at the same time, many organisations are quickly adopting BYOD as it has been shown that it offers many positive effects such as increased job satisfaction, employee morale, better productivity and consumer services. However, permitting employees to utilise their own device of preference in the work-place also brings some risks often associated with the loss of control over organisational data. Hence, this study set to determine and assess the risk of introducing BYOD in an ICT organisation. The Case Study approach elicited that the secure use of the BYOD requires the introduction of mixed measures: technical (e.g. Mobile Device Management - MDM) and non-technical (e.g. ICT or BYOD security policies). This study also explored the customer services view related to the BYOD initiative and suggests that use of this initiative can leverage services. The contribution of this study, aimed at practitioners and academics, is seen as threefold as it can help organisations to successfully manage the introduction of BYOD for employees and customers satisfaction, create and implement appropriate policies and also assist the individuals to learn about the risks related to the use of BYOD in an organisation.

Introduction

Modern mobile devices, such as smartphones and tablets, enable employees to work anytime and from anywhere. In that regard, the trend of bring your own device (BYOD) has been rapidly adopted by many organizations despite the pros and cons of BYOD adoption (Putri & Hovav, 2014). Thomson (2012), summarising the Cisco Connected World Technology Report (Cisco, 2012), stresses that many employees prefer to work with their own devices and expect to use them in the work-place.

This concept of BYOD, which can increase employees' productivity and be cost-cutting for organizations (Wood, 2012), is defined as an environment in which employees use their personal device to access their organizational resources in order to perform everyday work tasks

(PricewaterhouseCoopers, 2012; Walker-Osborn et al., 2013; Putri & Hovav, 2014). However, alongside noted benefits, BYOD also introduces many risks for the organisation; for example, loss of the device and weak credentials may weaken confidentiality, data leaks and malware attacks may compromise data consistency and potentially cause complete data loss (e.g. Lebek et al., 2013; Putri & Hovav, 2014; Berghaus & Back, 2014).

Successful implementation of the BYOD initiative also demands that an organisation modifies its policies, educates employees and further tightens information and communication technologies (ICT) security. Although the risk of adopting BYOD is evident, many authors advocate introduction of this initiative as "*the BYOD cannot be stopped and that best organisations can do is to seek solutions to address the problems*" (McLarty (2012). Thomson (2012) openly calls ICT professionals to embrace BYOD and adopt a viewpoint of accepted risk while McLarty (2012) cautions that those who do not meet the employees' BYOD requirements might experience reduced productivity, unnecessary risks, and dissatisfaction. Moreover, they risk giving their organisation an "old-fashioned" connotation, which could damage their image, especially when seen from a recruitment perspective.

The reviewed literature clearly states the importance of embracing the BYOD initiative within business processes and the potential benefits for employees and customers behind it are widely accepted. On the other hand, there is still a lack of understanding of number of risks related to BYOD and how to mitigate or eliminate those risks. This is particularly true for the South African and the Western Cape context, the empirical setting of this study. Our preliminary research shows that private and public organisations in the Western Cape are still not sure what risks and vulnerabilities the BYOD initiative can introduce and how to address them. Hence we set to find out what risks related to BYOD are faced by organisations and how can those risks be mitigated or eliminated**.**

From the customer services perspective, the modern literature strongly suggests that mobile computing is changing the nature of business operations. The next generation of mobile ICT devices and models can *"fundamentally reshape operations, business and marketplaces"* by delivering information and services directly to the decisions-makers (Hollingworth & Harvey-Price, 2013). The BYOD trend is firmly supporting this development as this concept is a consumer trend developed out of the continuously growing demand to stay connected with employees and also to personalise a *stay-up-to-date* relationship with customers. McCann (2013) states that "*this is the era of BOYD*" as customers are nowadays choosing a marketing strategy to interact with and are no longer passive receivers of information. However, the beneficial use of the BYOD initiative requires *inter alia* secure use of own ICT devices used within this initiative.

Approach to this study

The approach used in this technology-related study, on "*an unpredictable phenomenon*" (Sofaer, 1999), was qualitative, inductive and explorative in its essence (e.g. Yin, 1994; Creswell, 2009; Thomas, 2006), and made use of the Case Study Methodology (CSM), in particular. Given that the nature of the research problem and questions ("*What risks related to BYOD are faced by organisations and how can those risks be mitigated or eliminated in order to support better customer services*?") were qualitative (e.g. Hennink et al. 2011), this study utilised comprehensive interviews to obtain necessary information and reach its main objectives: (i) to explore the benefits of BYOD, (ii) to recognise main concerns and risk associated with BYOD, (iii) to identify and suggest possible solutions for mitigating or eliminating BYOD risks and concerns in an organisation in order to (iv) explore the consumer services implications.

The research design involved conducting a literature review on the BYOD phenomenon, followed by interviewees and their analysis using the Interpretative Phenomenological Analysis (IPA). This approach was useful in generating a single, idiographic case study with employees from Secure Cloud (an ICT company, empirical setting of this study). The participants were selected based on predefined criteria and consisted of managers and operational staff: Chief Technology Officer (CTO), director of sales, technical team leader, senior business manager, channel manager, network administrator and senior ICT consultant. The purposive sampling of seven interviewees was chosen as its power *"lies in selecting information rich-cases for in-depth analysis related to the central issues* [BYOD, in this case] *being studied*" (Royeen (1997: 47).

This paper is organised in the following way: we first present discussion regarding the emergence of BYOD initiative, its attributes and benefits. We further discuss BYOD risk and challenges as well as the possible solutions. As all these are based on the review of the contemporary literature, we have tested these findings and the empirical results are also reported in this paper. Finally, we discuss possible BYOD implications for enhancing consumer service, followed by the study concluding remarks.

Emergence of BYOD initiatives

The term BYOD represents the growing trend of using privately owned devices in the workplace and is associated with the multiple uses of employee owned devices for work related purposes within organisations (Niehaves et al., 2013).

The tendency toward the utilisation of privately owned devices can be traced back to 2007, when Apple introduced iPhone, their first smartphone device. The iPhone was the first smartphone created with a multi touch interface and it marked the beginning of the worldwide smartphone revolution (Kim 2011). Shortly after the iPhone became a massive success, other mobile manufacturers quickly followed, as smartphones were and still are one of the most sought after modern devices. Quickly adopted by the public, smartphones are now rapidly finding their way into many organisations. Currently, alongside smartphones, the most frequently used private devices for BYOD are laptops, tablet computers and phablets.

The BYOD initiative has a number of essential organisational drivers. For example, numerous worldwide organisations are now trying to accommodate changing needs of their staff that insist on improved work-place flexibility and show aspiration to use the latest high-tech products (Gatewood, 2012; Thomson 2012). A number of recent studies suggest that employees nowadays believe in being "*able to access whatever they need from wherever in order to do their jobs*" (Mansfield-Devine 2012), and are increasingly efficient when utilising their own devices which are not "*officious, obstructive, or even…old-fashioned*" (Thomson 2012). Therefore, it can be stated that BYOD is a reaction to a rising demand from employees and can be strategically used to preserve or attract the most talented employees – the workforce of the future. Recent widespread research across 22 countries conducted by Citrix (2012), with the subject of work-place of the future, showed that 62% of organisations globally have already adopted a BYOD policy.

The BYOD trend in South Africa accelerated in 2013 and it is predicted that this trend will continue to rise as it was estimated that South Africans would buy 10 million cell phones by the beginning of this year - and that more than half of those would be smartphones. It is also estimated that the number of smart phones in South Africa will reach 13.5 million by the end of 2013, meaning that almost every South African in a managerial position was utilising a smartphone for work (World Wide Worx, 2012). Furthermore, by the end of 2012, one million tablet computers were in use in South Africa, which is in actual fact more than double compared to just twelve months before (World Wide Worx 2012). However, the Southern African branch of Citrix states that South Africa is arguably 12 to 18 months behind Western Europe regarding the BYOD initiative, but it is expected to eventually follow suit (Citrix, 2012).

Vital attributes and benefits of BYOD

According to the pertinent literature, some of the most important characteristics of BYOD are: i) mobility, ii) mobile individuals, iii) mobile environment, iv) mobile technology, v) mobile equipment, vi) mobile computing and vii) consumerisation.

Mobility essentially means not being tied to a geographic location (Abowd et al., 1997) and is chronologically often related to making information available whenever and wherever is needed (Heijden &Valiente, 2002). Various technologies in a variety of ways support activities determined on the type of mobility that is in use: mobility can be an activity like the remote communication between individuals or the local integration of individuals with each other (Weilenmann, 2003).

Mobile individuals are individuals (e.g. employee or customer) who are in movement but the term mobile is also often associated with groups. For example, a group can be mobile to some degree when all or some of the group members move during their work at some point (Andriessen &Vartainen 2006).

A ***Mobile environment*** represents an environment in which people find themselves in motion, while they are more or less stationary (Weilenmann, 2003). Such environments may be, for example aeroplanes, boats, trains, taxis and public transport. In these environments, individuals have the opportunity to be productive and to use mobile technology for business purposes, because of their surroundings.

Mobile technology refers to equipment that is specifically designed to be mobile, i.e., the equipment that should be easy to carry and use by moving individuals. One example is a mobile phone that can easily be carried and used, even during motion. Laptops and some other technologies used for BYOD are often referred to as mobile, but in these cases are rather portable because they are specifically designed for use by moving individuals. Even in the context of a mobile environment where individuals are stationary, these technologies can be classified as mobile (Weilenmann, 2003).

Mobile computing is an important part of BYOD and is defined as "*an umbrella term used to describe technologies that enable people to access network services any place, anytime, and anywher*e" (Kumar 2011). Kumar also states that mobile computing originates from the cellular concept found in 1947 by Don Ring of Bell Labs.

Consumerisation is also an important BYOD characteristic and the term started gaining popularity in the early 2000s (Clevenger, 2011). For instance, new technology is first embraced by consumers and then distributed to organisations by consumers. Consumerisation can also be described as a choice of employees to use their preferred devices, applications and services at the workplace (Sen, 2012). As this approach drives significant changes in organisations, it means that *"workplace is becoming obsolete, giving way to a workspace that offers users access to applications and data anywhere, anytime, via the connected device of their choice"* (Midgley, 2013).

From an organisation's viewpoint, the most prominent benefit that BYOD can bring refers to improved mobility and better efficiency as employees are now able to work wherever and whenever they like, while utilising their personal devices (Baker, 2013). It is also believed that BYOD is supported inside the organisation, staff will be more enthusiastic and engaged, analytical capabilities can be improved and moreover, the organisation will in fact enjoy the benefits of innovative functionalities and technologies used by their employees (Thompson, 2013). Some of the additional organisational benefits which the BYOD initiative may bring include: (i) improved creativity and efficiency from motivated and more mobile employees; (ii) better sales efficiency and results through increased engagement with customers; and (iii) significantly lower ICT support costs as the direct result of the exclusion of software and hardware buying, which also mean less expenses from the organisational budget for maintenance (Moore & Warner, 2012; Caldwell 2012). Furthermore, by permitting employees to make use of their own devices, organisations can reduce ICT infrastructure expenses. On the other hand, from an employee standpoint, the quality of their work is improved immensely, as they have the possibility to choose the services, applications and devices they prefer for both personal and work purposes (Santhana & Kumar, 2011).

A recent worldwide study, conducted by IDC Manufacturing Insights, among over 460 enterprises across multiple sectors (e.g. industrial machinery and equipment, hi-tech and metal fabrication), and covering 13 countries worldwide, revealed that their top business initiatives are focused on growth and differentiation through value-added services and improved customer experience. Hence, it is important for these companies to respond to customers with speed and efficiency through strategies such as BYOD (Infonetics Research, 2014).

BYOD risks and challenges

Although, BYOD can bring a number of benefits, it also creates an immense challenge for ICT professionals who are tasked to keep the organisation's information and data secure, as well as to protect the organisation from malware infection and other security risks. Hunt (2012) establishes that data leak and mobile malware are two main concerns connected with the BYOD. As mobile devices become more and more sophisticated, the growing occurrence of malevolent programs on them is almost expected. More complex mobile devices, such as smartphones, run more complex operating systems and in return provide a programmable platform with many possibilities. Firewalls cannot prevent malware from distribution through ports that are typically utilised, and some security threats are also able to avoid the traditional antivirus software. As a result, private mobile devices are capable of travelling outside of the organisation's security mechanisms and are inevitably under risk (Friedman & Hoffman, 2008).

Miller et al. (2012) illustrate a similarity between the BYOD initiative and the laptops introduction to the organisation pointing out that some authors believe that the threats and security concerns associated with BYOD initiative are "*largely a replay*" of those previously faced with laptops. Nevertheless, they also advise that the BYOD phenomenon is a tougher challenge to security because of the large number of devices. BYOD also initiates the fragmentation of devices and their security levels into organisations. In most cases employee owned mobile devices have different degrees of protection methods, for instance, system settings, system updates and anti-viruses. As a result, any unauthorized application may have undesirable effects on the device and its data reliability. An additional delicate risk of BYOD is potential staff that may abuse technology usage and cause data leaks (Ghosh et al., 2013).

The BOYD security issues become even more complex due to the fact reported by Calder (2013) that personal devices in a researched organisation have infiltrated the workplace as 95% of employees have some type of smartphone. Additionally, 80% of employees possess more than one mobile device while more than 30% did not utilise any password to safeguard data located on their private mobile devices. This scenario presents organisations with a quite possibly serious security threat. Any device used in the workplace today is more likely to contain some sort of organisation sensitive information or data. If organisations permit staff to bring their private devices into the workplace, a security risk might emerge. On the other hand, it is challenging to control employees' own devices, even though they hold important corporate data, which raises the likelihood of data leak of the organisation.

In addition to all BYOD risks previously described, multiple authors agree that the three most frequently identified and certainly the biggest BYOD risks are:

- *Data leak* refers to confidential work related information, which is usually stored on employee owned private devices, thus creates a great risk to organisations due to the projected or unintentional leak of confidential information, such as business client information and sensitive organisation data (Ghosh et al. 2013; Miller et al. 2012; Morrow 2012; Wood 2012);
- *Forfeit of management and visibility* refers to the concern of "ownership" and is considered as the foundation of this difficulty. For the BYOD initiative, organisations possess a reduced amount of clarity of the security situation in comparison with the conventional data centres. There are, therefore, fewer alternatives to alleviate security concerns for un-managed devices in comparison with managed devices - simply because of poor management and visibility. (Miller et al. 2012; Morrow 2012; Thomson 2012);
- *Simplicity of device loss* is linked to the fact that many mobile devices are quite small in size as the portability is a significant factor. This, however, might cause loss of the devices used for BYOD and the data located on them (Ghosh & Swaminatha 2001; Morrow 2012; Miller et al. 2012).

Possible solutions for mitigating or eliminating BYOD risks

Security of mobile solutions, including BYOD, is a facilitating factor for organisational ICT departments, which requires strategic decisions in that regard as "*without protecting internal or customer data, operating departments will not be able to use mobile solutions*" (Berghaus& Back, 2014). The reviewed literature suggested at least five measures for achieving secure use of BYOD in an organisation: (i) application security, (ii) employee education, (iii) security policies, (iv) security culture and (v) Mobile Device Management (MDM).

Application security

Baker (2013) argues that applications are the "*backbone*'" of any employee who is mobile. Applications for interoperability and system integration are usually built within an organisation or acquired off the shelf, to assure that staff is capable to use organisational ICT systems or other practical applications on their private devices by means of the internet. Even though development of applications to maintain purpose and interoperability of diverse mobile devices is critical, it is not sufficient. When developing BYOD initiatives, security is as important as the purpose. Consequently, many applications have been developed to address risk, such as Data Leak Protection (DLP) (Thompson, 2013). It is important that the idea of security is embedded into the original design of applications, not simply as a late addition. Very often, when different security issues occur, organisations have a tendency to hasten everything to make sure the budgets and deadlines are met. On the other hand, this "*short sighted mode'*" not only places organisational data resources at risk, but also increases costs. A much prominent way to organise security during the initial deployment of BYOD initiative is to remove any prospective weaknesses (Baker, 2013).

Thompson (2013) establishes that one of the requirements of the BYOD initiative is the flexible and innovative solution for ICT personnel, for preserving security while permitting access to combined technology. He further points out that in order to ensure that organisational employees using their private devices are operating in a functional and secure domain, the work-related and security applications must be able to coexist. As a result, it is significant to find a sense of balance between risks and benefits so that security is not blocking business progression. Additional security intensity should be also considered with regard to confidential data that might be located on employees' private devices when implementing a BYOD initiative (Steven, 2013).

Employee education

While organisations gradually lose grasp over the security of their mobile devices, staff have a more significant part in the general preservation of organisational security. According to Mansfield-Devine (2012) organisations must integrate their staff into security design. In a 2011 international study by a world leader in firewall and network appliances, Fortinet Inc., it was established that for the most part employees prefer to utilise their private mobile devices in their work-place regardless of it being in opposition to organisational ICT and security policies. Furthermore employees consider themselves, not the employer, liable for any device security problems. Therefore, staff can be alleged as the most fragile security link and organisations must think about employee's needs when creating and implementing BYOD policies. Hence, it can be stated that it is of utmost importance for organisations to train all employees and increase their understanding of information security and make sure that they only use organisation information on their devices in a safe environment. Employees' actions are strongly influenced by the organisation's information security culture and as a result technical mechanisms along with employee awareness and behaviour (organisation security culture) should be combined in order to deal with BYOD risks.

BYOD and security policies

Due to the continuous growth of BYOD, organisations, at a bare minimum, should have appropriate policies that regulate this area. As in regard with information security, end-user behaviour can be very challenging (Herath& Rao, 2009), the employees must be familiar with these policies and possible should sign the document confirming that they are familiar and will obey these policies. This type of document, which generally outlines the rules, laws and practices, should not only deal with the security of the devices, but also grant permission for the organisational ICT support to examine the device for compliance with organisations policy (Semer, 2013).

Another complex and important issue which might be of concern to organisations is the accessibility mechanism and its related security solutions. It needs to be precisely specified, via policy, what kind of information is available to BYOD devices, how easily the employees can access sensitive business information via their own devices, and the different types of authorisation required for these devices (Gosh et al., 2013).Organisation should also re-visit whether its existing information security, confidentiality, privacy and employment policies address the company's approach on BYOD (Ambrosio, 2012).

In the South African context, the Protection of Personal Information Act (POPIA) requests the protection of personal information that is "*processed by public and private bodies*". It further requires protection of personal information through introduction of protection principles and code of conduct for establishing a minimum of requirements for protection of personal data "*across of the boarders of the Republic*" (POPIA, 2013). This Act is applicable to all organisations in the country and impacts all processes of collecting, retaining, processing, disseminating and disposing data (Duggan, 2012), hence, impacting the security of BYOD initiative.

Concept of security culture

As the BYOD initiative introduces immense cultural change to organisations, it was no surprise that a number of authors stress importance of this concept. According to Da Veiga (2010), "*the information security culture is cultivated by the behaviour of employees, which is directly influenced by the information security components*." In fact, every employee should play a role and share responsibility for organisational information security (Vljoen, 2008). In connection to the BYOD initiative, it is imperative for organisations to agree to the right leadership and governance, suitable security policies, and any security mechanism which enforces the actions of employees to be aligned with the organisational culture and makes it security conscious (Vroom& Von Solms, 2004). If the BYOD initiative is accompanied by an efficient security culture, it is more probable to bring a successful outcome for organisations.

Von Solms (2000) stated that security culture is "*to be created in an organisation by instilling the aspects of information security to every employee as a natural way of performing his or her daily job*". This security culture is described as a conglomerate of "all *socio-cultural measures that support technical security measures so that information security becomes a natural aspect in the daily activities of every employee*" (Schlienger &Teufel, 2003). Adams and Blandford (2005) point out that security culture must side with organisational policy and integrate into normal operational practice. They also indicated that the crucial tactic should be to inspire staff alertness.

Thompson et al. (2006) described that a security culture was greatly determined by organisational culture and jointly connected to it. They also gave emphasis to constant education of employees as a critical factor to ensure understanding of security concerns. Whitman and Mattord (2012) also support the stance that employee education was the reason for significant differentiation, which is best circulated through the organisation by supplying training, producing awareness, and essentially creating a culture. Furthermore, collective socialisation could present a significant feature, as individuals usually gain knowledge while studying one another (Thompson et al., 2006). Ruighaver et al. (2007) also described how an organisation's inner culture has a vast influence on security culture and that it might not be suitable to consider security culture in absolute segregation from general organisational culture. Hence, an organisational security culture can have an immense impact on the whole security perspective (Whitman &Mattord, 2012).

Mobile Device Management

Many organisations consider Mobile Device Management (MDM) the most effective and best solution to secure employee devices and a central part of an organisation's BYOD management and security tactic. MDM provides two independent data containers so business and private information stored on the same device are easily separated. In addition, organisations need to keep an eye on the information and policies for the business environment, which not only protects the employee's confidentiality, but also effectively benefits the security of the organisation's resources (Semer, 2013).

Although it is not the latest technology, MDM (Figure 1) is only recently beginning to grow in complexity as a result of the rise of the BYOD initiative. Currently the MDM system has been extensively employed by organisations for the administration of various mobile devices and has also offered a span of security features to permit organisations to preserve scalable visibility and centralized control of BYOD devices (Phifer, 2013; Semer, 2013).

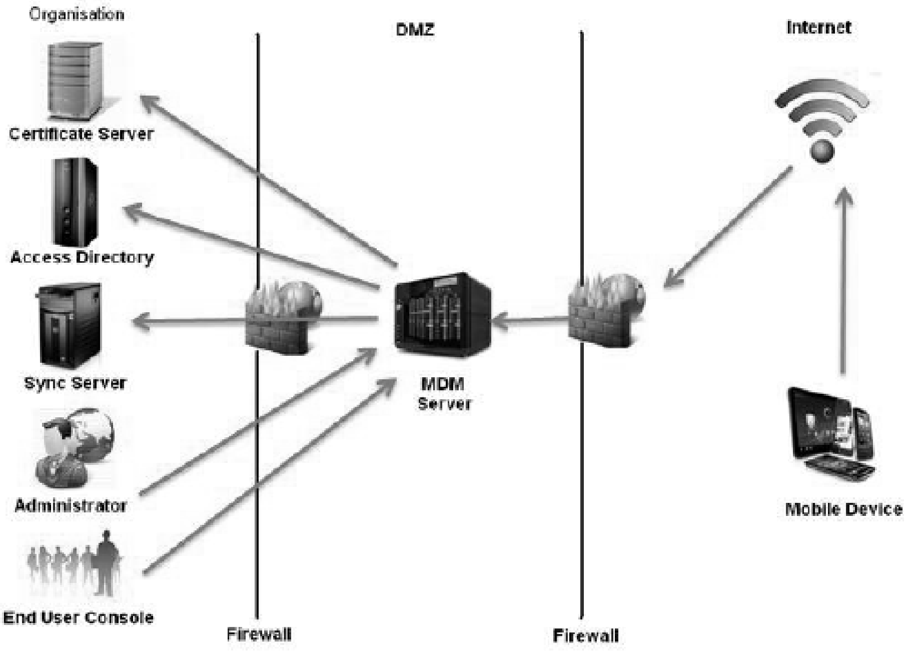

Figure 1: Typical MDM architecture (source: *Ghosh et al., 2013*)

In summary, it can be said, that the MDM technology may be seen as an efficient tactical answer for the management of many threats associated with BYOD such as weak passwords, data leaks, forfeit of management and complete device loss. Although detection capabilities of MDM are not sufficient without a proper response mechanism, MDM is a very comprehensive system as it also combines a response strategy (Schneier, 2003).

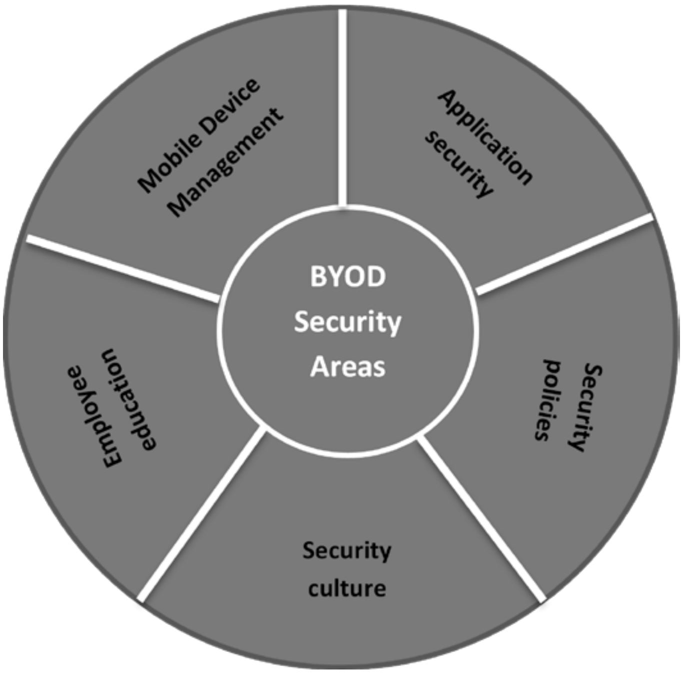

Figure 2: Areas of BYOD security management (source: *Authors*)

The identified areas of the BYOD security concerns are diagrammatically shown in Figure 2. Our findings suggest that achieving fairly secure use of BYOD in an organisation depends on "soft" managerial components of appropriate security culture, sound security policies and proper education and training of its employees. On the other hand, the BYOD security is inevitably linked to "core" technology security achieved through management of application security and the mobile device management.

Empirical findings

Participants in this study generally agreed that embracing of the BYOD initiative is rather important - not only for employees, but for the employer as well. Having in mind benefits, majority of participants shared the opinion that BYOD is the way forward into the future of modern workplace. The participants also concur with possible benefits and risks as portrayed by the reviewed literature.

Use of BYOD by the participants

When questioned if they have ever heard of BYOD, all interviewees responded with "yes" and provided different explanations for the term. For example:

"Yes, [there are] *companies which allows its employees to utilise their own devices at workplace"* (Interviewee 7). *"Yes, I have. I would describe BYOD as bringing a device not provided by your company in the corporate network to access business resources and do work related tasks"*

(Interviewee 5). *"BYOD allows employees to bring personally owned mobile devices to their workplace, and use those devices to access privileged company information and applications"* (Interviewee 6).*"Yes, it is when you take out a contract from your ISP, but you use your device instead of using a device they provide. Or in business terms, it is when you bring your own tools to work with*" (Interviewee 3).

Although the participants did not explain the term BYOD as it is found in the reviewed literature, this study has shown that the interviewees possess respectable knowledge of this concept. This confirmed that the selection of the research sample was appropriate for the purposes of this research.

In this introductory part of the interviews, all participants have confirmed utilising some form of mobile device in the workplace. Furthermore, all of the them have at least two different personal mobile devices which they use for work and personal purposes, e.g. laptop and smartphone, while three out of seven participants in this study additionally use a third personal mobile device, such is a tablet computer . For example, Interviewee 2 confirmed that for work and personal purposes he daily utilises "...own *Laptop, iPad and Android Smartphone".*This high dependability on mobile technology in the common workplace in South Africa and in the personal life is also reported by World Wide Worx (2012).

Six out of seven interviewees shared a common viewpoint on the importance to permit staff to use their private mobile devices in the work-place. For instance: *"Yes, very important! We might not always have our laptops and mobile devices that are provided to us and our personal devices are always available"* (Interviewee 3) or "*Very important; employee can choose their preferred device make and model with which they are comfortable with and able to use their device for both personal and business use"* (Interviewee 2). It seems that the BYOD trend is here and it's here to stay (Burt, 2011), hence it should be appropriately managed.

BYOD benefits confirmed

All interviewees agreed that BYOD has many benefits for both employers and employees, presented their own viewpoints on BYOD benefits: *"Increased productivity, simplicity, opex consideration as opposed to capex"* (Interviewee 1). "*Employee benefits are more productivity due to the use of technology they are familiar with. Also the ability to become mobile; therefore to be able to adopt the work style that suits them. BYOD also allows the employee to express who they are in the workplace through the adoption of technology that fits with them*" (Interviewee 4). "*Less devices; if you were issued with a company phone, and you have your private phone, you would need to carry and maintain 2 devices. The lower capital outlay for the company, as the employee is providing their own device*" (Interviewee 5).

The responses confirm our literature review findings. For instance, Baker (2013) points out that from an organisation's point of view, the most prominent benefit that BYOD brings is increased mobility and productivity, as employees can now work whenever and wherever they like, using their personal devices. Thompson (2013) points out that if BYOD is supported inside the organisation, staff will be more enthusiastic and engaged, analytical capacities can be improved and moreover, the organisation will in fact enjoy the benefits of innovative functionalities and technologies used by their employees.

Organisational benefits of BYOD, as established by Moore and Warner (2012) and Caldwell (2012), were also confirmed by interviewees. Better sales efficiency and results through increased engagement with customers (e.g. Interviewee 4*:"... our sales team has recorded a significant boost in sales since we started using various mobile business apps for direct engagement with our customers*..."). Significantly lower ICT support costs for as the direct result of the exclusion of software and hardware buying; less expenses from the organisational budget for maintenance (e.g. Interviewee 1*:"... significant cost savings for us as the employee in most cases do not expect the employer to fund the devices as they want full ownership thereof...*)".

On the other hand, Interviewee 2 gave interesting viewpoints on both benefits and disadvantages of BYOD, based on his own experience: *"To keep this short; increase of productivity and flexibility; freedom to move around and no longer desk-bound; on the other hand decrease in personal life quality; more difficult to switch off from work to focus on personal family life"*. This confirms the emergence of a blurry line between work and private life, which will certainly impact on security of BYOD: "*Many employees don't understand the implications of using their personal devices for work. Many companies don't understand that they are in fact liable for the consequences*…"(Trade Micro, 2012).

BYOD risks confirmed

All interviewees agreed with BYOD risks elicited by our literature review. Their responses and viewpoints, however, varied in general, as there were many different perceptions amongst them; e.g. what the real BYOD risk for both employees and employers is. For instance: "*Your list covers most… one other [risk] would be when an employee leave the employ of a company; the process to ensure access is denied and data recovered*" (Interviewee 1). "*Risk of corporate data staying on the device when passed on to family member or when he gets an upgrade; risk of lack of security awareness; protection devices are at risk of personal apps with malware or vulnerability to be installed*" (Interviewee 2). "*The cost and maintenance on the devices now falls under your responsibility and not your company. It is true antivirus and OS exploits will be a possibility, but the internet provides free updates for everyone. I never had a big problem with any of these issues, because I update on a regularly*" (Interviewee 3). "*Data leak/breeches - the company is no longer in control of the data*" (Interviewee 5).

All the above-mentioned is generally covered in the pertinent literature. For instance, Hunt (2012) establishes that mobile malware and data leak are two main concerns connected with BYOD. Furthermore, Miller et al. (2012) and Morrow (2012) point out that BYOD instigates high-security threats for organisations, as they are not able to manage both the device and the data located on the device. Therefore the application of protection measures is very challenging for concerns such as theft, regulatory compliance and data leak. In addition, number of authors agrees that the three most frequently identified and certainly the biggest BYOD risks are: i) data leak; ii) forfeit of management and visibility; and iii) simplicity of device loss (Ghosh et al 2013; Ghosh & Swaminatha, 2001; Miller et al. 2012; Morrow 2012; Thomson 2012; Wood 2012).

In the view of the findings presented above, it can be said that most of the BYOD risks are technical in nature and that security is as important as functionality, when developing BYOD initiatives. On the other hand, this study confirms that, besides implementing the right technology, it is also necessary for organisations to set up some effective BYOD policies which will assist them in avoiding potential security risks caused by BYOD.

Minimising BYOD risks by using MDM

Answers to this question varied in general, as interviewees had different perceptions and viewpoints. Three out of seven interviewees believed that the researched company did not take any steps to minimise BYOD risks. Interviewees 5 and 7 stated that the researched company has MDM service already deployed. Interviewee 6 was a bit unsure, but she assumed that the company had a BYOD policy deployed. However, Interviewee 4 believes that *"...policies are in place and mobile device management enrolment is encouraged but at this stage not compulsory..."*.

The analysis of the responses suggests that the interviewees generally agree about the steps necessary to minimise the BYOD related risks. The fact that some of them were not certain if the researched company has introduced the MDM as the solution suggests (at least) the lack of communication regarding use of BYOD in this organisation or even lack of strategy in this regard -the MDM is a very comprehensive solution as it also combines a response strategy (Schneier, 2003). This technology can also be seen as an efficient tactical answer for the management of many threats associated with BYOD such as weak passwords, data leak, forfeit of management and complete device loss. Furthermore, the MDM policy can also include additional policies for dealing with risks, by using mechanisms such as malware detection, encryption, device PIN and lockout control, jailbreak and root detection, and remote wipe (Semer, 2013).

BYOD and security policies

There were divided viewpoints amongst the interviewees on the existence of BYOD and security policies in the researched company. Four out of seven interviewees stated that the company does not have any BYOD or security policy; two interviewees believed that the organisation has both BYOD and security policy and one of them that *"We have a general IT security policy; but not a specific or enforced one for BYOD"* (Interviewee 2). This confusion amongst participants, as in the case of existence of MDM in their organisation, suggests that the company needs to make sure that (if BYOD or security policy really exists) a policy is circulated throughout the organisation to produce general awareness, to provide training and, most importantly, to help create a general security culture. The organisational security culture can have an immense impact on the whole security perspective (Whitman &Mattord, 2012) and that culture must side with organisational policy and integrate into normal operational practice - the crucial tactic should be to inspire staff alertness (Adams & Blandford, 2005), which does not appear to be in effect in this instance. Hence, the researched organisation faces "discretionary nature of adherence" to the security policies, which pose a challenge on enforcing organisational information security (Hearth & Rao, 2009.

Employee BYOD training and security culture

When questioned about their opinion, if the researched company employees' need to be educated or trained regarding BYOD and how they should use their personal devices in the workplace, all interviewees were of the same opinion stating that this is a very important topic and that it can directly influence the company's business - either negatively or positively. Interviewees, however, had different viewpoints regarding what should be the focus of the employee education and training on BYOD. For instance: *"Employees should be made aware of the general risks and best practice"* (Interviewee 2). *"I feel that employee training should be focused on security as a whole and not specific to BYOD. If a user has the knowledge around how to protect data from a day to day usage perspective then the BYOD simply falls within that same logic"* (Interviewee 4). "*I think training should be compulsory in order to properly educate your user and ideally BYOD related*" (Interviewee 5).

The literature reviewed in this study also supports that staff have a more significant part in the general preservation of organisational security. According to Mansfield-Devine (2012) organisations must integrate their staff into security design. A 2011 global survey by a world leader in the firewall, network appliances and security, Fortinet Inc. (Fortinet, 2012) pointed out, that it is of utmost importance for organisations to educate staff and increase their awareness on general IS security and make sure that they only use organisation information on their devices in a safe environment. Employees' actions are strongly influenced by the organisation's information security culture and as a result, technical mechanisms along with employee education should be combined in order to deal with the BYOD risks.

Customer Services implications

Businesses that wish to engage with customers must centre their strategies on developing new business models, which includes delivering products and services on the move (Hollingworth & Harvey-Price, 2013). According to Deloitte (cited in Hollingworth & Harvey-Price, 2013) mobile is the changing the nature of business operations: "*the next wave of mobile may fundamentally reshape operations, business and marketplaces-delivering information and services to where decisions are made and transactions occur. And the potential goes far beyond smartphones and tablets to include voice, gesture and location-based interactions; device convergence; digital identity in your pocket; and pervasive mobile computing. The very definition of mobile is changing*"

The Economist (2013) states that based on the balance of information, the customer is now in the driver's seat. Although companies realise their need to radically change the way they communicate with customers, many still mainly rely on their website (51%), followed by email (40%), whilst few make use of social media (23%) and even fewer make use of mobile apps (10%). Unless companies are plugged in to the new world of their customers and align their channels to emerging customer preferences, they will suffer.

The above and related concerns also apply to consumer issues in the ICT sector and all sectors influenced by the contemporary information and communication technologies. Technology solutions is not about how smart the technology is but more what the customer cares about - especially how solutions improve and increase customer experience. Design of user experience is key priority of technology, which is a key skills requirement alongside deep technical capabilities (Hollingworth & Harvey-Price, 2013).

Wishing to gain greater customer insight and transform customer experience, differentiate services and increase competitive and revenue, leading organisations do the following: (i) use big data collection and analysis as strategy to connect with their customers (ii) invest in mobile applications (III) appropriate leading edge technologies and (iv) social media (Bruhn, 2012). The BYOD trend is firmly supporting these developments. As already intimated BYOD is a consumer trend developed out of the continuously growing demand of employees (and consumers) for anytime, anywhere access afforded through the innovation and easy availability of high performance personal devices (Xavient, 2014). McCann (2013) asserts that "*this is the era of BOYD...we want content whenever and wherever we choose. Consumers are choosing which marketing to interact with and are no longer passive receivers of information*".

According to Mikale (cited in McCann, 2013) small business that wants to keep up with customer needs must be part of their daily lives whether through blogging, social media, local event, and this require agility and responsiveness. Anomah et al.(2013) state that BYOD is supporting businesses to obtain high productivity, efficiency and customer value through rich media applications such as voice integration, instant messaging, video and alike enabling sales staff and employees to communicate on real time basis. Some research highlights that business needs to adapt to new ways of technology use and digital lifestyle driven by the "consumerization" of ICT and the fit of personal devices into normal service processes of the business (Faulkner, 2013; Kearney & Davidson, 2012).

Here it is important to note that there are also deferring opinions about usefulness of BYOD initiative. Watson (2014) opines that online customer service and experience cannot match what a physical retail store can offer. In this respect, Watson believes that BYOD is not appropriate in the retailing sector. Although BYOD may to an extent provide satisfaction to the sales staff in having inventory information at their fingertips, the ICT department on the other hand, has to deal with a range of system, products and platform, and to maintain and integrate these devices will be complicated, if not impossible. This aspect is reinforced by Bridgewater (2012) who maintains that majority of ICT support team help service desks are unwilling to support employees who want to bring their own device (BYOD) to work. According to a survey by CompTIA of 400 ICT and business executives, 39 percent to 51 percent of respondents are not doing BYOD (Kaneshige, 2014). The reasons, according to this survey, why companies are reluctant to adopt BYOD include:

- BYOD was supposed to get ICT out of mobile device purchasing and deployment, and though some companies reported saving millions of dollars, others reported that BYOD is riddled with hidden costs, such as expense report processing, management, employees gaming expenses, zombie phones attacking mobile budget, messy conversion of phone service liability among some of the issues.
- BYOD was supposed to contribute to a happier workforce, but instead an increase in BYOD legal policy directives to safeguard corporate data and employee privacy concerns. Furthermore, employees faced threat of dismissal if they were found having flouted BYOD policy.
- BYOD was supposed to ensure a more productive workforce but there is no clear evidence that this is so.
- BYOD was supposed to contribute to ease of life but security and compliance issues, risk of data loss are major drawbacks.

Despite some non-sportive voices, it seems that many organisations are willing to introduce (or have already introduced) BYOD perceiving the benefits described earlier (Tam & Villanueva 2013): (i) improve customer services, (ii) drive employee satisfaction and loyalty, (iii) increase productivity, (iv) improve communication, collaboration and satisfaction, (v) drive revenue and (vi) reduce capital expenditure, ICT and mobile expenses.

Yet, despite its rapid adoption, BYOD remains a major security risk of which some that we deem very important are depicted in this paper and, also emphasised by Limonczenko (2014), Snow (2014) and Cox (2014). This study showed that BYOD security issues must be appropriately addressed if benefits for employees and consumers are to be achieved. Reliable and safe utilisation of the BYOD initiative will, according to the worldwide reported experience, certainly contribute to the higher consumer experience.

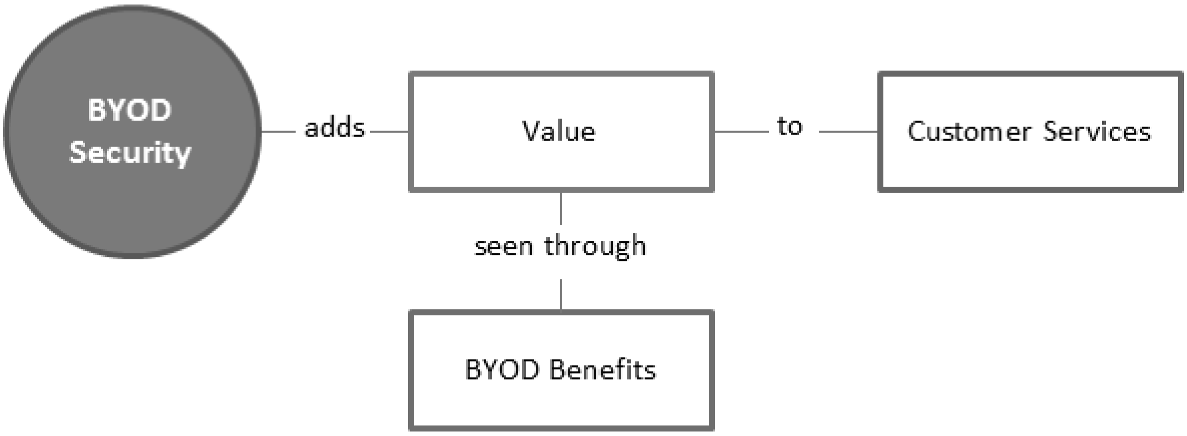

Figure 3: BYOD and customer services (source: *Authors*)

Summarising, it can be stated that the security management of BYOD can add value to the consumer services through the potential benefits of the BYOD initiative mentioned earlier (Figure 3).

Conclusion

The findings of this study suggests that the BYOD initiative has a potential to enable significant reduction of organisation expenses as the direct result of the exclusion of software and hardware purchases and bring other benefits. This study also shows that employees who utilise their own devices at workplace should have appropriate determination and attitude towards the use of BYOD in order to achieve better productivity. Hence, it is recommended that the introduction of the BYOD initiatives might be a worthwhile endeavour.

This study elicits that organisations which embraces the “changing times” and introduce BYOD, can gain a strategic advantage by being the first to harvest the benefits that come with having an optimistic, more productive staff and quite possibly increased return on investment (ROI). Additionally, these organisations “early adopters” will be able to preserve or attract the best talent and remain competitive on the market. The reviewed literature and the participants agreed that the BYOD initiative is the future of the work-place.

On the other hand, it was established that allowing staff to use their own device of preference in the workplace without any proper risk preventing mechanisms, can raise a number of potential risks such is data leak, loss of control and management, malware and the alike. Many organisations have failed to think through the new family of risks and vulnerabilities that BYOD introduces. Thus, it is recommended that, regarding security, the BYOD initiative requires a combination of technical and non-technical solutions to be introduced. To become successful in effectively deploying the BYOD initiative, organisations need to be also conscious of issues related to rapidly changing technology and to the way a business operates.

Concluding the security side of this study, it can be stated that minimising the BYOD related risks can be done by introducing appropriate strategies and policies and raising the employees' awareness of these. These measures, coupled with appropriate security training, are deemed plausible ways for manage BYOD risk in an organisation. Introducing appropriate BYOD policies, for example through general ICT organisational policies, can increase overall BYOD security, thus minimising the risks. Furthermore, adding appropriate technological solutions, such as MDM, can successfully mitigate or sometimes even eliminate potential risks related to the introduction and usage of the BYOD in an organisation.

From the consumer service perspective, although some organisations are still reluctant to adopt full-scale BYOD, the belief is that growth of mobility will blur the boundaries between personal computing and organisational ICT as consumer devices and applications cross over into business and enterprise markets (Hollingworth & Harvey-Price, 2013). Adopting BYOD organisations should revise its strategy taking into consideration the following two aspects of service strategy: (i) identifying what forms of BYOD services will be offered to which target customers or users in order to meet the business requirements and outcomes and (ii) defining a strategy for the management of BYOD services. Our study also suggests that the BYOD strategy must include the security component of this initiative if the benefits for employees are to be achieved and the consumer experience to be lifted to the next level.

Concluding this paper it is also important to acknowledge some limitations of our study and its potential contribution. In that regard, this research was limited to a single ICT security management and consulting company, located in Cape Town. One of the key limitations was the limited sample selection of seven participants, which inevitably limits generalization of this study on the researched or similar middle-sized organisations. However, we believe that these limitations, which are common for the qualitative studies, did not influence validity of our findings. We believe that this study can be used by: (i) organisation decision makers and businesses looking for securely introducing BYOD initiative, (ii) individuals who have an interest in the BYOD subject to gain some knowledge on the security issues BYOD presented in this study and (iii) researchers to further advance work on the topic presented here.

References

Abowd G., Atkeson C.G., Hong J., Long S., Kooper R., Pinkerton M. (1997) *Cyberguide: A mobile context-aware tour guide*, Wireless Networks, vol. 3, no. 5, pp. 421-433

Adams A., Blandford A. (2005) *Bridging the gap between organizational and user perspectives of security in the clinical domain*, International Journal of Human-Computer Studies, vol. 63, issue 2, pp. 175-202

Andriessen E., Vartainen M.(2006*) Mobile Virtual Work: a New Paradigm?,*Springer Verlag, Hindenberg

Ambrosio, P. (2012)*BYOD Also Means "Be Mindful of Your Old Duties" – BYOD Policies Raise Familiar Legal and Information Security Issues*, Information Security & Privacy News, Volume, 3 Issue 3, Summer 2012

Anomah, S. & Agyabeng, O. (2013) *The Art of Value Creation with Information Technology Potentials in Business Planning–the Role Strategic Information Systems*, In *Information and Knowledge Management* (Vol. 3, No. 8, pp. 49-58)

Baker T. (2013) *What you think about BYOD*, SC Magazine: For IT Security Professionals, pp. 32-33

Berghaus, S. & Back, A. (2014) *Adoption of Mobile Business Solutions and its Impact on Organizational Stakeholders*, 27th Bled eConferenceeEcosystems, June 1 - 5, 2014; Bled, Slovenia

Bridgewater, A. (2012). Majority of service desks not supporting BYOD, retrieved on 22 December 2013 from www.theitsmreview.com/2012/09/cant-wont/

Bruhn, C. (2014) *How iWorkers can draw customers closer using Big Data*, retrieved on 4 June 2014 from http://mds.ricoh.com/blog/how_iworkers_can_draw_customers_closer_using_big_data

Burt J. (2011) *BYOD trend pressures corporate networks*, eWeek, vol. 28, no. 14, pp.30–32

Calder A. (2013) *Is the BYOD Movement Worth the Risks?,*Credit Control, Vol. 34 Issue 3, p65

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

Cisco (2012) *Cisco Connected World Technology Report*, retrieved on 18 March 2014, from http://www.cisco.com/en/US/netsol/ns1120/index.htm l

Citrix (2012) *Workplace of the Future : a global market research report,* retrieved on 26 March, 2014, from www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf

Clevenger N.(2011) *Ipad in the Enterprise*, Wiley Publishing Inc., Indianapolis

Cox, J. (2014) *LinkedIn Survey finds enterprise mobility still in infancy*, retrieved on 30 May 2014 from www.itstrategist.net/articles/share/154389/

Creswell, J.W. (2009) *Research design: qualitative, quantitative, and mixed methods approaches*,3rd edition. U.S.A: SAGE publications

Da Veiga A. &Eloff., J. H. P. (2010) *A framework and assessment instrument for information security culture*, Computers & Security, vol. 29, pp. 196-207

Duggan, J.A. (2012) *The Protection of Personal Information Bull: safeguarding privacy or permitting secrecy*, retrived on May 2013 from www.archivalplatform.org/blog/entry/popia

Gatewood B. (2012), *The Nuts and Bolts of Making BYOD Work*, Information Management Journal, vol. 46, no. 6, p26-30

Ghosh A.K. Gajar P.K. and Rai, S. (2013) *Bring your own device (BYOD): security risks and mitigating strategies*, Journal of Global Research in Computer Science, vol. 4, no. 4, pp 62-70

Ghosh A.K..&Swaminatha T. M., 2001, *Software security and privacy risks in mobile e-commerce*, Communications of the ACM, pp. 51-57

Faulkner J. (2013), *BYOD and Beyond - Implementing a unified access solution*, retrieved on 12 November 2013 from http://h30458.www3.hp.com/media2.php/PDF/BYOD.pdf.

Fortinet (2012) *Fortinet® Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems*, retrieved on 16March 2014 from www.fortinet.com/press_releases/120619.html

Friedman J. & Hoffman D.(2008)*Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses*, Information Knowledge Systems Management, 7, vol. 1, no. 2, pp. 159-180

Heijden H. &Valiente P. (2002) The*value of mobility for business process performance: Evidence from Sweden and the Netherlands*, Proceedings of the European Conference on Information Systems, Gdansk

Herath, T & Rao, H.R. (2009) *Encouraging information security behaviours in organisation: role penaltie, pressures and perceivedeffectiveness*, Decision Support Systems 47(2): 154-156, May 2009

Hennink, M., Hutter, I. & Bailey, A.(2011)*Qualitative research methods*, SAGE.

Hollingworth, L. & Harvey-Price, A. (2013) Technology and skills in the digital industries. e-skills UK, retrieved on 14 January 2014 from www.gov.uk/government/uploads/system/uploads/attachment_data/file/305376/evidence-report-73-technology-skills-digital-industries.pdf

Hunt J. (2012) *BYOD Policy - What Businesses Need to Consider*, Credit Control, vol. 33, no. 5/6, p. 69

Infonetics Research (2014*) BYOD policies changing as mobility becomes a critical factor in organisational efficiency*, profitability, Infonetics Research, Johannesburg, 6 Mar 2014, available at http://www.itweb.co.za/index.php?option=com_content&view=article&id=71428:BYOD-policies-changing-as-mobility-becomes-a-critical-factor-in-organisational-efficiency-profitability&catid=355

Kaneshige, T. (2014) *What is going wrong with BYOD?*, retrieved on 2 June 2014 from www.itstrategist.net/articles/share/123076/

Kearney, D. J., & Davidson, J. (2012) *Continuous change: a help desk motto*, In *Proceedings of the 40th annual ACM SIGUCCS conference* (pp. 115-120), ACM

Kim R. (2011), *The iPhone effect: How Apple's phone changed everything*, Gigaom, viewed on 1 April, 2014, from http://gigaom.com/2011/06/29/the-iphone-effect-how-apples-phone-changed-everything

Kumar, R. S. (2011) *Paper Presentation on Mobile Computing*, viewed February 6, 2014 from http://www.scribd.com/doc/48271633/4-mobile-computing

Lebek, B., Degirmenci, K. &Breitner, M.H. (2013) *Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use Byod Mobile Devices*, Proceeding of AMCIS 2013 Conference.

Limonczenko, M. (2014) *Why BYOD is like cancer (And how Endpoint security is the cure)*, retrieved on 2 June 2014 from

www.business-software.com/blog/byod-like-cancer-endpoint-security-cure/

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

McCann, S. V. (2013) MetApp: an efficient and cost saving method for small businesses to create iOS applications, University of Texas, Electronic Theses and Dissertations

McLarty M. (2012) *BYOD is unstoppable : Smart companies must build apps*, retrieved on April 1, 2014 from http://gigaom.com/2012/04/08/byod-is-unstoppable-smart-companies-must-build-apps/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+webworkerdaily+%28GigaOM%3A+Collaboration%29

Miller K. W., Voas J. &Hurlburt G. F. (2012), *BYOD: Security and privacy considerations*, IT Professional, pp 53-55

Moore, C. & Warner, J. (2013) "Industry Contexts and Constraints Diversify Approaches To Bring-Your-Own Technology, December 13, 2012.

Morrow B. (2012) *BYOD security challenges: control and protect your most sensitive data*, Network Security, vol. 2012, no. 12, December, pp. 5-8

Niehaves B., Köffer S., &Ortbach K. (2013) *IT consumerization under more difficult conditions: insights from German local governments*, Proceedings of the 14th Annual International Conference on Digital Government Research, pp. 205-213

Phifer L. (2013) *Bring your own danger*, Information Security, pp. 29-35

POPIA (2013) *Protection of Personal Information Act, Act No4 of 2013*, Government Gazette, 581(37067), 26 November 2013

PricewaterhouseCoopers (2012)Bring Your Own Device: Agility through Consistent Delivery, retrieved on 12 June 2014 from http://www.pwc.com/en_US/us/increasing-it-effectiveness/assets/byod-1-25-2012.pdf

Putri, F. &Hovav,A. (2014) Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory, Twenty Second European Conference on Information Systems, Tel Aviv 2014.

Royeen, C. (1997)*What is Sampling? (A research primer in occupational and physical therapy)*, American Occupational Therapy.

Ruighaver A.B., Maynard, S.B. & Chang, S. (2007) *Organisational security culture: Extending the end-user perspective* , Computers and Security, vol. 26, pp. 56-62

Santhana, S. & Kumar A. (2011), *Mobilizing SAP Enterprise Applications,* viewed April 2, 2014, from http://www.infosys.com/SAP/thought-leadership/Documents/mobilizing-enterprise-applications.pdf

Schlienger T. &Teufel S. (2003), *Analyzing information security culture: increased trust by an appropriate information security culture*, In the proceedings of 14th International Workshop on Database and Expert Systems Applications, IEEE

Schneier B. (2003), *Beyond fear: Thinking sensibly about security in an uncertain world*, Springer New York

Semer L. (2013) *Auditing the BYOD Program* , Internal Audit, February, Vol.70, no.1, pp. 23-27

Sen P. (2012) *Consumerization of Information Technology Drivers*, Benefits and Challenges for New Zealand Corporates, Magisteruppsats, School of Information Management, Victoria University of Wellington

Sofaer, S. (1999)*Qualitative methods: what are they and why use them?* Health services research, Vol.34, 1101.

Snow, D. (2014) *BYOD versus corporate-liable: How do you COPE?* Retrieve on 2 June 2014 from www.itstrategist.net/articles/share/125541

Steven, F. (2013) *Mobile Devices: Securing mobile devices: technology and attitude*, Network Publishing

Tam, F. & Villanueva, K. (2013) BOYD: should convenience trump security? Retrieved on 2 June 2014 from www.mossadams.com/.../Moss-Adams-Webcast-BYOD-March-2013.pdf

The Economist (2013) *The rise of the customer-led economy*, retrieved on 14 January 2014 from http://www.economistinsights.com/sites/default/files/EIU_Salesforce_Proof-7.pdf

Thomas, D.R. (2006) *A General Inductive Approach for Analyzing Qualitative Evaluation Data*, American Journal of Evaluation 2006 27: 237.

Thomson G. (2012) *Feature: BYOD: enabling the chaos*, Network Security, Vol. 2012, No. 2, pp. 5-8

Trend Micro (2012) *The Dark Side of BYOD – Privacy, Personal Data Loss and Device Seizure*, viewed May 3, 2014, from http://blog.trendmicro.com/consumerization-byod-privacy-personal-data-loss-and-device-seizure/

Viljpen, M. (2008) *A framework towards effective control in information security governance*, UnpublishedMasters thesis, NMU, Port Elisabeth, South Africa

Von Solms B. (2000) *From policies to culture*, Computers & Security, Vol.23, No. 4, pp. 275-279

Vroom C. & Von Solms R. (2003) *Towards information security behavioural compliance*, Computers & Security, Vol. 23, No. 1, pp. 191-198

Walker-Osborn, C., Mann, S.& Mann, V. (2013) *To Byod or … Not to Byod*, ITNOW (55:1), March 1, 2013, pp 38-39.

Watson, S. (2014) Why the bring your device trend isn't right for retail? Retrieved on 15 June 2014 from www.retaildesignworld.com/home/article/53da686a134ff-opinion-why-the-bring-your-own-device-trend-isnt-right-for-retail

Weilenmann A. (2003) *Doing Mobility*, Gothenburg studies in Informatics, nr 28, School of Business, Economics and Law, Göteborg University

Whitman M.E. &Mattord H.J. (2012), *Principles of Information Security, Course Technology*, Boston

Wood, A. (2012) *BYOD: The Pros and Cons for End Users and the Business*, Credit Control, Vol. 33, no 7/8, p. 68.

World Wide Worx, 2012, Internet Matters, retrieved on 2 April 2014 from
www.internetmatters.co.za/report/ZA_Internet_Matters.pdf

Xavient (2014)- The implications BOYD in an enterprise, retrieved on June 2 2014 from
https://docs.google.com/viewer?url=https://www.xavient.com/media/9901/the_implications_of_byod_in_an_enterprise.pdf

Yin, R.K. (1994)*Case study research: Design and methods*, London, Sage Publications